Security-First Compliance for Small Businesses

Karen Walsh

CRC Press
Taylor & Francis Group

Security-First Compliance for Small Businesses

Organizations of all sizes struggle to secure their data in a constantly evolving digital landscape. Expanding digital footprints and the rapid expansion of cloud strategies arising from the COVID-19 pandemic increase an organization's attack surface. When combined with limited resources caused by the cybersecurity skills gap, securing small and mid-sized business IT infrastructures becomes more complicated. With limited staffing and budgetary restrictions, small businesses need to create cost-effective, security-driven programs that protect data while also meeting increasingly stringent compliance requirements.

This book bridges the gap between complex technical language and business objectives to create a security-first review of the security and compliance landscapes. Starting from the premise that "with security comes compliance," this book starts by defining "security-first" and then walking readers through the process of creating a holistic security and compliance program.

Looking at security and privacy through the lens of zero trust, this overview of regulations and industry standards provides both background about and implications drawn from modern security practices. Rather than focusing solely on individual cybersecurity frameworks, this book offers insights into best practices based on the commonalities between regulations and industry standards, highlighting some of the primary differences to show the nuances.

Woven throughout are practical examples of solutions that enable small and mid-sized businesses to create "cybersustainable" security-focused policies, processes, and controls that protect today's future for tomorrow's digital ecosystem.

Karen Walsh passed the Connecticut Bar in 2004. She then worked as a Bank Secrecy Act internal auditor and contract compliance manager for fourteen years before discovering her passion for cybersecurity and privacy compliance. She spent eleven years teaching first-year college writing and applies many of the same pedagogical approaches to writing about information security. The *ISACA Journal* published her coauthored pieces on cybersustainability in 2019. Her book *100 Geek Heroines* was published by ABC-CLIO, part of Bloomsbury, in October 2019, and she has also authored chapters in *At Home in the Whedonverse* (MacFarland, 2017) *and Transmediating the Whedonverse* (Springer, 2019).

Security-First Compliance for Small Businesses

Karen Walsh

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

First edition published 2024
by CRC Press
6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742

and by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

Library of Congress Cataloging-in-Publication Data
Names: Walsh, Karen M., author.
Title: Security-first compliance for small businesses / Karen Walsh.
Description: First edition. | Boca Raton : CRC Press, 2024. |
Includes bibliographical references and index.
Identifiers: LCCN 2023008024 | ISBN 9780367652456 (hardback) |
ISBN 9781032550725 (paperback) | ISBN 9781003128588 (ebook)
Subjects: LCSH: Small business—Security measures.
Classification: LCC HV8290 .W3238 2024 | DDC 658.4/7—dc23/eng/20230530
LC record available at https://lccn.loc.gov/2023008024

ISBN: 9780367652456 (hbk)
ISBN: 9781032550725 (pbk)
ISBN: 9781003128588 (ebk)

DOI: 10.1201/9781003128588

Typeset in Adobe Caslon
by codeMantra

This book is dedicated to all past, current, and future business owners solving customer problems.

To my Teen, may you continue to protect your information responsibly, knowing that your actions today can change your tomorrow.

Contents

Acknowledgments

As with any book, this one would not have been possible without the help and support of my personal and professional support network.

To my family, thank you so much for giving me the time and space to work on this, even when a whole chapter magically disappeared.

To my ever-patient Husband, you are the Han to my Leia, but I'm sure you'd answer that with "I know."

To my Teen, thank you for not interrupting me while I was writing, and I promise that I'll spend some extra time with you on GTA.

To my parents, thank you for always telling me to believe in myself and raising me with a strong sense of self.

To Shannon, my hype-woman and business-bestie, thank you for choosing to be my friend and telling me to trust myself.

To Liz, my compliance-geek bestie, thank you for listening to all my rants about new mandates and not sleeping through my long rambling monologues about what these things should say that they don't say.

To AJ, my bestie, my writer ride-or-die, I always have been, am currently, and always will be so grateful for you listening to and supporting all my ridiculous. As Queen Lizzo would say, "In case nobody told you today, you're special."

To Sonia, my personal cheerleading PR squad, thank you for putting me out there, telling me to highlight myself, and making sure that others see me the way you do.

To Jeff, but for your knowledge and guidance around centralized log management, I'd never have been able to understand what "technical compliance documentation" really meant.

To the entire team at Taylor & Francis, especially Gabrielle, thank you for your patience while this book took longer than expected to come together. Without you, I wouldn't be able to share this information with an audience that needs something to help guide them.

Introduction

Securing Customer Loyalty

When the COVID-19 pandemic forced a global lockdown, most businesses changed how their employees managed daily activities. In the span of a few short weeks and months, companies adopted remote work models. Suddenly, people who had been staunch brick-and-mortar shoppers purchased groceries and other essentials online.

Even after the world reopened, many of these behaviors are permanent. Research from 2022 found that online purchases have consistently remained above pre-pandemic levels since October 2020.[1] Similarly, research proves that work models have changed permanently. A 2022 study found the following[2]:

- 60% of employees were fully on-site in 2019, while only 19% were fully on-site in February 2022.
- 8% of employees were exclusively remote in 2019, while 24% were fully remote in February 2022.
- 32% of employees were hybrid in 2019, while 53% were hybrid in February 2022.
- A fundamental result of these changes is that cybersecurity, data privacy, and compliance are now more important than ever. In both the business-to-business (B2B) and the business-to-consumer (B2C) spaces, people care about how companies handle their information.

Cloud Services Providers (CSPs) and Digital Transformation

When people talk about cloud services, they really mean that an organization is renting space and computer power from a company that owns high volumes of servers, the hardware that computers use to run programs or communicate over networks. Just as the organization lacked the financial capacity to pay someone a full-time salary to do eight hours of work per week, they pay the cloud services provider (CSP) for the storage space and compute power they need.

Purchasing enough servers to handle modern business IT needs is expensive and creates a budgeting challenge. Organizations need to understand current and future needs because they must pay for all the hardware upfront while considering how they plan to use the server for its entire lifespan. Additionally, when companies purchase the hardware, they need the staff to maintain it, including updating operating systems and ensuring uptime.

For example, a company with twenty-five to fifty employees that runs a highly trafficked e-commerce website, Software-as-a-Service (SaaS) applications, and a database can spend anywhere from $3,000 to $10,000 on a single server. As the company grows, it needs to purchase additional hardware to accommodate its computing needs. Additionally, the company needs to

- Maintain the hardware's operating system.
- Ensure uptime.
- Troubleshoot issues.
- Pay for electricity and cooling.

Most companies leverage cloud services for the following reasons:

- **Cost**: Cheaper and easier to rent space on someone else's hardware that they maintain.
- **Scalability**: Ability to increase or decrease storage and computer power on an as-needed basis.
- **Speed**: Faster for users to connect and apps to run.

Cloud Services

From a business perspective, comparing cloud services to renting a house is the easiest way to understand the different implementation. Typically, people rent a home because they need someone else to help them:

- Pay the mortgage.
- Pay the property taxes.
- Maintain the property.
- Keep the plumbing and heating running.

CSPs deliver their products the same way, and companies can choose from various implementations. Regardless of the model, all cloud services share the following characteristics:

- **Subscription model**: Paid on a monthly or annual basis with ability to cancel at any time.
- **Physical storage**: Housing the hardware, supplying power, cooling servers to prevent overheating and outages.
- **Maintenance**: Updating operating systems and software.

Infrastructure-as-a-Service (IaaS)

The IaaS model is the basic home rental model. With an IaaS implementation, a company pays for the CSP to

- Provide storage and compute power.
- Maintain the servers.

Platform-as-a-Service (PaaS)

A PaaS model is like renting a furnished home. With a PaaS implementation, a company pays the CSP to

- Provide storage and compute power.
- Maintain the servers.
- Manage operating systems and software.

Software-as-a-Service (SaaS)

A SaaS application is the furniture that lives in a company's digital house. SaaS applications are any programming module that requires a public internet connection. Companies can easily deploy SaaS applications by purchasing the subscription and providing people with passwords. Since users access these programs through a web browser, the organization saves money on storage space.

Digital Transformation and Protecting Customer Data

Digital transformation is the process of adding new technologies that enable business operations. Although most companies had begun a digital transformation journey prior to 2020, the COVID pandemic accelerated those strategies an average of six years.[3] In their rush to maintain operations, most companies incorporated cloud technologies as quickly as possible. Often, they lacked the security capabilities to protect data as they changed their operational processes.

Recognizing these weaknesses, malicious actors targeted cloud infrastructures, leading to the highly publicized ransomware attacks in 2020 and 2021. Although companies tried to keep pace with the changing attack types, they often lacked the resources necessary to hire the right people, implement the right processes, or deploy the right technologies.

Simultaneously, people relied more heavily on digital services and experiences. Even in a post-lockdown world, businesses and consumers want the digital experiences they now recognize as normal, meaning that data security and privacy are increasingly important to a business's success.

The Importance of Legal Trust in Customer Relationships

In both B2B and B2C relationships, data protection matters. Customers want digital experience. Consumers want the applications that suggest items they might like or offer loyalty discounts. Businesses want applications that enable them to process payments or manage their sales pipelines.

Customer data sharing is now a transactional experience. Just as consumers pay a company money for a product, they are willing to share data with a company for an experience.

Companies need to understand that while these are both transactional experiences, they differ in a fundamental way. With a financial transaction, people exchange money for goods and services, meaning they freely give up ownership to and rights over the money. With data, people share information to gain access to an experience, meaning that they never completely give up that data. In many cases, they have no ability to transfer the rights of that data to someone else.

Where money is a replenishable resource, data is finite. People cannot earn a new date of birth. They cannot easily obtain a new government identification number, like social security or driver's license number. This data become a unique identifier.

Companies hold data in legal trust. The legal definition of trust is

> a form of division of property rights and a fiduciary relationship, in which ownership of assets goes to a third party, known as a trustee, and the beneficial enjoyment goes to the beneficiary. The person who transfers the property into the trust is known as the grantor or settlor.
>
> A trust is a right, enforceable in equity, to the beneficial enjoyment of property held by another party who actually holds legal title.[4]

In a data sharing relationship, customers are both the grantors who transfer data to a company, and the beneficiaries who receive the beneficial enjoyment of their data. For example, if someone shares a driver's license number with a bank, the person is still legally able to drive, never losing the benefit associated with that unique identifier. Additionally, they receive the benefit from the bank by being able to open and maintain their account.

As companies collect and use more customer data, their responsibility to the customer changes. In a legal trust, the trustee has a fiduciary duty to the beneficiary. At a high level, companies owe customers a fiduciary duty of good faith and fair dealing, meaning that they need to act with honesty, good faith, and fairness when engaging in daily tasks and organizational operations.

In recent years, a few legislative bodies have started to incorporate the term "data fiduciary." India's 2019 and 2022 attempts at enacting a digital privacy law both contain the term. The 2022 draft Digital Personal Data Protection Bill defines data fiduciary as

> any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.[5]

Similarly, in 2019, the New York state senate included the term in its "drafted but never passed" New York Privacy Act (NYPA) defining a data fiduciary as

> Every legal entity, or any affiliate of such entity, and every controller and data broker, which collects, sells or licenses personal information of consumers, shall exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk; and shall act in the best interests of the consumer, without regard to the interests of the entity, controller or data broker, in a manner expected by a reasonable consumer under the circumstances.[6]

While neither of these draft bills has been passed into law, they highlight changes in how people view corporations' responsibility for data protection. Legislators represent their constituents' interesting, acting as their voice in government. As such, these two draft bills speak to how people need to trust companies yet appear to distrust them.

Building Customer Trust through Digital Trust

Laws that seek to punish an action indicate a lack of trust. Without speed limits acting as a punishment, people would drive too fast and too dangerously. The increased number and severity of data breaches similarly create a lack of governmental and customer trust. When people no longer trust companies to protect their data, they ask for laws that punish poor data protection.

Customers want to give their business to companies that take data protection seriously. Too often, companies have failed to take their data protection responsibilities seriously. Too often, companies have collected and used customer data without acting as a responsible trustee. From both a legal and customer relationship standpoint, organizations need to start building and maintaining digital trust. In recent research, analyst McKinsey defines digital trust as

> confidence in an organization to protect consumer data, enact effective cybersecurity, offer trustworthy AI-powered products and services, and provide transparency around AI and data usage.[7]

By building digital trust based on a foundation of data security and privacy, companies can build brand trust and brand loyalty. Building customer loyalty is a fundamental challenge that many companies face, yet something they recognize brings continued revenue growth. A new customer may only purchase from a company once. A loyal customer purchases multiple times and makes referrals to new customers. Instead of viewing security and privacy as business obstacles, organizations need to view them as revenue enablers.

When organizations embrace digital trust as the foundation for customer brand trust and brand loyalty, they build the customer relationships that grow their business. Trust and loyalty are complex emotional responses driven by conscious and subconscious factors. The American Psychological Association defines loyalty as "faithfulness and allegiance to individuals or social groups."[8] To continue to collect and use data, organizations need to understand that data loss negatively impacts customers' emotional connection to their brand.

Over the years, researchers have studied the impact that emotional factors can have on people's purchasing decisions. Recent research found that a positive brand experience increases the level of trust customers place in a brand. Additionally, this is functionally a bidirectional relationship because brand trust also increases brand loyalty.[9] Further, customer loyalty has an emotional component. Research also found that brand experience, brand loyalty, and emotional attachments to brands are highly interrelated.[10] Customers build emotional attachments with and are loyal to the companies who provide positive experiences and earn their trust.

Organizations use customer data to build positive digital experiences. However, a failure to protect data leads to a negative customer experience that undermines the original reason for processing the information. Modern customers increasingly view their experience, trust, and loyalty through a lens of data protection.

While customers are willing to provide their data to get the services they want, they also have expectations about how companies will use it. McKinsey's research found that digital trust drives consumer choices, as evidenced by[7-]

- 85% of respondents saying that knowing a company's data privacy policies before making a purchase is important.

- 46% of respondents saying that they often or always consider another brand if the one they consider purchasing from is unclear about how it will use their data.
- 54% of respondents saying that they make online purchases or use digital services only after making sure that the company has a reputation for protecting customer data.

By building and maintaining digital trust, companies prove that they are responsible data trustees, ultimately gaining customer trust and loyalty.

A Security-First Approach to Compliance

Too often, organizations see compliance as nothing more than a list of boxes that an auditor needs to check off. When companies take a compliance-first approach to security, they scan through a mandate, write a policy based on headers or checklists, and only review things during their annual audit.

However, IT environments are dynamic. They constantly change and evolve, especially in a digitally transformed world. Today, users have more access to more data than ever before. People are constantly interacting with the organization's data, both from corporate offices and from their homes.

People can collaborate on the same document, changing data without having to retain the older version first. IT teams can spin up containers or virtual machines when they need them and remove them when they finish a project. Business analysts can use a data lake containing the entirety of the company's customer data, including addresses and account numbers.

Companies of all sizes need to comply with data protection mandates. To do this, they need to build a foundation of data security first. A security-first approach to compliance begins by understanding

- What sensitive data the company collects, stores, transmits, and processes.
- Where it stores that data.
- What people can and should access that data.
- What devices people use to access the data.
- How the data travels across and between devices, networks, and applications.

From here, companies begin to look at the different protections that they need to put around data, from limiting users' access to encryption transmissions. Finally, the organizations need to document everything from policies and procedures to daily security activities.

Security-First Compliance for SMBs

While data security and privacy compliance is challenging for organizations of all sizes, it can often feel overwhelming for small and mid-sized companies. Bombarded with information from news media and technology vendors, business owners can struggle finding the information they need. Meanwhile, governments and standards organizations publish new compliance requirements that can be difficult to sift through.

At its core, data security and privacy focus on five primary fundamental control categories:

- User access.
- Device and endpoint security.
- Network security.
- Application security.
- Data security.

For each type of control, companies need to have the ability to

- **Identify**: Know what they have and where it is.
- **Protect**: Have people, processes, and technologies to mitigate risk.
- **Detect**: Be alerted to security incidents and attacks.
- **Respond**: Investigate an issue, contain an attacker, and recover resources to their pre-incident/attack state.

Implementing security and staying compliant will always be a challenge, but understanding the fundamentals and business imperative is possible.

References

1. Croudace, L. (2022, July 11). *How Our Spending Has Changed since the End of Coronavirus (COVID-19) Restrictions – Office for National Statistics*. Retrieved from Office for National Statistics: https://www.ons.gov.uk/businessindustryandtrade/retailindustry/articles/howourspendinghaschangedsincetheendofcoronaviruscovid19restrictions/2022-07-11

2. Wigert, B. B. (2022, November 11). *The Future of Hybrid Work: 5 Key Questions Answered with Data*. Retrieved from Gallup.com: https://www.gallup.com/workplace/390632/future-hybrid-work-key-questions-answered-data.aspx
3. Koetsier, J. (2020, September 10). *97% of Executives Say Covid-19 Sped up Digital Transformation*. Retrieved from Forbes: https://www.forbes.com/sites/johnkoetsier/2020/09/10/97-of-executives-say-covid-19-sped-up-digital-transformation/
4. *Trust*. (n.d.). Retrieved from LII/Legal Information Institute: https://www.law.cornell.edu/wex/trust
5. *The Digital Personal Data Protection Bill, 2022*. (n.d.). Retrieved from Ministry of Electronics and Information Technology, Government of India: https://www.meity.gov.in/content/digital-personal-data-protection-bill-2022
6. *New York State Privacy Act, 2019*. (n.d.). Retrieved from New York State Senate: https://legislation.nysenate.gov/pdf/bills/2019/s5642
7. Boehm, J. G. (2022, September 23). *Why Digital Trust Truly Matters*. Retrieved from McKinsey & Company: https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters
8. APA Dictionary of Psychology. (n.d.). Retrieved from APA Dictionary of Psychology: https://dictionary.apa.org/loyalty
9. Maura, N., Wibowo, J., Candraningrat, C., Fianto, A., & Ekonomi dan Bisnis, F. (2022). *Analysis the Effect of Brand Experience and Brand Innovation on Brand Loyalty with Brand Trust as a Mediation Variable*. Retrieved from DIE: Jurnal Ilmu Ekonomi dan Manajemen: http://jurnal.untag-sby.ac.id/index.php/die/index
10. Maheshwari, V., Lodorfos, G., & Jacobsen, S. (November 2014). Determinants of Brand Loyalty: A Study of the Experience-Commitment-Loyalty Constructs. *International Journal of Business Administration*.

1

Into the Mind of a Malicious Actor

Introduction

Small and mid-size businesses (SMBs) struggle with two unique problems. First, most security experts agree that the cybersecurity skills gap disproportionately impacts smaller organizations' ability to protect data. Second, many SMBs falsely believe that their size reduces the likelihood that cybercriminals will target them. Unfortunately for most SMBs, these two problems amplify one another, ultimately increasing cybersecurity risks.

Cybercriminals already target SMBs precisely because they often lack the resources necessary to establish robust cybersecurity programs. Additionally, many small business owners need to focus their energies on generating revenue, leaving them little time to study the complexities of cybersecurity and privacy. On a basic level, SMBs often hire IT staff who can set up firewalls and ensure device connectivity. However, traditional controls that protected information no longer work as companies need to embrace remote work and move information to the cloud.

Moreover, digital transformation now creates extended ecosystems, even for small and mid-sized businesses. A small online retailer using eBay, for example, might add third-party integrations for services like listing and inventory management, order management, shipping and fulfillment, advertising and marketing, accounting and analytics, or repricing. These applications that streamline the business's operations connect to the eBay account and increase cybersecurity risk. A small business owner with an eBay shop may want to connect a Shopify account to automatically update listings and pricing in real time. Shopify uses an application programming interface (API) that allows it to "talk" to the eBay platform. The API creates a digital access point

DOI: 10.1201/9781003128588-1

to the eBay platform. A malicious actor might be able to eavesdrop when the two digital systems "talk" to one another, similar to leaving a door open during a private office conversation and having someone listen in without being noticed. Ultimately, that "one-click integration" that the retailer uses could lead to a data breach that bankrupts the company or loses customer trust.

Regardless of size and industry, all businesses collect, transmit, and store sensitive information. The data can be as simple as a user email and password for a rewards account or as complex as electronic protected health information (ePHI). In order to protect the business's reputation and financial stability, owners need to understand the risks facing them, why cybercriminals target them, and how different types of attacks work.

Data Breach Statistics for SMBs

Although companies conceptually understand the cybersecurity risks, many lack the time to research the statistics underscoring SMB risk. Often, owners erroneously assume that their organization's size protects them from cybercriminals. A large enterprise with over two million customer records seems like a better payout than a small business with 5,000 customer records. However, the large enterprise often has more financial and human capital to spend protecting information, making it harder to gain access to systems, networks, and software. If it takes a cybercriminal less time to infiltrate five small businesses than it takes to gain access to one large enterprise, the cost–benefit analysis makes attacking the SMB more appealing.

Likelihood of Experiencing a Data Breach

Like all research, data breach statistics largely depend on aggregating individual experiences and finding patterns. Problematically, the research provides little definite response. Additionally, research for 2020 focuses on cybercriminals leveraging the rapid move to remote workforces that left many enterprise organizations struggling to secure the extended perimeter.

At first glance, the data looks grim. The Ponemon "2019 Global State of Cybersecurity in Small and Medium-Sized Businesses"

(Global State) studied 2,176 individuals across the United States, United Kingdom, and Europe working in organizations with less than 1,000 employees. Additionally, the study compared data collected in fiscal years 2017, 2018, and 2019 for comparison purposes. The number of organizations that admitted to experiencing a cyberattack in the last twelve months maintained stable across the three-year period, ranging between 61% and 67%. However, the data showed that from 2017 to 2019, the percentage of companies experiencing a data breach in the last twelve months increased steadily from 54% in 2017 to 63% in 2019.[1] Meanwhile, the "2020 Data Breach Investigations Report" (DBIR) which also defines small businesses as under 1,000 employees found that 28% of breaches involved small business victims.[2] Looking critically at the two studies, they seem to provide extremely different information around SMB data breaches.

While the Global State report indicates that two out of every three SMBs experienced a data breach in the last twelve months, the DBIR reduces that to slightly less than one out of three. However, the impact of the COVID-19 pandemic on cyber attacker decisions needs to be considered when comparing these numbers. An Interpol report in August 2020 explained, "to maximize damage and financial gain, cybercriminals are shifting their targets from individuals and small businesses to major corporations, governments and critical infrastructure, which play a crucial role in responding to the outbreak."[3] In other words, the change in attack percentages between the 2019 and 2020 reports could be indicative of the shift in cyber attacker targeting decisions. Normally, large enterprises have more resources to secure data, making infiltrating their systems, networks, and software more difficult. The rapid move to remote workforce, however, left many traditional controls ineffective which made it easier to gain access to enterprise data. In other words, the pandemic lowered the cost associated with attacking the enterprise organization while simultaneously increasing the benefit because large companies store more data.

Another problem when trying to quantify SMB risk is that no standard definition of small or mid-sized business exists. For example, research from February 2020 focused on businesses with under fifty employees, noting that while nearly 60% of owners felt that they were not likely to be targeted by cyber criminals, 18.5% had experienced a

cyberattack or data breach in the previous twelve months.[4] Compared to the other two reports, this research hints that just under one in five small businesses experience a data breach. However, by defining SMB as a business under fifty employees, the study removes many businesses that fell into the category for the other reports.

Cyber attackers primarily focus on getting the largest return on their investment. When SMBs provide the easiest avenue for stealing information, cyber attackers will focus on them. When the large enterprise provides the easiest avenue, cyber attackers will focus their efforts on those organizations. This shift in focus provides an example of what security professionals mean when they say that cyber criminals continuously evolve their methodologies.

Costs Associated with a Data Breach

Costs associated with data breaches continue to increase every year because malicious actors continuously change their attack methods. As soon as security professionals manage to protect against one attack method, criminals find new ways into networks, devices, software, and systems.

The difficulty in reviewing data breach costs for SMBs is that the research can be deceiving depending on how it presents the question. For example, one April 2020 study noted that while 73% of respondents had paid a ransom in the previous twelve months, 43% of those were in the $10,000–$50,000 range, while 13% paid more than $100,000.[5] However, this research focused only organizations hit by a ransomware attack and the ransom paid. While ransomware may be the most prevalent attack method, the research did not incorporate other types of data breaches nor the additional legal costs and compliance fines that companies also need to pay.

The IBM "Costs of a Data Breach" report incorporates all attack types as well as the additional notification, legal, and compliance costs. The report notes that between 2019 and 2020, the costs associated with a data breach decreased for organizations under 1,000 employees but increased for organizations between 1,000 and 10,000.[6] The average cost of a data breach for companies with less than 500 employees was $2.35 million, while organizations between 500 and 1,000 employees

paid on average $2.53 million.[6] Comparing the ransomware payment costs to the total costs of a data breach in the SMB universe shows a staggering difference between one ransom payment and the total costs of a data breach.

Expanding on this, the costs arising from notification, fines, and legal fees bring into focus the total impact a breach can have on a company's financial solvency. The 2020 NetDiligence "Cyber Claims Study" reviewed 3,547 claims between 2015 and 2019, including 1,633 new claims made in 2020.[7] The "Cyber Claims Study" focuses on data incidents, not just breaches, which expands the number of claims. Data incidents include "recordless" events or those events where cybercriminals did not steal the data. Defined as companies under $2 billion in annual revenue, SMEs had an average revenue $92 million and accounted for 98% of the claims.[7] This indicates that despite the large dollar values associated with front-page news breaches, SMEs file significantly more cyber insurance claims. These data indicate that cybercriminals focus more heavily on SMEs than large enterprises, despite the lower dollar values per data breach.

By looking at reported insurance claims, the "Cyber Claims Report" provides insight into the breakdown of cost types. For example, according to the report, SMEs spent on average[7]:

- $175,000 on all costs associated with the incident.
- $131,000 on crisis services such as counsel, notification costs, forensics, credit/ID monitoring, and public relations.
- $276,000 on business interruption.
- $83,000 on legal costs such as lawsuit defense, lawsuit settlement, regulatory action defense, and regulatory fines.
- $33,000 on recovery expenses.

Additionally, the industries impacted differed when comparing large enterprise to SME. Under large companies, financial services institutions spent the most on data breaches with an average of $22.9 million. For SMEs, however, professional services spent an average of $245,000 and financial services organizations spent $237,000.

Looking at the average costs only tells one part of the story. Averages aggregate all claims and divide by the total number of claims made, which means that a single extremely large loss can skew the numbers.

A look at the median costs gives a slightly different, but still disconcerting story. Because the median looks at the number where half the numbers in the set are lower and half are higher, it can also adjust for the outliers that fold into the average. According to the report, the median costs associated with data incidents were as follows[7]:

- $36,000 on all costs associated with an incident.
- $25,000 on crisis services.
- $10,000 for legal/regulatory costs.
- $34,000 on business interruption.
- $11,000 on recovery expenses.

These numbers show that while a few very large data incidents can skew the average, most of the costs appear more reasonable. However, "reasonable" for an SME with $2 billion in revenue might be very different from an organization with only $11,000, which was the smallest organization in the data set.

SMEs with revenue under $50 million constituted 53% of the claims for the period of 2015–2019. For 2019 alone, the nanorevenue group constituted 46% of the data incident claims. The incident costs for this "nano-revenue" group were as follows[7]:

- Minimum: $1,000 reported.
- Maximum: $7.1 million reported.
- Average: $91,000.
- Median: $41,000.
- Total: $145.4 million.

Small businesses suffer the most from even the smallest data incident. For example, if the data incident costs are $1,000, the amount is 9% of the company that generates $11,000 in annual revenue. If the incident costs anything more than $11,000, that organization is bankrupt. Data incidents that appear "low cost" can have a devastating impact on a startup or small family business.

Types of Attacks

Nearly all the research supports the point that ransomware and social engineering attacks wreak the most havoc on SMBs. The "Cyber

Claims Study" lists ransomware, social engineering, business email compromise, and "hacker" as the top four causes of a data incident. This causes a problem when trying to connect the dots. First, the report fails to define "hacker." Second, all four of these data breach types overlap. Social engineering attacks often incorporate phishing, which is a type of business email compromise. Many business email compromise or social engineering attacks lead to installation of malware that drives a ransomware attack. With the interconnection between these, the data in that report provide little visibility into the most common attack methods. An article in *Security Magazine* from January 2020 corroborates this data, noting that 46% of respondents believed ransomware was the largest threat, while 25% felt phishing was the greatest threat.[8] Although these threats are most prevalent regardless of organizational size, SMBs are often more vulnerable to them.

Bringing together all the data, cybercriminals appear to focus on attacking SMBs and might be more successful.

Why SMBs Can Be a Better Target Than Enterprise

At first glance, SMBs seem as though they would be less enticing targets for cybercriminals. Since cybercriminals take a cost–benefit approach when choosing targets, the fact that SMBs hold less data overall than enterprise or Fortune 500 companies should mean they offer less benefit. However, SMBs also have fewer resources to protect their IT stack. Since they may be easier to infiltrate, cybercriminals spend less time to gain access to sensitive data.

The data support this assertion. In March 2020, *Agility SMB* published a collection of statistics that highlight the dissonance between small business owner beliefs and cybersecurity realities. For example[9]:

- **43%**: Percentage of cyberattack targeting small businesses.
- **1 in 323**: Ratio of malicious emails small businesses receive.
- **121**: Number of emails the average employee receives in a day.
- **40%**: Percentage of SMBs experiencing eight or more hours of downtime from a cyber breach.

Depending on the research source, data around SMB IT staffing and cybersecurity tell multiple stories. For example, the 2020 SMB IT Security Report by network security firm Untangle found that 32% of respondents identified budget as their greatest barrier.[10] Meanwhile, 13% of respondents indicated that they have limited time to research and understand emerging threats.[10] Meanwhile, a 2020 report by industry leader Cisco, "Big Security in a Small Business World," gives further insight into some of the Untangle findings. First, the Cisco report notes that SMBs felt budget constraints remained their top challenge while lack of trained personnel tied for third place.[11] The lack of budget and appropriately trained staff has often been seen as one reason cybercriminals target SMBs. While they may collect, store, and process less sensitive data than the large enterprise, they often have less resources to allocate to data protection.

SMBs recognize the need to secure information and look to find ways around these constraints. For example, the Cisco report also noted that 60% of SMB respondents indicated having twenty people or more dedicated to cybersecurity.[11] This last fact indicates that SMBs may be outsourcing cybersecurity operations, leveraging managed services providers. For many SMBs, business solutions "as a service" provide a lower-cost option. An article in *ZDNet* noted that IT staffing salaries limit the ability to add additional full-time employees, making outsourcing technology support services appealing.[12] In combination, these two articles indicate that SMBs recognize leverage managed services providers to reduce cybersecurity risk with limited budgets.

Fundamentally, SMBs know that they must secure data and protect privacy. However, the logistics and costs often act as barriers. As companies move to cloud-first and cloud-only models, the traditional controls that protected SMBs, like firewalls, become less effective. Meanwhile, a project that protects the identity perimeter, such as attribute-based access controls, often requires specialized training, time commitments, and infrastructure spending. As SMBs look to retain customers or grow their business, owners and senior leadership need to understand how cybercriminals think and the most common attack methodologies so that they can create cost-effective programs for managing data security and privacy.

Common Attack Methodologies

Although cybercriminals can gain unauthorized access to systems, networks, and software in various ways, they consistently apply certain attack methodologies because they work. When small business owners understand the attacks malicious actors will use against them, they can build stronger security programs.

Malware/Ransomware

The 2020 Cisco "Big Security in a Small Business World" report found that ransomware, a type of malware, was the most likely threat to cause downtime for small and large businesses.[11] During the COVID-19 pandemic, when companies of all sizes needed to adapt rapidly to remote work and stay-at-home orders, cybercriminals doubled down on their malware and ransomware attacks.

Malware is a type of software that cybercriminals use to disrupt, damage, or gain unauthorized access to systems, software, devices, and networks. Often, cybercriminals hide malware in phishing emails using fake downloadable documents or links that then install the malicious software on a user's device. Once installed, the malicious software continues to run in the background while the user works with legitimate software such as Word or Excel.

For example, in 2020, researchers detected a malware that targeted file storage servers.[13] Once installed on the device, the malware's code rewrote the code on the device to prevent security patch updates.[13] When security teams thought they had updated the software, the malware would create a "loop" that automatically uninstalled the security update.[13] This process allowed the malware to continue to exfiltrate information even though the security team was engaging in best practices.

Ransomware is a type of malware that traditionally encrypts information to make it unusable. Encryption is a way of using code to scramble information and make it unreadable. In many cases, digital encryption turns letters into numbers so that people cannot decipher the text. Ransomware is a digital "kidnapping" of data. Once the cybercriminals encrypt the data, they hold it "hostage" and ask

companies to pay a "ransom." Upon payment of the ransom, the malicious actors unencrypt the data so that the business can get up and running again. In the early days of ransomware, most organizations struggled because they did not have adequate backup copies of their data. Once encrypted, they were unable to maintain business continuity. In recent years, more organizations have created strong backup and recovery programs to undermine cybercriminals. In response, ransomware attacks in recent years now also incorporate data theft and encryption. Because the cybercriminals now have copies of the data as well as having scrambled it, organizations need to pay the ransom because the backup alone no longer protects them if the cybercriminals choose to sell the stolen information.

Dictionary Attack/Brute Force Attack

Dictionary and brute force attacks both leverage poor password hygiene. With a dictionary attack, cybercriminals use a "dictionary" or database of known weak passwords combined with software that they can find on the Dark Web to guess a login ID and password combination. For example, many devices, such as routers or servers, come with default administrative passwords. Not only are these passwords often weak, but they are also easily found in user manuals on manufacturers' websites. Additionally, despite employee cybersecurity awareness training, many users still use weak passwords. One common list, SecLists, on Github has the ten million most common passwords available to anyone who wants to use them in a dictionary attack.[14] Another dictionary attack methodology uses a guess about usernames by using the organization's "naming mechanism" and then runs common names against the most commonly used passwords. Organizations tend to use one of the several variations when setting email address IDs:

- **FirstName.LastName**: John.Smith@company.com
- **FirstNameLastName**: JohnSmith@company.com
- **FirstNameInitialLastName**: JSmith@copmany.com

Once cybercriminals determine the formula the organization uses, often by looking up employees on social networking websites like

LinkedIn, they apply the most used passwords and hope that they get lucky.

A brute force attack is a more sophisticated version of a dictionary attack. Where a dictionary attack applies a list of well-known passwords, the brute force attack tries every possible combination of login and password. As part of this, the software that cybercriminals use takes into account probabilities around weak passwords and how people normally follow corporate password policies.

Corporate password policies often use the same "best practices" requirements such as a minimum number of characters, at least one upper-case letter, at least one number, and/or at least one special character. The software will often take into account that people tend to capitalize the password's first letter or use the number "1" at the end of the password. Additionally, the algorithm may prioritize weak passwords.

Ultimately, brute force attacks take the dictionary attack to the next level, making them more sophisticated.

Credential Theft

Although credential theft is less a single methodology and more a category of attack types, they are increasingly important as organizations use more cloud-based technologies. Most credential theft attacks start with social engineering methodologies.

Phishing, spear-phishing, and whaling are the most common social engineering attacks used to steal credentials. A phishing attack is when the cybercriminal sends a fake email, such as suggesting the victim needs to change a login password. In a spear-phishing attack, cybercriminals target users at a specific organization. In a whale-phishing attack, cybercriminals target senior leadership or management team members. Despite targeting different users, all of these attacks use the same general social engineering principle to steal credentials.

Social engineering preys on emotions. A typical social engineering attack starts by getting the victim to feel a strong emotion, such as fear. Then, it creates a sense of urgency, suggesting that the victim needs to take immediate action to prevent a bad thing from happening.

Generally, the action the victim takes is downloading a document or clicking a link in the email. The download often drops a malware used to track keystrokes, or keys the person types. The malicious links often look like the login page for a well-known brand, such as bank, video streaming service, or shared drive. When the victim types their ID and password in the fake website, the cybercriminal obtains it. For example, during the COVID-19 public health emergency, Interpol noted that between January and April 2020, approximately 907,000 spam messages, 737 malware-related incidents, and 48,000 malicious URLs related to COVID.[3] Because people's fear and desire for information outweighed their risk-averseness, the early days of the pandemic created fertile ground for social engineering attacks.

If the cybercriminals targeted an organization to get employees' login ID and passwords, they can use those to get access to the company's resources. Once the malicious actor gains access to systems, networks, or software, organizations often struggle to detect them. With stolen credentials, the attackers disguise themselves as people who *should* have access, so the organization's security staff only detect the infiltration if they notice abnormal resource use.

Administrative credentials offer the most return on investment because they have the most access to resources. However, even a standard user credential can be dangerous. Cybercriminals know how to take standard credentials and elevate privileges to turn them into the equivalent of an administrative account.

As organizations use more cloud-based resources, credential theft has become a primary attack methodology. As digital transformation increasingly abstracts IT infrastructures, login IDs and passwords become more valuable to cybercriminals.

Cross-Site Scripting (XSS)/SQL Attacks

Most organizations use web applications. For example, any software that a user logs into with a web browser, such as Google Chrome or Safari, is a web application. When a user logs into the application, they need to input a username and password. Cybercriminals use XSS and SQL attacks to steal this information.

Many web-based databases and servers use the Structured Query Language (SQL) coding language which enables programmers to organize information and put it into readable tables that make sense to users.

SQL injections, one of the least sophisticated attacks, take advantage of web page security weaknesses. The malicious code infiltrates databases by replacing traditional login code used with web applications so that when users enter their name/ID and password, the cybercriminals can obtain access to the databases.

SQL injections are dangerous primarily because SQL is a database language that provides access to databases, allowing for data manipulation. The standard coding allows users to retrieve, update, and remove data.

Often shortened to "XSS," cross-site scripting attacks target users' browsers rather than the applications. A type of web application vulnerability that also incorporates malware, an XSS attack installs a malware on the user's browser, then leaves the malware on the application and the device. Although this attack is a hybrid, its goal is to steal web application login information for the same reason that a malicious actor would engage in a SQL attack, ultimately making it a web application security issue.

Distributed Denial of Service (DDoS) Attack

In a DDoS attack, cybercriminals attempt to overwhelm a server by sending them multiple service requests. The attack relies on an army of "bot" computers, or a series of computers infected with a virus, that the malicious actor then commands to send messages to the server. The server gets overwhelmed attempting to respond to the requests, ultimately shutting down and crashing. For example, imagine being a kindergarten teacher in a room of twenty-five very curious children. If the children raise their hands, the teacher can answer them one at a time. If all twenty-five children are asking questions at the same time, the teacher can become overwhelmed and unable to answer any of the questions. In a DDoS attack, the bots bombard the servers, much like the twenty-five children asking questions all at once. Similarly, the company's server becomes overwhelmed and unable to function, much

like the overwhelmed teacher is unable to answer all the questions at once.

To build a botnet, the cybercriminal, or botmaster, needs to infect as many online devices as possible with malware. Using a trojan horse virus, the botmaster infects systems through phishing attacks or pop-up ads on websites. Since many botnet infections use only a small amount of computer memory, people may not even notice the infection. Thus, the infected device continues to send requests to the internet. Moreover, many of the infections can self-propagate, which means they can seek out other infected devices automatically and connect to them.

The botnet C&C protocol is the server that commands the network of infected computers. These centralized machines send commands and receive outputs. They can come in four different forms. A star C&C structure is a single server that sends commands to every infected computer within the botnet, yet these setups are easy to disrupt by locating and neutralizing the commanding server. The multiserver structure consists of multiple central servers, similar to a battalion of soldiers directed by a general, which makes shutting down the attack more difficult. A hierarchic structure divides botnets into separate chunks making it difficult to locate the primary attack server, similar to a king commanding multiple generals who control multiple battalions.

Conclusion

In cybersecurity as in sports, the best offense is a good defense. Before putting together any compliance program, security-first or otherwise, organizational leaders need to understand the risks facing their IT stack. An enterprise-level CEO may have twenty or more years in business, creating a depth and breadth of experience in risk management. However, SMBs often have CEOs or CFOs with deep industry knowledge that might not include IT and data protection. The best way to protect the organization is to understand the places cybercriminals most often attack and the ways they successfully steal information. Informed leadership is effective leadership.

Small businesses across industry verticals collect more sensitive data than they realize. A consulting business established as a sole

proprietorship may collect and store non-public client information such as names, email addresses, and physical addresses. A small online store selling handmade crafts collects payment information, including credit card data, addresses, and names. A sole-owner therapist still needs to protect patient data privacy and meet strict compliance requirements.

Moving beyond the smallest businesses, mid-sized organizations face additional concerns. Startup technology companies need to secure their technologies, but they also need to make sure that their business operations protect data security and privacy. Mid-sized services companies looking to grow might need to prove that they have secure business processes to bring investors on board.

The definition of SMB includes everything from the stay-at-home mom making handmade soap to the 500-person organization with $50 million in funding. Because no set definition exists, no single security program can cover the different needs each business has. However, fundamentally, they all need to understand that they face the same risks regardless of size. The mom making handmade soap needs to understand that if the platform she uses for her shop has a history of data breaches, she puts her customers and business at risk. The startup needs to keep security in mind from the start because eventually investors will require reporting.

In a digitally transformed world, business success relies on information. Adopting cloud-based technologies to create business IT ecosystems transforms every business into an IT company on some level. Every day business owners make IT decisions. They choose Microsoft OneDrive over Google Drive. They choose to connect their invoicing systems with their bank accounts. They choose to use Shopify or Stripe as ways to collect payments. They choose payroll systems. They choose HR applications. They connect all the different technologies so that they can save time and reduce operational costs. Each choice is an IT decision, that may not always be made by an IT person.

Protecting data security protects business stability. As small businesses make IT decisions, they need to do it purposefully. They need to know the risks and meaningfully accept them. They need to understand the potential legal or compliance risks.

References

1. Ponemon Institute, LLC. (2019, October). *Keeper Security*. Retrieved from 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses: https://www.keeper.io/hubfs/2019%20Keeper%20Report_Final%20(1).pdf
2. Ponemon. (2020). *Verizon* 2020 *Data Breach Investigations Report*. Retrieved from Verizon: https://enterprise.verizon.com/resources/reports/dbir/
3. Interpol. (2020, August 4). *Cybercrime: COVID-19 Impact*. Retrieved from Interpol: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
4. BullGuard. (2020, February 19). *New Study Reveals One in Three SMBs Use Free Consumer Cybersecurity and One in Five Use No Endpoint Security at All*. Retrieved from PRWeb Cision: https://www.prweb.com/releases/new_study_reveals_one_in_three_smbs_use_free_consumer_cybersecurity_and_one_in_five_use_no_endpoint_security_at_all/prweb16921507.htm
5. Staff, D. R. (2020, April 16). *Small Business Is Big Target for Ransomware*. Retrieved from Dark Reading: https://www.darkreading.com/attacks-breaches/small-business-is-big-target-for-ransomware/d/d-id/1337583#:~:text=According%20to%20a%20new%20survey,%25)%20have%20paid%20a%20ransom
6. IBM. (2020). *Cost of a Data Breach Report* 2020. Retrieved from IBM: https://www.ibm.com/security/data-breach
7. NetDiligence. (2020). *Cyber Claims Study* 2020 *Report*. Retrieved from NetDiligence: https://netdiligence.com/wp-content/uploads/2020/11/NetD_2020_Claims_Study_1.1.pdf
8. Staff. (2020, January 23). *SMB Budget Constraints and Increase of Cyberattacks in* 2020 *among Top Cybersecurity Concerns*. Retrieved from Security Magazing: https://www.securitymagazine.com/articles/91592-smb-budget-constraints-and-increase-of-cyberattacks-in-2020-among-top-cybersecurity-concerns
9. SMB Consortium. (2020). https://agilitysmb.com/2020-cybersecurity-statistics-for-smbs/.
10. Untangle. (2020). SMB IT Security Report. (n.d.). https://www5.untangle.com/2020smbitsecurityreport.
11. Cisco. (2020). *Big Security in a Small Business World*. Retrieved from Cisco Secure: https://www.cisco.com/c/dam/global/en_uk/products/security/pdf/2020_cisco_smb-cybersecurity-report_uk.pdf
12. McLellan, C. (2021, December 22). Tech Priorities for Small Business in 2022: Here's What's Top of the Shopping List. ZDNET. https://www.zdnet.com/article/outsourcing-and-everything-as-a-service-business-tech-priorities-for-2020/.
13. SecurityScorecard. (2020). QSnatch Technical Report. Retrieved from SecurityScorecard: https://s3.amazonaws.com/ssc-corporate-website-production/documents/qsnatch-technical-report.pdf
14. https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10-million-password-list-top-100.txt

2

Reviewing the Compliance Landscape

Introduction

Regulatory compliance is nothing new for businesses or IT departments. For example, financial institutions, such as banks and credit unions, have been regulated since the National Bank Act of 1863.[1] Privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) enacted in 1996, are nothing new either. However, over the last ten years, legislative bodies at local, country, and regional levels have begun to focus on data security and privacy more purposefully. With companies expanding their data collection and adding new technologies for business enablement, governments increasingly add more security and privacy regulations to their books as a way to protect their citizens.

In fact, the first privacy law in the United States dates back to the Colonial era. Common law, legal standards created through litigation rather than enacted as regulations, protected people from eavesdropping, defined as listening to conversations under walls, windows, or "eaves of houses."[2] In the 1800s, technology started complicating the concept of privacy. Invented in 1844, the telegraph communications between Union and Confederate armies became valuable military intelligence, leading the opposing armies to tap wire communications for the first time.[2] In short, for as long as technology has existed, it has created privacy concerns.

Modern technologies, despite their sophistication, pose the same problems as telegraph messages. Just as telegraph messages transported information from one area to another, today's technologies do the same thing, only faster. While the methodologies have evolved with new technology, the principles underlying data security and privacy remain fundamentally the same. For example, the first national privacy legislation, Sweden's 1973 Data Act, required organizations collecting personal data to obtain a permit from the Data Inspection Board.[3] The

DOI: 10.1201/9781003128588-2

history of the Data Act aligns with the evolution of privacy law generally. Although amended significantly over time, the law considered outdated by the 1990s.[3] As is the case with most regulations, government moves slower than technology. Since governing bodies need to follow democratic processes, they often fail to update laws in a timely manner. Discussion, consensus, and voting all take time, preventing regulations from evolving fast enough to stay ahead of cybercriminal activities.

As the regulatory landscape continues to expand, organizations need to understand the evolution of cybersecurity and privacy laws. If businesses remain unwilling to secure data on their own, governmental bodies will continue to add more laws, likely with increasingly stringent requirements and heavy fines.

Regulatory Landscape Overview

The Health Insurance Portability and Accountability Act (HIPAA)

Enacted in 1996, HIPAA remains one of the most impactful privacy laws in the United States. In passing HIPAA, the US congress sought to protect individual's health information, called protected health information (PHI), and give patients more control over how the healthcare industry used this information. The law required "covered entities," defined as healthcare providers, healthcare clearing houses, and health insurance companies, to obtain permission for sharing PHI with one another or with a patient's family members. Over time, the Department of Health and Human Services (HHS) added new requirements to try to keep pace with the digitalization of patient data. In December 2000, HHS published the Privacy Rule that required covered entities to protect individually identifiable health information. Three years later, HHS published the Security Rule that established national standards for protecting electronic PHI (ePHI) confidentiality, integrity, and availability. In 2009, US Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act, which intended to improve data sharing efficiency for coordinating care.[4] Ultimately, HHS aggregated HIPAA and HITECH into a single rule called the Omnibus Rule, unifying paper and electronic patient healthcare data protection.

HIPAA can be considered one of the highest impact privacy regulations in the United States. During 2019, HIPAA fines totaled $15,270,000, while between March 2, 2020 and September 25, 2020, healthcare organizations and business associates racked up $11,951,500 in fines.[5] HIPAA's penalty structure intends to force organizations to take privacy seriously. Separated into tiers, the fines levied include[6]:

Tier 1: A minimum of $100 per violation for unknowing violations with an annual maximum of $25,000 for repeat violations. The maximum penalty can be $50,000 per violation with an annual maximum of $1.5 million.

Tier 2: A minimum penalty of $1,000 per violation with "reasonable cause," with an annual maximum of $100,000 for repeat HIPAA violations. The maximum penalty is $50,000 per violation, with an annual maximum of $1.5 million.

Tier 3: If the violation arose out of willful neglect but was corrected within the required time period, the law imposes a minimum penalty of $10,000 per violation, with an annual maximum of $250,000 for repeat violations. The maximum penalty in this tier is $50,000 per violation, with an annual maximum of $1.5 million.

Tier 4: If an organization willfully neglected HIPAA requirements without correcting within the required time period face a minimum of $50,000 per violation, with an annual maximum of $1.5 million. The maximum penalty here is the same as the minimum.

Additionally, HIPAA also established criminal penalties for covered entities separated into tiers as well. Violations include whether the entity knowingly obtained and disclosed PHI, lying to obtain PII and using it inappropriately, and compromising PHI or ePHI with an intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm.[6]

Folded into HIPAA are the Security Rule, Privacy Rule, Breach Notification Rule, and Enforcement Rule. Moreover, HIPAA sets out a series of Technical Safeguards and Administrative Safeguards. From a high level, the Technical Safeguards include[7]:

- Access Controls:
  - Unique User Identification.

    - Emergency Access Procedure.
    - Automatic Logoff.
    - Encryption and Decryption.
- Audit Controls.
- Integrity:
    - Authentication of ePHI.
    - Person or Entity Authentication.
    - Transmission Security.
- Slightly more detail shows that required Technical Safeguards also require[7]:
- Risk Analysis.
- Risk Management.
- Sanction Policy.
- Information System Activity Review.
- Isolating Health Care Clearinghouse Functions.
- Response and Reporting of Security Incidents.
- Data Backup Plan.
- Disaster Recovery Plan.
- Emergency Mode Operation Plan.
- Written Contract or Other Agreement with Business Associates.

Although HIPAA is industry specific, many organizations fall under the broad heading of "business associate," including accountants and law firms. As such, HIPAA's broad reach and high standards act as an introductory template for many subsequent privacy and security laws.

Payment Card Industry Data Security Standard (PCI DSS)

Although not a governmental legislation, PCI DSS incorporates fines for violations similar to regulations. In 2006, five major credit card brands American Express, Discover Financial Services, JCB international, Mastercard, and Visa, Inc. established the Payment Card Industry (PCI) Data Security Council (PCI SSC). Originally intended to protect consumers against credit card theft and fraud, PCI DSS is now a primary compliance requirement for any merchant or financial institution that collects cardholder data.

PCI DSS defines cardholder data as any information on a consumer's payment card including

- Primary account number (PAN).
- Cardholder name.
- Service code.
- Expiration date.
- Magnetic stripe data.
- CAV2/CVC2/CVV2/CID.
- PIN/PIN Block.
- Under PCI DSS, organizations need to segregate their Cardholder Data Environment (CDE) from other networks. Additionally, PCI set forth twelve prescriptive requirements:
- Install and maintain a firewall.
- Remove vendor-supplied defaults for passwords or other security parameters.
- Protect stored cardholder data.
- Encrypt data in transit across open, public networks.
- Install and regularly update antivirus software.
- Develop and maintain secure systems and applications.
- Limit access to cardholder data on a "need to know" basis.
- Identify and authenticate access to system components.
- Restrict physical access to cardholder data.
- Track and monitor access to network resources and cardholder data.
- Regularly test networks, security systems, and processes.
- Maintain an information security policy.

Within each requirement, PCI DSS provides detailed instructions and controls necessary for compliance. For example, Requirement 3, "Protect stored cardholder data," explicitly states that an organization must "Encrypt PAN with either one-way hash function, truncation, index tokens, or strong cryptography to ensure portable digital media, backup media, logs, and wireless networks cannot read PAN."[8]

While any organization that collects payments online or via payment card reader needs to meet PCI compliance standards, the PCI SSC recognizes that smaller organizations have different

capabilities than larger merchants and banks. As such, the Council established four levels defined based on number of total annual transactions:

- **Level 1**: Merchants processing over six million Visa and/or Mastercard transactions per year
- **Level 2**: Merchants processing between one million and six million Visa and/or Mastercard transactions per year
- **Level 3**: Merchants processing between 20,000 and 1 million Mastercard and/or Visa transactions per year
- **Level 4**: Merchants processing less than 20,000 Visa and/or Mastercard transactions per year.

Under PCI DSS, payment card brands can fine a bank attached to a credit card anywhere between $5,000 and $100,000 per month for a compliance violation. Generally, banks then pass the cost of the fine to the merchants. Additionally, banks can either increase transaction fees or terminate their relationship with the merchant. Although the fines are not made public in the way HIPAA fines are, the costs passed on to the merchant can bankrupt a small or mid-sized business.

European Union General Data Protection Regulation (GDPR)

In 2016, the European Union (EU) enacted the GDPR which was later enforced starting in May 2018. The landmark privacy regulation acts as the foundation of many later privacy laws. Most notably, the GDPR set forth the first extraterritorial liability structure. Extraterritorial reach means that organizations located outside the original jurisdiction can be held liable under the law. The GDPR states in Article 3[9]:

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor

not established in the Union, where the processing activities are related to

a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union;
b. the monitoring of their behavior as far as their behavior takes place within the Union;
c. notably, the GDPR focuses on the data subject not the company collecting the data. Data subjects are the users who give the company their personally identifiable information. Looking at Article 3, the language specifically states that the processing does not need to occur in the European Union or by a company located in the EU. Rather, the regulation focuses on whether the data subject is an EU citizen living in the EU or outside of the EU. Additionally, non-EU citizens residing in a country that belongs to the EU are also protected.

The interconnected nature of data security and privacy is also important when looking at the impact the GDPR has on regulatory compliance. In Article 25, the GDPR states[9]:

> The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

This article set forth the principal of "Privacy by Design" which means building data protection through the technology implementation process. In nontechnical terms, "Privacy by Design" means incorporating privacy and security due diligence as part of creating business enhancing technology bundles.

The GDPR also established certain technical requirements that companies need to incorporate as part of building and maintaining

their IT stack. In Article 32, "Security of Processing," the GDPR requires:

> the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
>
> a) the pseudonymisation and encryption of personal data;
> b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
> c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
> d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The GDPR only offers two specific technical controls, pseudonymization and encryption. Other than these requirements, organizations must engage in a risk assessment process and establish their own targeted security controls.

From a privacy, not security, perspective, the GDPR also created significant access governance issues. Unlike security which focuses on external unauthorized access, privacy focuses on limiting the access that authorized users have to information. Generally termed Identity Governance and Administration (IGA), these controls ensure that the right people have the least amount of access necessary to electronic resources to fulfill their job functions. For example, one of the first GDPR fines levied was against the Portuguese hospital, Centro Hospitalar Berreiro Montijo. The Portuguese supervisory authority, Comissão Nacional de Protecção de Dados, fined the hospital 400,000 euros for violations, including violating Article 5(1)(c) for allowing too many practitioners access to ePHI.[10] The hospital failed to limit access appropriately, which meant that even though practitioners were trusted on systems, they had the ability to access information they did not need. While the hospital secured the systems from external malicious actors, it failed to apply the necessary access controls to limit the potential for snooping files.

Supervisory authorities continue to push organizations to meet GDPR compliance. In 2019, GDPR fines totaled €2,256,936,740.00

in fines for 2019 and for the period January 1 through August 31, 2020 fines totaled €3,770,578,154.[11] The GDPR's historic impact on privacy and security cannot be undersold. Many regulations, notably, the California Consumer Privacy Act, borrowed the GDPR principles.

New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 500)

In March 2017, NYDFS, which regulates financial, insurance, and securities institutions, published its Cybersecurity Rule. While a state regulation focused on a single industry might seem innocuous, the NYDFS Cybersecurity Regulation generated a ripple effect across the United States.

From an impact perspective, the NYDFS Cybersecurity Regulation formalized the need for continuous risk monitoring, continuous assurance, enhanced vendor risk management, documented cybersecurity policy, and hiring a Chief Information Security Officer. Although many organizations had these controls in place, the codification of them changed the game for many companies.

From a corporate impact perspective, the continuous monitoring and assurance requirement coupled with the liability for third-party data security incidents established new business models for managing cybersecurity. For the first time, organizations needed to move beyond traditional "point-in-time" audits and provide continuous documentation over their cybersecurity posture. Now, regulated entities needed to not only prove governance over their own security but also monitor their supply stream. The second change to the status quo became a new burden for many organizations. While a company may be able to monitor its own information security monitoring, most organizations focus on vendor submitted questionnaires to validate security posture, which fail to meet the new regulation's definition of due diligence for liability purposes. In other words, regulated entities now need to monitor their vendors as diligently as they monitor themselves.

In July 2020, the NYDFS published its first violation proceeding.[12] According to the charging document, First American Title Insurance Company (First American) left sensitive personal information exposed even after knowing of the security control weakness. From at least

October 2014–May 2019, a known vulnerability in the public-facing website meant that changing a number in the website URL provided access to documents. For example, if the URL for Jan Doe's document was www.website.com/123456 someone with that information could change the number to www.website.com/1234567 and gain access to the document with that identifier. According to the complaint, First American found the vulnerability at least as early as December 2018 but failed to remediate the risk for at least six months.

As the first regulatory requirement in the United States to change data breach liability structures and IT auditing requirements, the Cybersecurity Regulation is a historic document in the cybersecurity realm.

California Privacy Rights Act (CPRA)

Enacted in 2018, the California Consumer Privacy Act (CCPA) granted organizations a two-year window of opportunity to become compliant with a 2020 enforcement date. In November 2020, California voters ratified changes to the CCPA, expanding it to include security requirements and explicating company responsibilities. When comparing the CPRA to the GDPR, the similarities between extraterritorial jurisdiction, data types protected, opt-out rights, and data portability highlight the GDPR's impact on the California legislature. However, the CCPA differs from the GDPR in several significant ways.

The CCPA limits its reach to for-profit companies doing business in California or with Californians that meet one or more of its requirements[13]:

- Gross revenue greater than $25 million.
- Annually buy, receive, sell, or share personal information of more than 50,000 Californians, households, or devices for commercial purposes.
- Earn 50% or more of their annual revenue from selling personal information.

Additionally, the CPRA applies only to consumers instead of all natural persons. These consumers must either be California residents

with primary residence in the state while living temporarily elsewhere or people living in California for more than a temporary period. Additionally, the CPRA extends the definition of "personal information" to twelve categories, including geolocation and biometric data.

Possibly the most important change arising from the CCPA is that it allows people to sue companies in civil court for violations that lead to a data breach. The GDPR and other regulatory requirements prior to the CPRA focused strictly on people being able to send requests to governmental agencies. The CPRA, however, changes that and allows people to directly sue for damages in civil, not criminal, court.

Australian Privacy Act of 1988 (APA) Updated 2019

While many countries choose to pass new laws, others update old ones so they can better align with new risks. Australia, for example, chose to amend its preexisting privacy law rather than tear everything down.

The APA in part follows the CCPA and GDPR by establishing an extraterritorial jurisdiction. However, it distinctly differs from the previous laws by applying to any Australian citizens, companies, or subsidiaries that own or operate an organization. In short, it establishes a broad "Australian link" based on company ownership rather than on data subject, functionally the opposite approach to its predecessors.

The APA also takes data privacy a step further than the other laws. It very specifically defines data breaches as "unauthorized access to, or unauthorized disclosure of" information that "a reasonable person would conclude…would likely to result in serious harm to any of the individuals to whom the information relates" or "information is lost where unauthorized access to, or unauthorized disclosure of, the information is likely to occur" when a "reasonable person would conclude that the access or disclosure would be likely to result in serious harm." In this situation, the legislation provides that the access or disclosure is an "eligible data breach" and an individual is "at risk" from it.[14] Distilling this down, the APA defines a data breach as access to nonpublic data that leads a reasonable person to consider their privacy "at risk."

Significantly, the APA's definition of a data breach focuses on unauthorized access, rather than data download or theft. Additionally, it

creates a "reasonable person" standard to define "at risk." The information, as long as it "relates" to a person and that person would "reasonably believe" the unauthorized access could cause harm, is defined as "at risk." No one needs to download or try to sell the information. The information does not need to directly tie to an individual, it needs to relate to an individual. Although the law is fuzzy around what "relates" means, it can be interpreted as someone else's data that implicates another person. For example, if a person's data is impacted and that person's partner can, as a reasonable person, assume their information is also at risk, both parties are covered by the law.

Although a tiny shift in language, the APA does indicate that legislative bodies recognize the way multiple people's data is connected and looks to expand privacy rights to match the new data landscape.

Cybersecurity Maturity Model Certification (CMMC)

Recognizing the cybersecurity issues throughout the Defense Industrial Base (DIB), the US federal government established CMMC to standardize controls and enhance defense supply chain security. All Department of Defense (DoD) contractors need to meet their assigned CMMC level as part of their contracts.

The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD (A&S)) in conjunction with the Department of Defense (DoD) stakeholders, University Affiliated Research Centers (UARCs), and Federally Funded Research and Development Centers (FFRDC) released the first version of CMMC in January 2020. After much discussion about the impact it would have on the DIB, the governmental stakeholders released CMMC 2.0.

CMMC 2.0 focuses on three maturity levels, defined based on the type of data a company manages.

- **Level 1 foundational**: Organizations managing Federal Contract Information (FCI) must engage in self-assessments that they implement and maintain seventeen practices.
- **Level 2 advanced**: Organizations managing Controlled Unclassified Information (CUI) must engage in triennial third-party assessments and annual self-assessments that they implement and maintain 110 practices mapped to the

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171.

- **Level 3 expert**: Organizations identified by the DoD that must meet this level need to engage in triennial government-led assessments that they implement and maintain the 110 NIST SP 800-171 practices plus a set of additional practices outlined by the DoD.

Additionally, CMMC includes "flow down" provisions, meaning that contractors need to ensure that all their subcontractors comply with their level.

Executive Order on Improving the Nation's Cybersecurity

On May 12, 2021, President Biden released the "Executive Order on Improving the Nation's Cybersecurity" (the EO) that only applies to US Federal Civilian Executive Branch (FCEB) agencies. The EO sits in an odd space somewhere between a law and an industry standard since it only applies to agencies. However, the impact on agencies mirrors a federal law.

While this may likely have flow-down issues for contractors working with FCEB agencies, the EO is groundbreaking because it provides the first directive requiring entities to implement zero-trust architectures.

To enhance the protection of Federal IT, the EO makes specific suggestions around modernizing the approach to cybersecurity, including

- Accelerating cloud adoption.
- Adopting Zero Trust.
- Centralizing and streamlining security analytics.
- Investing in people and technology.

Although the EO includes various other provisions, the focus on zero-trust strategies and the specific requirement that agencies implement multifactor authentication (MFA) highlight shifting cybersecurity priorities based on increased cloud adoption.

Regulatory Requirement Summary

Although security and privacy differ, they significantly overlap with one another. Under cybersecurity regulations, malicious actors need

to either download or take possession of data. However, privacy laws consider unauthorized access, even by a company's employees, to be a data breach if workforce members do not need access to the information to complete their job functions.

Industry Standards Overview

While most business owners worry about regulatory compliance, many also need to understand that regulations give high-level directions. To meet compliance requirements, organizations usually apply controls detailed in industry standards.

Industry standards are often drafted by agencies that do not enforce regulations but can suggest best practices for meeting compliance requirements. While still risk-based, these industry standards often incorporate specific controls, such as encryption requirements, for securing data. Despite significant overlap, the industry standards often differ which means that to meet a regulatory compliance requirement based on multiple industry standards, businesses need to cross map their security controls to multiple frameworks.

Saudi Arabian Monetary Authority Cybersecurity Framework (SAMA CSF)

In May 2017, the Saudi Arabian Monetary Authority (SAMA) issued Version 1.0 of its Cyber Security Framework (SAMA CSF). In the introduction, SAMA noted that applying new online services and new developments, such as Fintech and blockchain, require additional regulatory standards to protect against continuously evolving threats.

SAMA explained its Framework's objectives as[15]:

1. To create a common approach for addressing cyber security within the Member Organizations.
2. To achieve an appropriate maturity level of cyber security controls within the Member Organizations.
3. To ensure cyber security risks are properly managed throughout the Member Organizations.

Moreover, SAMA noted that it relied on frameworks previously established by the National Institute of Standards and Technology

(NIST), Information Security Forum (ISF), International Standards Organization (ISO), BASEL, and Payment Card Industry Data Security Standard (PCI DSS).

The SAMA CSF defines cyber security as:

> the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the member organization's information assets against internal and external threats.

Within that definition, it incorporates specific definitions governing confidentiality, integrity, and availability:

- **Confidentiality**: Information assets are accessible only to those authorized to have access (i.e., protected from unauthorized disclosure or (un)intended leakage of sensitive data).
- **Integrity**: Information assets are accurate, complete, and processed correctly (i.e., protected from unauthorized modification, which may include authenticity and non-repudiation).
- **Availability**: Information assets are resilient and accessible when required (i.e., protected from unauthorized disruption).

The SAMA CSF defines its scope as:

- Electronic information.
- Physical information (hardcopy).
- Applications, software, electronic services, and databases.
- Computers and electronic machines (e.g., ATM).
- Information storage devices (e.g., hard disk, USB stick).
- Premises, equipment, and communication networks (technical infrastructure).

Additionally, it focuses more broadly than other financial cybersecurity frameworks by incorporating applicability to the following industries:

- All banks operating in Saudi Arabia.
- All insurance and/or reinsurance companies operating in Saudi Arabia.

- All financing companies operating in Saudi Arabia.
- All credit bureaus operating in Saudi Arabia.
- The financial market infrastructure.

As a risk-based framework based on organization maturity, SAMA CSF requires formalized policies, controls, and continuous monitoring to achieve a fully functioning compliance program.

International Organizations for Standardization (ISO)

Founded in 1946, ISO's initial delegates from twenty-five countries congregated at London's Institute of Civil Engineers with a mission to coordinate industrial standards. Today, ISO consists of 778 technical committees and subcommittees with members representing 162 countries.

From a cybersecurity standpoint, organizations need to know ISO's 27000-series. The 27000-series incorporates various standards that specify requirements, describe general guidelines, and describe sector-specific guidelines.

From a high level, the mission critical standards include:

- **ISO 27001**: It sets out the requirements for developing and operating a risk-based information security management system (ISMS), including controls that mitigate risks.
- **ISO 27006**: It sets out requirements and offers guidance for audits and ISMS certification.
- **ISO 27002**: It provides a list of common control objectives and best practice controls for implementing and achieving information security.
- **ISO 27003**: It addresses monitoring and measuring information security performance, effectiveness of ISMS processes and controls while also giving guidance into analyzing and evaluating monitoring and measurement.
- **ISO 27005**: It offers guidance on implementing a process-oriented risk management program that fulfills ISO 27001 requirements.
- **ISO 27007**: It provides guidance on conducting ISMS audits and competence of internal and external auditors.

- **ISO 27008**: It gives auditors guidelines for reviewing an organization's implementation and operation of controls.
- **ISO 27014**: It provides guidance on organizational leadership oversight of information security.

ISO sets out broad, risk-based requirements that offer generalized guidance but little step-by-step control suggestions. The lack of specified controls can make it a difficult starting point for organizations with smaller IT departments and limited cybersecurity resources.

National Institute of Standards and Technology (NIST)

As part of the United States Department of Commerce, NIST is not a regulatory agency. NIST releases Special Publications (SP) that outline fundamental controls necessary for US federal agencies to meet their compliance requirements. Many organizations leverage the NIST SPs to set controls since the NIST publications offer more details than ISO standards.

NIST has a Cybersecurity Framework and a Privacy Framework, both of which can be implemented by referring to different Special Publications.

Framework for Improving Critical Infrastructure Cybersecurity (also called the NIST Cybersecurity Framework or NIST CSF) sets forth a core structure consisting of four elements:

- **Function**: Identify, protect, detect, respond, and recover.
- **Categories**: Asset management, identity management and access control, and detection processes.
- **Subcategories**: Specific technical and/or management activities.
- **Informative references**: Standards, guidelines, and practices across common critical infrastructure sectors.

The NIST Privacy Framework establishes implementation tiers and builds on the CSF to incorporate privacy risks across:

- **Functions**: Identify, govern, control, communicate.
- **Profiles**: Current (how an organization manages data privacy in the moment) and target (outcomes needed to achieve privacy risk management goals).

- **Implementation tiers**: Partial, risk informed, repeatable, and adaptive.

In order to implement these effectively, organizations most often refer to the following Special Publications:

- **800-53**: Security and Privacy Controls for Information Systems and Organizations specifies twenty controls, including details and examples for how to implement them.
- **800-53A**: Assessing Security and Privacy Controls in Federal Information Systems and Organizations outlines how organizations and their auditors can appropriately assess their controls to ensure effective cybersecurity and privacy.
- **800-63-3**: Digital Identity Guidelines defines digital identity, sets out a Digital Identity Risk Management process, and continues with companion documents that provide more details including
- **800-63A Digital Identity Guidelines**: Enrollment and identity proofing.
- **800-63B Digital Identity Guidelines**: Authentication and lifecycle management.
- **800-63C Digital Identity Guidelines**: Federation and assertions.
- **800-122**: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) provides confidentiality safeguards including operational safeguards, privacy-specific safeguards, and security controls.

Center for Internet Security (CIS)

CIS is a nonprofit, nongovernmental organization whose mission is to help develop, validate, and promote best practices that protect people, businesses, and governments from cyber threats. Many cybersecurity professionals prefer the CIS Controls and CIS Benchmarks because they provide specific, nearly prescriptive controls for securing data while incorporating a tiered approach that provides flexibility for smaller organizations.

In response to the need for smaller organizations to balance security and cost, CIS released an update that established three Implementation Groups (IGs) with controls and subcontrols.[16]

The three Implementation Groups are defined as follows:

- **IG 1**: Small to medium-sized companies who have staff with limited IT and cybersecurity expertise with data protection.
- **IG 2**: Companies who have staff dedicated to managing and protecting IT infrastructure and who need to meet regulatory compliance requirements.
- **IG 3**: Companies who have a dedicated security team consisting of people who specialize in various cybersecurity areas, operate in a highly regulated industry and who could potentially cause significant harm to public welfare if they experienced a successful attack.

CIS contains eighteen control categories and lists various safeguards within each. Companies start with the basic safeguards, and then incorporate more as they move from one Implementation Group to the next.

The eighteen categories of controls are as follows:

1. Inventory and Control of Enterprise Assets.
2. Inventory and Control of Software Assets.
3. Data Protection.
4. Secure Configuration of Enterprise Assets and Software.
5. Account Management.
6. Access Control Management.
7. Continuous Vulnerability Management.
8. Audit Log Management.
9. Email and Web Browser Protections.
10. Malware Defenses.
11. Data Recovery.
12. Network Infrastructure Management.
13. Network Monitoring and Defense.
14. Security Awareness and Skills Training.
15. Service Provider Management.

16. Application Software Security.
17. Incident Response.
18. Penetration Testing.

Each CIS Control contains the following four elements:

- **Overview**: Control description.
- **Why is this control critical?**: Control's important in blocking, mitigating, or identifying attacks plus how lacking the control helps attackers.
- **Procedures and tools**: Technical description of processes and technologies used to implement and automate the control.
- **Safeguard descriptions**: Specific actions to implement controls.

Conclusion

Understanding the legal landscape is often easier than choosing the right framework that enables regulatory compliance. Most often, an SMB's regulatory compliance requirements are based in geolocation or industry. A small retailer in California needs to comply with CCPA but not the NY DFS Cybersecurity Regulation.

However, knowing the cybersecurity framework that enables regulatory compliance is often more abstract. Many SMBs have a small IT staff, possibly one or two people. Even mid-sized organizations with five or ten IT employees may find themselves struggling to meet the increasingly burdensome compliance requirements and understand the best controls framework for their needs.

Unfortunately, no "one-size-fits-all" framework can make compliance easier. However, as an organization builds out its security and privacy programs, it needs to understand how its business plan and operational strategies fit into the overarching compliance landscape.

References

1. Britannica, Editors of Encyclopaedia. (2020, April 9). *Wildcat Bank*. https://www.britannica.com/topic/wildcat-bank#ref280697
2. Solove, D. J. (2006). A Brief History of Information Privacy Law. *The George Washing University Law School Scholarly Commons*. https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications

3. Öman, S. (2010). Implementing Data Protection in Law. *Scandinavian Studies in Law*: 390–403.
4. HIPAA Journal. (n.d.). *What Is the HITECH Act?* 1 October 2020. https://www.hipaajournal.com/what-is-the-hitech-act/
5. Compliancy Group. (n.d.). HIPAA Fines Listed by Year. https://compliancy-group.com/hipaa-fines-directory-year/
6. Walsh, K. (2018, April). What Are the Penalties for Violating HIPAA? https://reciprocitylabs.com/what-are-the-penalties-for-violating-hipaa/
7. Department of Health and Human Services. (n.d.). "HIPAA Security Series." *Department of Health and Human Services*. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf?language=es
8. Payment Card Industry Security Standards Council. (2018, May). "Payment Card Industry Data Security Standard." *PCI Security Standards Council*. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
9. European Parliament and the Council of the European Union. (2016). General data protection regulation. *Office Journal of the European Union*: 1–88.
10. Monteiro, A. (2019, January 3). First GDPR Fine in Portugal Issued against Hospital for Three Violations. https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/
11. *GDPR Enforcement Tracker*. (n.d.). https://www.enforcementtracker.com/?insights
12. New York State Department of Financial Services. (2020, July 21). "First American Notice Charges." *New York Department of Financial Services*. https://www.dfs.ny.gov/system/files/documents/2020/07/ea20200721_first_american_notice_charges.pdf
13. Walsh, K. (2019, March 7). CCPA vs. GDPR Compliance. https://reciprocitylabs.com/california-consumer-privacy-act-vs-gdpr/
14. "Privacy Act 1988." (n.d.). *Federal Register of Legislation*. https://www.legislation.gov.au/Details/C2020C00237
15. Saudi Arabian Monetary Authority. (2017, May). https://cdn2.hubspot.net/hubfs/3821596/SAMA%20Cyber%20Security%20Framework%201.0.pdf?t=1517406425028
16. Center for Internet Security. (2019, April 1). "CIS Controls." *Center for Internet Security*. https://www.cisecurity.org/controls/

3

Compliance Risk

In business and cybersecurity, risk often drives decision-making. Risk is generally defined as the probability that something will have a negative effect, like causing physical or emotional harm. Analyzing risk is the process of weighing the benefit of an activity against the potential cost that a negative outcome might inflict. In fact, people calculate risk all the time, often without realizing it. When someone drives a car somewhere, they make many small risk calculations. Consider some of these small risk analyses:

- **Driving over the speed limit**: Is it worth the negative outcome of a speeding ticket?
- **Speeding up at a yellow light**: Is it worth the possibility that the light will change before they pass through the intersection and cause an accident?
- **Tapping the breaks at an empty four-way stop intersection**: Is it worth the potential that a camera will capture the "not really a full stop" or that the car will hit a pedestrian?

Then, they compare the likelihood that the adverse outcome will occur. Some considerations for the risk analyses above include:

- **Driving over the speed limit**: This is a stretch of road that people know the local or state authorities often monitor, so the risk is *high*.
- **Speeding up at a yellow light**: The car is within ten feet of the intersection and the light is known to be a long yellow, so the risk is *moderate*.
- **Tapping the breaks at an empty four-way stop intersection:** The intersection is in the middle of a quiet, residential neighborhood, far away from main roads, so the risk is *low*.

DOI: 10.1201/9781003128588-3

Finally, people consider the cost of the adverse outcome. In all of these examples, the risk is quantifiable, meaning people can measure with numbers. Traffic tickets and accident costs can be measured in dollars and cents. A person can consider whether they have the money to pay for these costs.

- **Driving over the speed limit**: A speeding ticket costs $200 which is very expensive.
- **Speeding up at a yellow light**: An accident would probably be low impact because other cars are waiting for their red to turn green, so the cost might be $1,000 in repairs and no one would get seriously hurt costing $0.
- **Tapping the breaks at an empty four-way stop intersection**: Several children live in the neighborhood, and if one runs out into the street, hitting the child would cost thousands of dollars.

Taking the costs into account might change the level of risk. For example, someone with a lot of money might feel $200 is not a lot of money so even though the likelihood of a ticket is high, the cost of the ticket makes the act a low or moderate risk. Meanwhile, even though the chance of a child running into the street might be low the costs of hitting one is too high to make only tapping breaks lightly worthwhile.

Ultimately, risk is calculated across all of these factors, with an equation that looks like this:

$$\text{Risk} = \text{Likelihood of Event} \times \text{Impact of Event}$$

However, not all risk can be quantified. Risk calculations also need to take qualitative impact into account as well. For example:

- **Driving over the speed limit**: A speeding ticket might add to points on a driver's license.
- **Speeding up at a yellow light**: An accident might make people think a person is irresponsible.
- **Tapping the breaks at an empty four-way stop intersection**: Hitting a child would make the person feel guilty and cause the parents emotional harm.

These qualitative calculations are critical to decision-making because they do impact actions. For example, if a person is a local politician, like a mayor, then speeding through a yellow light and looking irresponsible could negatively impact the next election.

At all points during the risk assessment phase, people and organizations take context into account. On an individual level, much of that contextual analysis is subconscious or internalized. However, as part of the compliance process, organizations need to document their risk review processes to meet legal and industry standard requirements.

Cybersecurity risk analyses might be even more critical for SMBs than for enterprise organizations. SMBs have a different risk profile from enterprise cohorts. For example, an SMB and enterprise-level organization in the same industry collect the same type of sensitive data. Quantitatively, the enterprise organization stores, processes, and transmits more information because it has more customers. However, the enterprise also has a larger budget which means it has more access to cybersecurity resources, including staff, tools, and information about new security threats.

Taking context into account, cybersecurity may have a larger impact on SMBs because while they have less data, they also have fewer resources available to them. In 2019, the National Cybersecurity Alliance surveyed 1,008 SMBs, noting that 10% went out of business and an additional 25% filed for bankruptcy after a data breach.[1] Meanwhile, enterprise organizations often rebound from these events. For example, in a list of top ten data breaches for 2020, technology giant, Microsoft, was listed as the largest breach of the year.[2] However, Microsoft maintains its robust revenue posture.

Ultimately, for SMBs to remain financially solvent, they need to understand business risks and cybersecurity risks while applying a contextual analysis that includes their organization's ability to mitigate those risks.

What Are the Different Risks Associated with Cybersecurity and Privacy

The overarching term "data breach risks" includes multiple risk categories from both a business perspective and a technology perspective.

Thus, to mitigate risks, organizations need to define and understand them before seeking to address them.

Compliance Risk

Compliance risk is the potential for material losses arising from violating a regulatory or industry standard compliance requirement. When organizations fail to follow the standards set forth by these governing bodies, they may face fines or even, in severe cases, incarceration.

For example, under the Health Insurance Portability and Accountability Act (HIPAA), individuals can face anywhere from one year in jail if they have reasonable cause or no knowledge of the violation to ten years in jail if they obtained protected health information (PHI) for personal gain or with malicious intent.[3] While both of these scenarios might be extreme, they are also real risks that even small healthcare providers face.

Legal Risk

Legal risks apply to the money an organization spends on attorney services in response to a negligent act. In some cases, these costs include compliance risks. However, they also include expenses a company incurs when responding to a data breach. According to the 2020 NetDiligence "Cyber Claims Study 2020 Report" found that legal cost insurance claims for SMBs ranged from less than $500 to $5M for defending legal actions around a data breach. Additionally, the range of settlement costs associated with data breaches ranged from less than $1,000 to $6.8M.[4] Often, these costs include activities as follows:

- Notifying customers that their data was compromised.
- Paying credit monitoring costs for impacted customers.
- Hiring digital forensics firms.
- Paying for public relations professionals to engage in crisis management.

Legal costs and risk might be considered "soft" or hidden costs because data breach statistics often focus on costs considered directly related to

a data breach, like fines, ransom payments, and response or remediation costs. However, costs arising from legal risk can quickly add up, so SMBs need to include them in any risk assessment process.

Financial Risk

A broader category than the other two, financial risk is the total cost impact that the organization suffers in the aftermath of a data breach. Although legal and regulatory costs fall into this bucket, financial risk also includes tangential costs like purchasing new technologies to enhance security, reduced revenue when customers choose to purchase products or services elsewhere, or reduced investor interest.

While an organization may easily quantify compliance and legal risk, financial risk can be more challenging. For example, an organization may know that some customers will stop purchasing goods and services after a data breach but not how many. They may also recognize the impact a data breach has on getting investors but not how much of a reduction it will cause. These future "what if" scenarios can have dollars attached, but these costs are less well-defined than the others.

Reputation Risk

Of all the business risks associated with a data breach, none is more elusive than reputation. Reputation risk is the impact that an event has on the way others perceive a business as reliable or trustworthy. Annually, Salesforce releases a "State of the Connected Customer" report that provides some insight into what customers expect from businesses.

For example, in 2019, the "State of the Connected Customer" noted that of customers surveyed[5]:

- 84% are more loyal to companies with strong security controls.
- 46% feel they have lost control over their own data.
- 41% do not believe companies care about the security of their data.

Meanwhile, the 2020 "State of the Connected Customer" found that of customers surveyed[6]:

- 86% want more transparency over how companies use their data.
- 61% feel they have lost control over their own data.
- 47% of Generation Zs hold companies entirely responsible for the ethical use of technology even if it negatively impacts revenue.
- 46% of Millennials hold companies entirely responsible for the ethical use of technology even if it negatively impacts revenue.
- 37% of Generation Xers hold companies entirely responsible for the ethical use of technology even if it negatively impacts revenue.
- 35% of Baby Boomers hold companies entirely responsible for the ethical use of technology even if it negatively impacts revenue.

These two reports provide insight into how data security and privacy relate to reputation risk. In light of the spate of high-profile data breaches, people want more transparency around how companies use their data while more than half feel they have lost control over their information. Meanwhile, younger generations who are both technology adopters and growing into their roles as buyers increasingly hold companies accountable for ethical technology use.

Although the term "ethical use of technology" is vague, several customer engagement technologies that likely fall under the umbrella of the survey include artificial intelligence (AI) and machine learning (ML) to suggest products or services, corporate website analytics that monitor buyer engagement, and mobile applications that provide better purchase experiences. Many of these technologies require nonpublic personal information (NPI), including email addresses, user names, IP addresses, and cardholder data.

Ultimately, reputation risk remains far more qualitative than quantitative. Organizations can use analytics to predict a percentage of users likely to purchase goods or services elsewhere after a data breach. However, these numbers are far less reliable than compliance violation costs and far more reliant on subjective context.

The Risk Assessment Process

While understanding business risk types is the first step to mitigating risk, the risk assessment process is far from complete. Once a company identifies the risks, it needs to start incorporating its current security posture by taking an in-depth look at the data it manages and the technologies it incorporates.

Identify

The identification step may sound easy at first, but the modern IT stacks and data collections processes are complex which makes identification challenging.

Data First, organizations need to identify all the sensitive data they collect, transmit, and store. They need to consider customer, employee, and vendor NPI, including:

- Names.
- Birth dates.
- Home addresses.
- User login IDs.
- Passwords.
- Bank account/payment information.
- Email addresses.
- IP addresses.
- Healthcare data.

They also need to identify sensitive corporate information, which can include:

- Intellectual property, like patents and trade secrets.
- Corporate financial data.
- Merger and acquisition information.
- Supplier information.

At a minimum, organizations should know whether they manage these categories of sensitive information. Based on their industry, they

also need to consider whether they collect any other valuable data that cybercriminals can sell.

Locations After breaking out the sensitive data types, organizations need to know where they store, transmit, and process sensitive data. At a minimum, organizations should consider the following locations:

- **Networks**: Internal and public-facing.
- **Servers**: Hardware and cloud-based.
- **Devices**: Laptops, desktops, tablets, smartphones, modems, routers, and other network devices.
- **Applications**: Installed on devices and Software-as-a-Service (SaaS).
- **Cloud**: Private and public (AWS/Google/Azure).

Hypothetical Case While the list looks short, SMBs need to understand that documenting all of these locations can be overwhelming. For example, an SMB might have

- Fifty employees.
- Ten vendors.
- Fifty workstations.
- Two networks.
- One on-premise server.
- Twelve SaaS applications:
  - Video conferencing (Zoom/Skype).
  - Chat (Microsoft Teams/Slack).
  - Email.
  - Collaboration suite (Google Suite/O365).
  - [[Tab]]Payroll.
  - Human resources.
  - Customer relationship management system (Salesforce /Hubspot/Freshbooks).
  - Content management system (Wordpress/Drupal/ Squarespace).
  - Project management (Trello/Jira/Asana).

- Social media scheduler (Hootsuite/Buffer).
- Customer support ticketing (Zendesk/Freshdesk).
- Chatbot AI (Drift/Chatterbot).

Each user, network, device, storage location, and application poses a risk. Taking that into account, every SaaS application creates an access point that a cybercriminal can use to gain access to sensitive information.

Taking the analysis a step further, ten employees might be in sales. Assuming that each person can only connect to the organization's network from the physical office, no remote work, each person needs:

- A workstation that connects to the network.
- Network access that requires a user ID and password.
- Access to:
  - Video conferencing tool.
  - Chat tool.
  - Email.
  - Collaboration suite.
  - Payroll application.
  - Human resources application.
  - Customer relationship management system.

Each member of the sales team is a minimum of nine data risks. Across the ten employees, the organization can identify ninety unique data risks. Next, the organization needs to consider additional heightened risk factors, including excess access, administrative privileges, lack of encryption, or poor password hygiene.

In other words, even for a small organization with a limited application stack, identifying data security risks becomes challenging almost immediately.

Assess

When organizations assess risk, they take their data, device, user, network, and application inventory and then determine whether each poses a low, medium, or high risk.

For example, the organizations have to compare risk levels for the types of users, networks, or applications, as follows:

- Standard compared to administrative user access.
- On-premise servers compared to cloud storage locations.
- Installed compared to SaaS applications.
- Internal compared to external facing web resources.

For example, a standard user is generally a lower risk than an administrative user because they have fewer access privileges. An on-premise server that never connects to the public internet is a lower risk than a cloud storage location because no one outside the organization can access it and physical security might be easier to implement. Installed applications can be protected with an antivirus software while a SaaS application is a higher risk because misconfigurations give malicious actors can exploit misconfigurations.

The organization is primarily looking at the inherent, individual risks that users, devices, networks, and applications pose. Ultimately, this forms the baseline for the analysis phase.

Analyze

Finally, the organization analyzes its risk by incorporating business risk and context. Risk analysis takes the process of assessing risk and then applies the risk formula. Generally, organizations will create a scale for their risk. For example, the organization might set the following values:

- **1**: Low risk.
- **2**: Low-moderate risk.
- **3**: Moderate risk.
- **4**: Moderate-high risk.
- **5**: High risk.

As they work through context-based scenarios, they review the various likelihoods, costs, and impacts, assigning one of the risk values to each. Organizations then can create a Risk Matrix that might look something like this:

	LOW IMPACT	LOW-MODERATE IMPACT	MODERATE IMPACT	MODERATE-HIGH IMPACT	HIGH IMPACT
Low likelihood	1	2	3	4	*5*
Low-moderate likelihood	2	4	*6*	*8*	**10**
Moderate likelihood	3	*6*	**9**	**12**	*15*
Moderate-high likelihood	4	*8*	**12**	*16*	**20**
High likelihood	*5*	**10**	*15*	**20**	**25**

No Formatting -> No or Low Risk; Italicized -> Moderately Low Risk; Bold -> Moderate Risk; Underlined and Italicized -> Moderately High Risk; Underlined and Bold -> High Risk

While the math might be similar from one organization to another, the overall ranking of risk might differ. For example, while one organization might consider anything with a risk score of 3 a "low risk," another company might designate that as "low-moderate risk."

Applying Context At this stage, organizations may also be considering whether low-risk data or applications maintain their low-risk categorization. For example, the organization needs to consider the level of risk that user poses to the organization based on the type of data with which they interact. For example,

- A standard user in the customer service department might have access to customer names and email addresses.
- A standard user in the human resources department might have access to employees' names, physical addresses, birthdates, and financial account information.
- An administrative user might have access that lets them make changes to software or sensitive data.

Thus, while each of these users might create a data security risk, the level of risk changes based on the access they have and the type of data they can access. For example, an admin for the corporate website might not be accessing high-risk data or applications. However, if the website can be used as an entry point for a malicious actor to move laterally within the infrastructure, then the user's access is a high risk

to the organization. This might turn what was considered a low risk into something that is assessed as a medium or high risk.

Hypothetical Analysis When organizations engage in a risk analysis, they need to consider potential, real-life data breach scenarios.

One scenario might be that malicious actors compromise a standard user account for a customer service manager who can access customer names and email addresses. For the scenario, the following data impacts to different organizations:

- Event:
  - Standard user account exploited because of poor password hygiene.
- Costs:
  - **Moderate legal costs of $150,000**: notification, forensics, crisis management.
  - **Low compliance costs**: $15,000.
- Impact:
  - **Low-moderate reputation impact**: $20,000 revenue from customers leaving.
  - **Moderate financial impact**: $50,000 in new security technology and cybersecurity staff costs.

Organization A Organization A generates an annual revenue of $5 million, has two dedicated cybersecurity professionals on staff, feeds event logs into a single platform that enables a single source of documentation. The risk analysis for Organization A might look like this:

- **Event likelihood**: Low-Moderate 2.
  - **Estimated probability**: 30% chance Standard user account exploited because of poor password hygiene.
  - **Reasoning**: This likelihood is based on statistics around credential theft attacks, the number of access points, the security team size, and the maturity of the security tool stack.
- **Impact**: Moderate 3.

    - **Moderate legal costs**: $150,000 (notification, forensics, crisis management).
    - **Low compliance costs**: $30,000.
    - **Low-moderate**: $20,000 lost revenue from customers leaving, reputation impact.
    - **Moderate**: $40,000 in new security technology.
    - **Total estimated costs**: $240,000.
    - **Reasoning**: Total estimated costs are 4.8% of total revenue meaning this will have a moderate impact on the organization but not devastating.
- **Overall risk score:** Likelihood × Impact = 6 (Low-Moderate).

Organization B Organization B generates an annual revenue of $1 million, has a three-person IT team, relies on managed services for most cybersecurity monitoring, and manages documentation manually in spreadsheets. The risk analysis for Organization B might look like this:

- **Event likelihood**: Low-moderate 2.
    - **Estimated probability**: 30% chance Standard user account exploited because of poor password hygiene.
    - **Reasoning**: This likelihood is based on statistics around credential theft attacks, the number of access points, the security team size, and the maturity of the security tool stack.
- **Impact**: High: 5
    - **Moderate-high legal costs**: $150,000 (notification, forensics, crisis management).
    - **Low-moderate compliance costs**: $30,000.
    - **Moderate-high**: $20,000 lost revenue from customers leaving, reputation impact.
    - **Moderate-high**: $40,000 in new security technology based on a $500,000 IT budget, inclusive of staff.
    - **Total estimated costs**: $240,000.
    - **Reasoning**: Total estimated costs are 24% of total revenue meaning this will have a moderate impact on the organization but not devastating.
- **Risk = Likelihood × Impact = 10** (moderate).

This relationship between revenue, impact, and risk is the reason that context matters. Despite the exact same likelihood and cost, the scenario impacts the organizations differently because their annual revenue is different. Organization A generates five times *more* revenue than Organization B. Therefore, the Organization A's impact is five times *less* than Organization B. Another way of thinking about the impact is that Organization B earns five times *less* than Organization A, which makes the impact five times *greater*.

Driving Security Based on Risk Tolerance

After completing the risk analysis, organizations have a final step to take before putting security controls in place. They need to determine their risk tolerance. A company's risk tolerance is the amount of risk that it is willing to accept in order to achieve a goal.

For example, organizations want to create digital transformation strategies. Adopting new technologies increases risk, and all companies know this. However, companies need to decide how they plan to manage that risk.

A risk averse company will make conservative choices when adopting new technologies and business strategies. Often these traditionalist organizations wait to see how what happens to other companies that implement new strategies and technologies. These risk averse organizations value stability, ultimately wanting more proof that the benefits outweigh the potential costs.

Other organizations who are willing to accept more risk are often early technology or strategy adopters. These mavericks are the ones that the risk averse companies watch. Organizations with a higher tolerance for risk are the innovators who feel the potential value outweighs the potential risks over the longer term.

Every organization has a different level of risk acceptance and averseness, which is why there are four different actions organizations can take in response to risks.

Refusing Risk

When the risk a new technology poses to the organization far exceeds the potential benefit, organizations can choose to refuse the risk.

For the most part, risk refusal means not purchasing a technology or adopting a strategy.

For example, when organizations review technology vendors, they need to engage in due diligence. An organization may be looking for a new payroll services provider. Because the technology will handle employee and vendor financial information, a vendor newer to the market might appear to pose more risk than an established vendor. While the newer vendor may offer unique capabilities, the company might decide that the vendor's newness means it has less security information and history to share. Therefore, these new capabilities might not be enough to outweigh the unknown risks. Ultimately, the organization chooses the known vendor with an established history, refusing to accept the risk the newer technology creates.

Accepting Risk

On the other end of the spectrum, organizations might be willing to accept a risk because the benefits far outweigh the data breach risks. Despite knowing that the technology provider could lead to a data breach, the organization needs the service desperately.

An excellent example of accepting risk would be the story of Zoom during the early months of the COVID-19 pandemic stay-at-home orders. Zoom, a web-based video conferencing application, offered a free version of its software. With free accounts, users could hold conference calls lasting up to forty minutes. For anything longer, they needed to purchase a premium account. When schools rapidly moved to a remote model as a result of the COVID-19 pandemic, they needed a user-friendly way to meet with students. Many school systems chose Zoom because it was easy for people to use, even if they people lacking strong technology skills. However, Zoom had several security weaknesses that soon became a problem. In multiple cases, people "Zoom-bombed" classes by exploiting several security vulnerabilities, often engaging in hate crimes during class meetings.[7] In this case, school district IT departments, who normally engage in detailed vendor risk due diligence reviews, lacked the time to fully vet the services. Moreover, schools must comply with several different types of

privacy regulations because they need to protect children's privacy. However, the easy-to-use technology and free accounts made it easy for students, parents, and teachers to learn how to use the technology.

In other words, the school districts that moved online classes to Zoom were willing to accept the risks because the technology's benefits appeared to outweigh the potential impact to family and staff.

Transferring Risk

Transferring risk is one "middle-ground" approach organizations can take in response to identified risks. Cyber risk insurance is a primary method of transferring risk. Similar to car insurance, cyber risk policies set out a series of terms, conditions, coverages, and exclusions that allow an organization to transfer financial risks to the carrier. In the same way that people can make an insurance claim that will pay for damages arising from a car accident, businesses can make insurance claims under these policies for damages arising from a security incident.

Often, these policies cover costs to mitigate the impact of data breach, including business loss from downtime, property damage to devices, legal fees, forensic costs, crisis management services, and breach notification costs.

In recent years, insurance carriers are able to leverage more historic data so that they can better price policies. While increased numbers of data breaches create social and economic challenges, they also provide additional data points that insurance carriers can use to make cyber risk policies more affordable.

Mitigating Risk

Although last one this list, mitigation is the primary response to managing risk. More often than not, organizations choose to put security controls in place that mitigate the impact a data breach can have. These technical controls reduce vulnerabilities and limit exposure. Some primary risk mitigation controls are as follows:

- Data encryption.
- Firewall policies.

- Continuous controls monitoring automation.
- Identity Governance and Administration (IGA) technologies.
- Automated vulnerability scanners.
- Antivirus software.
- Installing software and firmware security updates.

By putting these security controls in place, organizations reduce the likelihood that a malicious actor will be successfully infiltrate systems, networks, and applications. Despite no single security control or solution fully protecting an organization, the more controls a company has in place, the stronger its security posture is.

Differentiating SMB and Enterprise Risk

While SMBs and enterprise organizations face the same malicious actors, their ability to mitigate or transfer risks differs. While an enterprise organization collects more data, incorporates more devices, and has more users, they also have larger IT budgets so they can afford best-in-class security technologies. Additionally, they often have entire teams dedicated to security, including people focused on looking for new vulnerabilities and teams focused on threat response.

Meanwhile, SMBs may be able to leverage managed service providers, companies that can provide Cybersecurity-as-a-Service (Caas). CaaS can be remote security operations centers, automated continuous monitoring platforms, or companies that managed device or application access controls. Additionally, more insurance companies offer cyber risk policies priced specifically for the SMB market.

Cyber attackers will always try to hook the "big whales" of enterprise data. However, they increasingly target SMBs because while an attack may net fewer pieces of data, it also requires less resources. Cyber criminals approach data breaches the same way businesses approach technology investments. Malicious actors want the best return on investment, which means that if it takes less time to infiltrate five SMBs compared to one enterprise organization, they make more money per data point in the long run.

Digital transformation and cloud services are the future of business. For SMBs to stay financially viable, they need to mature their security programs, enhance their risk mitigation programs, and document

their activities to prove governance so they can meet stringent compliance requirements.

References

1. *Small Business Cyber Target Survey Data*. (2019, October 23). Retrieved from Stay Safe Online: https://staysafeonline.org/small-business-target-survey-data/
2. Henriquez, M. (2020, December 4). *The Top 10 Data Breaches of* 2020. Retrieved from Security Magazine: https://www.securitymagazine.com/articles/94076-the-top-10-data-breaches-of-2020
3. *What Are the Penalties for HIPAA Violations?* (2021, January 21). Retrieved from HIPAA Journal: https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/
4. *Cyber Claims Study* 2020 *Report*. (2020). Retrieved from NetDiligence: https://netdiligence.com/wp-content/uploads/2020/11/NetD_2020_Claims_Study_1.1.pdf
5. *Winning Customer Loyalty Hinges on Data Privacy and Trust*. (2021, January 28). Retrieved from Salesforce: https://www.salesforce.com/blog/customer-loyalty-data-privacy-trust/
6. *State of the Connected Customer*. (2020). Retrieved from Salesforce: https://www.salesforce.com/resources/research-reports/state-of-the-connected-customer
7. *FBI Warns of Teleconferencing and Online Classroom Hijacking during COVID-19 Pandemic*. (2020, March 30). Retrieved from Federal Bureau of Investigation: https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

4

Looking at Risk through a Security Lens

Cybersecurity and privacy risk often seem overwhelming, especially to entrepreneurs running small and mid-size businesses (SMBs). If large enterprises fail to manage the plethora of laws and ever-changing nature of attacks, SMB owners with limited budgets often feel that they will never be able to respond appropriately. In reality, no organization—large or small—will ever fully prevent an attack. The best an organization can do is create a resilient, risk-focused mitigation program.

Some SMBs choose to outsource their cybersecurity activities to managed services providers (MSPs) or managed security services providers (MSSPs). Although this reduces staffing burdens, the companies still need to understand how to manage risk and what an attack on the MSSP means for them. According to a cybersecurity insurance market condition report from February 2021,[1] ransomware attacks frequently target MSSPs because it creates a supply chain attack giving them the ability to impact the entirety of the MSSP's client base.

For example, in 2021, a threat actor targeted Kaseya, a company providing technologies for MSPs, impacting an estimated 800–1,500 medium-sized business who contracted with MSPs using the cybersecurity technologies.[2] While contracting with an MSSP may make managing cybersecurity easier, it comes with its own set of security concerns. The SMB is no longer the sole party managing their security and privacy risk.

From the compliance and risk perspective, even companies who outsource their security activities maintain some semblance of responsibility. A look at the FFIEC IT Examination Handbook, the regulatory exam guide for financial services organizations provides some insight. For example, according to the *FFIEC IT Handbook*, a financial

DOI: 10.1201/9781003128588-4

services organization that outsources its security to an MSSP remains responsible for[3]

- Governance over understanding and managing data risks like reviewing procurement, operation, and service delivery costs, including Service Level Agreement (SLA) review.
- Due diligence review, including engaging in a risk assessment over the MSSP's security controls.
- Continuous oversight, including the MSSPs on-premises and cloud security posture.

Although this applies strictly to the heavily regulated financial services industry, the requirements apply equally across all industries as new laws and compliance requirements focus on maintaining supply stream security.

Ultimately, the final line of the *FFIEC IT Handbook* acts as a guiding principle for all SMBs, whether they manage their own security or outsource it, "As with all outsourcing arrangements FI management can outsource the daily responsibilities and expertise; however, they cannot outsource accountability."[3]

The Not Always Rosy Security Lens

While it might seem like SMBs are in a no-win situation, they are not alone. From the smallest online business to the largest enterprise, looking at risk through the lens of security appears dismal. Often, organizations become overwhelmed, much like a student with too much homework. It might seem easier to just throw hands up in the air and give up, leaving everything to chance.

In the alternative, SMBs in highly regulated industries might find themselves aligning all their security practices to the law or industry standard governing their business. For example, a small medical practice might assume that meeting the Health Insurance Portability and Accountability Act (HIPAA) requirements automatically assumes that they have secured sensitive information. A small online shop might assume that meeting the Payment Card Industry Data Security Standard (PCI DSS) compliance requirements protects them.

Unfortunately, this belief is a fundamental issue for all organizations. While meeting compliance mandates mitigates the risk of fines and penalties, the practice often fails to secure information.

Compliance Is Not Security

The problem with assuming that security and compliance are the same thing lies at the heart of what makes compliance a general burden. Whether the compliance standard comes from a law, regulatory agency, or industry standards organization, the bureaucratic red tape and long-tail timelines in issuing these mandates mean that they fail to stay relevant.

The Problem with Legislation as a Foundation

A look at the US processes for how bills become laws and regulatory agency requirements gives some insight into why many mandates fail when it comes to creating security despite setting out compliance requirements.

In the United States, a bill goes through nine different stages before becoming a law, including

- **Introduction**: When a member submits the bill to either House of Representatives (House) or Senate.
- **Committee action**: When the committee(s) that manage the bill's content review and research the bill, including holding hearings.
- **Floor action**: When the members of the House or Senate debate and vote on the bill.
- **Other chamber review**: If the nonvoting chamber has a similar bill, this step is skipped, otherwise the legislative body can debate and vote on the bill (if House voted first, Senate gets to vote and vice versa).
- **Conference committee**: When both chambers have similar bills, this committee reviews both to reach a compromise.
- **Conference report vote**: When the chambers vote on the combined, compromise bill.
- **Presidential review**: When the president reviews or vetoes the bill.

If Congress only had one law in front of it, this process would still be lengthy. However, Congress reviews multiple bills at the same time and has breaks between sessions. Further, according to the House of Representatives website, members of Congress actively work on legislation for, at most, 193 days per year.[4]

The Problem with Agency Regulations as a Foundation

Meanwhile, regulatory agencies also need to go through lengthy Notice and Comment period, not including the time it takes to research and develop the standard. For example, according to the National Institute of Standards and Technology (NIST), the NIST Cybersecurity Framework (CSF) took a year to generate.[5] According to the agency, the outline for the process of the first version of the CSF looked like this:

- Presidential Executive Order "Improving Critical Infrastructure Cybersecurity" on February 12, 2013.
- Request for information February 13, 2013–May 28, 2013.
- Five workshops with over 3,000 people across industry, academia, and government.
- Request for Notice and Comment from October 29, 2013 to December 13, 2013.
- Final issuance February 2014.

In other words, establishing the first round of the NIST CSF took the regulatory agency a year. Additionally, the first update to the NIST CSF, moving to version 1.1 took from the initial "Request for Information" on December 11, 2015, until final issuance on April 16, 2018.[6]

The long-tail timelines across these examples provide insight into the problems associated with relying on legislative bodies and regulatory agencies to define security practices. Cybercriminals continuously evolve their methodologies, trying to exploit changes in attack surfaces. For instance, according to one article, malicious actors responded to the changes the COVID-19 pandemic caused[7]:

- Phishing activities surged among streaming services.
- 54% of phishing sites used HTTPS, disguising themselves as legitimate websites.

- Trojans and malware as an attack methodology for Android devices increased from 92.2% in 2019 to 95.9% in 2020.

Ultimately, organizations that rely only on controls set forth in laws, regulatory requirements, and industry standards might reduce their compliance risk but they increase their data breach risk. A complete cybersecurity program must be flexible enough to respond to both the static nature of laws, regulations, and standards while also continuously evolve to respond to new security risks.

Continuous Risk Visibility for Continuously Changing World

Despite the need to meet compliance mandates, organizations need to focus their time on securing their environments and ecosystems rather than simply taking a "once and done" approach. As part of this process, they need to be continuously looking at security controls' effectiveness in preventing malicious actors from gaining unauthorized access to their systems, networks, and software.

To do this, they need to understand the risks malicious actors pose to data, then review their current controls. In addition, they need to stay informed about how threat actors change their approach to infiltrating environments and ecosystems.

Fundamentally, security is no longer about eliminating attacks. It is about limiting the impact an attack has on the organization's data, systems, networks, finances, and reputation. To limit impact, SMBs need to be aware of the changing threat landscape and constantly review for new risks.

The threat landscape combines the types of data, technologies, and resources an organization uses with the types of attack methodologies, malicious actors, and attack methodology changes seen in the real world. When security professionals discuss the "changing threat landscape," they mean that as organizations adopt different technologies and devices, malicious actors change the ways in which they seek to steal or access the organization's sensitive data. As the threat landscape changes, so does an organization's risk profile.

For example, if an organization only uses resources that reside in their building, with no connection to the public internet, physical

controls and network controls like firewalls can help protect sensitive data. Since a malicious actor would need to be in the building to steal a device or to connect to the network, the organization has little risk.

However, the move to cloud-based resources changes the threat landscape because it changes how users access information. If an organization allows connection to its internal network from the public internet, like using a Google Drive or OneDrive shared drive, then the organization opens itself up to more risk. All a malicious actor needs to deploy an attack is a motive, a device, and the internet.

In short, the need to monitor new threat methodologies and the risks new technologies pose, means that organizations need to ensure they take a continuous monitoring approach to their own IT stack as well as their third-party vendors' stack.

Converging Security and "Enterprise Risk Management"

Whether an organization is large or small, leadership understands the value of risk management. Organizational leaders engage in risk management practices daily, although many call it engaging in a "cost–benefit" analysis. By applying that mindset to security, the organization can create a stronger security-first approach to compliance.

Understanding Enterprise Risk Management (ERM)

Enterprise risk management (ERM) is the process of planning, organizing, leading, and controlling an organization's activities with the goal of minimizing a risk's impact to the company's financial security.[8] ERM includes plans for managing financial, strategic, and operational risks as well as risks arising from accidental losses. This short definition underplays the challenges and complexity of complete risk management.

Analyst Gartner defines ERM as[9]

> Enterprise risk management is identifying, analyzing and treating the exposures an organization faces as seen by the executive levels of management. This means looking at exposures in finance, credit, fraud, strategic and operational matters for the company. Most matters at the enterprise level only peripherally consider technological risk, and that's

> when they are looking at how technology increases or decreases those business exposures.

This definition notes that technology risk only matters to the extent that it increases or decreases the other types of business risk. However, in a world where nearly all business operations require technology, ERM now becomes intricately interwoven into the overall fabric of business risk.

ERM is similar to playing a sport, like soccer. Coaches need to consider the strengths and weaknesses of both their team and the opposing team. They need to consider how individual players contribute to the team's overall strength. They need to make sure that they put the strongest offensive players in the appropriate position. The qualities that make a good striker may not make a good midfielder. They need to do the same for their defense. Then, they need to focus on how the opposing team's lineup impacts their current lineup. For example, if the striker is small and fast but the opposing team's defense is large and slow, then the matchup works. However, if the opposing team's defense is large and fast, the coach might need to put a different player in as striker. In some cases, a passing game works best. In other cases, focusing on dribbling works better. In the end, the coach needs to consider all information that impacts the team's ability to win.

Cybersecurity is the same way. Creating ERM program requires leadership to have access to information, evaluate it, analyze risk, and then find risk mitigation strategies.

The Five Steps of ERM

ERM programs align with the company's risk tolerance and model. Thus, while several steps focus on the risk assessment itself, other steps require the organization to apply these to business operations and processes.

Define and Set Objectives and Goals

Every strategy requires a set of clear, measurable objectives. Organizations apply their ERM programs to everything from daily

operations to procurement processes, which is why they need to create appropriate objectives and goals from the beginning.

Best practices for defining and setting objectives and goals is to use the "SMART" process:

- **Specific**: Defined in ways that enable effective planning.
- **Measurable**: Tracked with metrics that prove value and progress.
- **Attainable**: Accomplished within a reasonable and articulated timeframe.
- **Relevant**: Aligned with overarching goals like revenue or roadmap.
- **Time-based**: Reviewed and reassessed by a specific date or within a specific timeframe.

For example, ERM for technology procurement might be

- **Specific**: The IT and Security Teams must engage in a due diligence review prior to purchasing a Software-as-a-Service (SaaS) application.
- **Measurable**: The due diligence report must incorporate a review of data security incidents occurring in the past eighteen months and include a service organization controls (SOC) report detailing current security posture.
- **Attainable**: The IT and Security Teams must provide the report to senior leadership within forty-five days.
- **Relevant**: The due diligence report should detail potential impact to core systems and networks.
- **Time-based**: The IT and Security Teams must engage in an annual review of the SaaS application to ensure continued due diligence.

Assess Risk

This step is where the organization engages in its overarching security risk assessment process. Ultimately, that requires the organization to

- Identify all assets and risks.
- Assess all risks.

- Analyze risk impact to the business.
- Determine whether to accept, transfer, mitigate, or refuse risk.
- Set controls that mitigate risk.

Create a Risk Response

The risk response overlaps with risk tolerance and setting controls. However, it should also include incident response (IR), business continuity, and disaster recovery planning.

Incident Response An organization's IR team and plan document how to manage security incidents. At the highest level, every IR plan should include

- **Preparation**: Determining high-risk and high-value digital assets.
- **Identification or detection**: Defining baselines against which abnormal activities are measured, setting alert rules, creating processes for investigations.
- **Containment**: Preventing additional damage with both short- and long-term responses.
- **Eradication**: Engaging in activities that remove attackers and restore systems.
- **Recovery**: Removing remnants of attack and testing systems.
- **Lessons learned**: Reviewing processes for strengths and weaknesses to prevent similar events.

Business Continuity Business continuity plans cover various disasters from natural to digital. Their goal is to ensure that the organization is able to function without interruption when a disaster strikes.

From a cybersecurity risk management perspective, the BC plan should consider core business activities and how to maintain availability of

- Information necessary to maintain operations.
- Systems necessary to continued core operations.
- Software required to prevent business service and customer service outages.
- Third-party services needed to ensure continued operations.

In order to reduce the impact of a digital disaster, like a ransomware attack or distributed denial of service (DDoS) attack, an SMB needs to understand the interdependencies between the product or service it provides and the technology it uses.

Part of business continuity is ensuring that the workforce can continue to function. However, more important than lost productivity is customer impact.

Disaster Recovery Disaster recovery focuses on how an organization can move from emergency operations to restoring full functionality. Most organizations, even SMBs, have plans for recovering from natural disasters. For example, a traditional plan might include having an agreement with another organization or a branch location in a different state that can act as an emergency operations location.

As part of a cyber disaster recovery plan, SMBs need to consider the following:

- **Data backup and recovery**: Three separate data backups, on two different media, with one off-site or in the cloud.
- **Responsible parties**: Ensuring that everyone who works on the recovery knows and can manage the activities.
- **Documentation**: Network configuration diagrams, data flows, processes for implementing recovery, and anything else necessary for recovering impacted data, systems, and networks.
- **Timeline**: Mapped out timelines in advance to reduce impact.

Set Controls

Organizations define technical and administrative risk mitigation controls as part of their risk assessment process. An ERM program applies the organization's risk tolerance at a macro level. While setting technical security controls reduces data incident impact, organizations need cross-functional, cross-departmental controls to mitigate risk.

For example, while the IT risk assessment might set controls like password requirements, an ERM might include mitigating controls

like providing password managers to all employees or limiting the ability to share passwords.

NIST Internal Report (NISTIR) 8286, "Integrating Cybersecurity and Enterprise Risk Management (ERM)" defines five types of controls[10]:

- **Preventative**: Reduce or eliminate specific instances of a vulnerability.
- **Deterrent**: Reduce the likelihood of a threat event by dissuading a threat actor.
- **Detective**: Provide warning of a successful or attempted threat event.
- **Corrective**: Reduce exposure by offsetting the impact of consequences after a risk event.
- **Compensating**: Apply one or more controls to adjust for a weakness in another control.

Translating these broad definitions into actions that align with the organization's objectives and goals can be difficult. Some examples might include

- **Preventative**: Employee cybersecurity awareness education.
- **Deterrent**: Adding a liability clause to a vendor SLA for any security incidents it causes.
- **Detective**: Providing tokens or requiring MFA.
- **Corrective**: Backup and recovery policies and procedures.
- **Compensating**: Separating conflicting job functions, like preventing the same person from managing vendor payments and setting up new vendor accounts.

Create an Appropriate Corporate Culture

Although this sounds easy, many companies fail at it. For SMBs, creating a culture that understands risk, especially cyber risk, means finding ways to communicate with all employees. Additionally, the business leadership needs to be involved in defining, communicating, educating, and practicing risk mitigation.

Cybersecurity awareness education can be done in different ways. Problematically, most organizations use training programs that, while

able to document compliance, fail to really teach people about cybersecurity. For example, every compliance mandate incorporates a security training requirement. The trainings often provide information about phishing risk and impact. However, phishing remains a primary problem facing organizations at every level. The videos and multiple-choice tests document passing scores, yet the human element remains a security problem.

In some ways, smaller organizations have an advantage when compared to enterprise-level companies. SMBs often have smaller teams for a stronger sense of community that makes it easier to create a culture of security and awareness. SMBs can engage in regular, informal conversations around new threats and focus on the type of cyberawareness that makes a difference. Team leaders can include cybersecurity as part of monthly meetings.

Understanding Integrated Risk Management (IRM)

Integrated Risk Management (IRM) can be considered the evolution of ERM. Gartner defines it as

> a set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks. …
>
> To understand the full scope of risk, organizations require a comprehensive view across all business units and risk and compliance functions, as well as key business partners, suppliers and outsourced entities. Developing this understanding requires risk and security leaders to address all six IRM attributes.[11]

Additionally, Gartner applies six attributes to IRM:

- **Strategy**: Use of a framework that includes iteration through governance and risk ownership.
- **Assessment**: Identifying, evaluating, and prioritizing risks.
- **Response**: Identifying and implementing risk mitigation strategies.
- **Communications and reporting**: Giving internal stakeholders the means to track risk response effectiveness.

- **Monitoring**: Establishing processes that track governance, accountability, policy compliance, and decisions.
- **Technology**: Design and implement an IRM solution.

How ERM and IRM Are Similar

Both ERM and IRM require organizations to

- Identify risk.
- Analyze risk.
- Respond to risk.
- Mitigate risk.
- Track metrics.

Both ERM and IRM start with the foundation of having a strategy that incorporates a risk assessment process. Fundamentally, a strong ERM program acts as the foundation for an IRM program. For an SMB to effectively mitigate business-level risks, it needs to understand how technology increases or decreases risk. However, it also needs to create key performance indicators that show how well or poorly it mitigates these risks. IRM starts with the same foundation.

Where IRM Differs from ERM

IRM builds on the ERM foundation, adding what appear to be additional requirements. IRM primarily formalizes many implied ERM requirements and then adds a level of technology on top of them.

Governance While ERM never specifies that organizations need to focus on governance, IRM spells this out quite clearly. IRM specifically requires organizations to prove that they know whether their risk mitigation strategies work or not. This governance requirement ultimately drives the other differentiators as well because they all work toward enhancing governance.

Governance is about holding an organization's leadership accountable for the way in which it reviews and manages risk. For many organizations, this includes

- Ensuring that leadership and/or Boards of Directors review risk regularly.
- Understand how changes impact risk.
- Document their review process.

By requiring governance, IRM places final responsibility on a company's leadership.

The Facebook Example Holding leadership accountable for security and privacy violations has become more important in the aftermath of the 2018 Federal Trade Commission (FTC) investigation into Facebook. The brief history of the FTC investigation is that social media company, Facebook, shared user information with data firm Cambridge Analytica which violated a 2012 FTC Settlement.[12]

A setting that supposedly enabled users to restrict data sharing to only their "friends" misrepresented how the information could be used by third-party developers. Users believed that by limiting how the platform could share their data that only applications and friends they approved would be able to access their information. However, if a user's "friend" approved a third-party application, then the application could access and collect the original user's data. In other words, if User A restricted data sharing to only User B and User B approved Application 1, then Application 1 was able to access User A's information as well.

Testifying during the trial was Mark Zuckerberg, Facebook's Founder, Chief Executive Officer, and Chairman of the Board of Directors. Zuckerberg notably testified, "I started Facebook, I run it, and I'm responsible for what happens here."[13] In a Dissenting Opinion opposing the FTC 2019 settlement, FTC Commissioner Rohit Chopra wrote

> officers and directors cannot avoid responsibility under these orders simply by burying their heads in the sand as their subordinates break the law. … It is especially critical in this investigation, which involved a firm that is tightly controlled by its founder, CEO, and Chairman, Mark Zuckerberg. Given the structure of his ownership and his special voting rights, it is hard to imagine that any of the core decisions at issue were made without his input.

> For repeat offender firms, regulators should consider seeking governance changes in addition to more traditional injunctive relief. This is because repeated lawbreaking is a sign that the governance structure has failed – either because leadership sanctioned profitable lawbreaking or because it failed to implement reasonable compliance controls.[13]

While the Facebook story focuses on privacy violations rather than security ones, the governance concerns exist in both areas. An organization's leadership is held responsible for making informed decisions around policies, processes, and procedures. When they fail to do this, they can be held responsible for the outcomes.

The dissenting opinion noted,

> In my view, it is appropriate to charge officers and directors personally when there is reason to believe that they have meaningfully participated in unlawful conduct, or negligently turned a blind eye toward their subordinates doing the same.[13]

Although none of Facebook's officers or directors were held liable for their willful or negligent actions, the need for leadership to effectively oversee privacy and security compliance is increasingly important. Thus, the move toward IRM which requires this level of oversight is increasingly being seen in new security and privacy laws.

Communications and Reporting

Another difference between IRM and ERM is the reporting requirement. Derived from the governance requirement, communications and reporting focus on tracking and measuring the risk response's effectiveness.

As a company looks to find an MSSP or other solution, communications and reporting become even more important. When a company outsources a capability, whether security or payment processing, it needs to assess whether the organization is following its contractual obligations. SMBs that keep their security functions in-house need to design reporting capabilities that track performance.

When considering the types of reporting, organizations need to consider whether they

- Give leadership the information necessary to make decisions.
- Incorporate meaningful metrics.

- Show historic data indicating improvement, stability, or deterioration.
- Can be easily understood by everyone.

Additionally, the reporting requirement often overlaps with audit requirements. SMBs who need to undergo audits, whether required by law or considered best practice, need to have the data that shows they follow their policies, processes, and procedures. Audits require documentation, including the communications and reports that are integral to the company's IRM program.

Monitoring and Technologies

Monitoring is a key component of communicating and reporting. SMBs need a way to show that their risk management program works. Thus, they need to monitor the program continuously. Although Gartner sets these out as separate functions, they are too intertwined to separate out.

Modern "monitoring" means continuously reviewing risk mitigation controls to ensure their continued effectiveness. However, it also means holding people responsible for maintaining this effectiveness. However, to hold people responsible and view metrics, organizations need technologies that help them. Too many business processes rely on connected technologies.

Example An SMB might decide to use Google Suite as its primary email, calendar, and file-sharing solution. The business also uses Slack as a chat tool. Meanwhile, the marketing department uses Asana as its task management system while sales uses Trello. To understand the different risks, the organization needs a way to assign responsibility and view risk. Doing this manually becomes overwhelming for the IT department, especially when the team is small.

This connectivity is the reason that the cybersecurity vendor market has exploded in the last five years. According to a 2021 report from Grand View Research, the global cybersecurity market size was valued at $167.13 billion in 2020, with an expected compound annual

growth rate (CAGR) of 10.9% by 2028.[14] In short, the risk monitoring requirement for IRM has created a successful industry.

As SMBs look for monitoring solutions and technologies that enable risk management, they need to consider

- **Value across multiple cybersecurity segments**: Collecting monitoring technologies that respond to individual security concerns becomes cost-prohibitive over the long term.
- **Cross-departmental and cross-functional enablement:** Any technology should be able to help manage risks across departments and company functions.
- **Readability**: Technology and business leaders need to get the information they need in a way they can consume meaningfully.
- **Ease of implementation and deployment**: Technologies that require deep technical skills can increase the costs.

Finding the Just-Right Risk Management Strategy

Both ERM and IRM have a place in an SMB's overall cybersecurity risk management strategy. SMBs face all the same security risks that enterprise organizations face, only they have different needs. Meanwhile, many need to manage security and maintain compliance, which makes it more challenging.

Many SMBs need to comply with multiple regulations or industry standards, leading to overlaps or even conflicting requirements. Then, they need to dig into the risk aspect. Since regulations remain outdated, the controls they suggest may not actually mitigate risk. To properly mitigate risk, the company might outsource certain technical functions using an MSSP. However, the SMB's leadership still needs to monitor, document, and report on the risk mitigation strategies because their audits require it. For many SMBs, the need to monitor, document, govern, and manage everything can feel overwhelming.

The Security-First Compliance Approach

Fundamentally, laws, regulations, and standards have a single goal. They act as the "stick" that forces organizations, under threat of

financial penalty, to focus on data security. Lacking the financial or other resources to provide a "carrot," or reward, for strong security, governments, agencies, and industry standards organizations can only rely on these sticks. As SMBs look to meet the sometimes divergent security needs and compliance requirements, focusing on security and risk gives them a way to get compliant more rapidly. By doing the hard work of security, organizations are both less likely to have compliance violations and better positioned to show that they are trying to comply.

One of the easiest ways for SMBs to cut through the chaos is to establish a security-first compliance program. Governance, risk, and compliance (GRC) practitioners use the term "security-first" to mean that an organization start by applying the most complete, up-to-date security controls possible, then reviews for any "compliance gaps." In other words, they put all the best-practice technical controls in place, map them to the compliance mandates, and then add any additional controls that the law, regulatory requirement, or industry standard says they should have.

To mitigate risk as much as possible, SMBs should start by ensuring that they focus on securing their systems, networks, and applications according to most recent best practices. Security-first compliance most often takes a risk-based approach to security that aligns with mission-critical compliance mandates. As the way SMBs engage in business operations changes, so does their security risk.

Continuously assessing cybersecurity risks and iterating security programs is the most efficient way to meet the fundamental goal underlying laws, regulations, and standards.

References

1. *The 2021 Cyber Insurance Market Continues to Harden*. (2021, February). Retrieved from Gallagher: https://www.ajg.com/us/news-and-insights/2021/jan/2021-cyber-insurance-market-report/
2. Osborne, C. (2021, July 23). Updated Kaseya Ransomware Attack FAQ: What We Know Now. ZDNET. https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/.
3. *FFIEC IT Examination Handbook InfoBase – Appendix D Managed Security Service Providers*. (2021). Retrieved from FFIEC: https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/appendix-d-managed-security-service-providers.aspx

4. 110th to *Current Congresses (*2007 *to Present) | US House of Representatives: History, Art & Archives*. (2021). Retrieved from History, Art, & Archives United States House of Representatives: https://history.house.gov/Institution/Session-Dates/110-Current/
5. *Questions and Answers*. (2021, May 18). Retrieved from NIST: https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics
6. *NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1*. (2019, April 25). Retrieved from National Institute of Standards and Technology: https://www.nist.gov/system/files/documents/2019/04/25/csf-roadmap-1.1-final-042519.pdf
7. *Cybercriminals Evolving Their Tactics to Exploit Collective Human Interest*. (2021, April 21). Retrieved from Help Net Security: https://www.helpnetsecurity.com/2021/04/26/cybercriminals-evolving-tactics/
8. Walsh, K. (2019, November 29). *Choosing Enterprise Risk Management Tools*. Retrieved from Zeguro: https://www.zeguro.com/blog/choosing-enterprise-risk-management-tools
9. *Definition of Enterprise Risk Management – Gartner Information Technology Glossary*. (2021). Retrieved from Gartner: https://www.gartner.com/en/information-technology/glossary/enterprise-risk-management
10. *Integrating Cybersecurity and Enterprise Risk Management (ERM)*. (2020, October). Retrieved from National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf
11. *Definition of Integrated Risk Management (IRM) – Gartner Information Technology Glossary*. (2021). Retrieved from Gartner: https://www.gartner.com/en/information-technology/glossary/integrated-risk-management-irm
12. Fiegerman, S. (2018, March 21). Mark Zuckerberg *Breaks His Silence* on Cambridge Analytica scandal. Retrieved from CNNMoney: https://money.cnn.com/2018/03/21/technology/mark-zuckerberg-cambridge-analytica-response/index.html?iid=EL
13. Chopra, R. (2019, July 24). *Dissenting Statement of Commissioner Rohit Chopra in re Facebook, Inc. Commission File No. 1823109*. Retrieved from FederalTradeCommission:https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_fa
14. *Cyber Security Market Trends & Growth Report, 2021–2028*. (2021, April). Retrieved from Grand View Research: https://www.grandviewresearch.com/industry-analysis/cyber-security-market
15. *The State of SMB Security* 2020. (2020, October 12). Retrieved from Connectwise: https://www.connectwise.com/globalassets/media/assets/ebook/the-state-of-smb-cybersecurity-2020.pdf

5
How to Set Controls

While laws and industry standards may use different language, they point to the same control categories. Further, the control categories align to zero-trust architectures. In other words, even though cloud adoption shifts the way companies need to view security, the protections themselves remain functionally the same.

A Brief Introduction to Zero Trust

In 2010, Forrester analyst John Kindervag published a report titled "No More Chewy Centers: Introducing the Zero Trust Model of Information Security."[1] The report explained that traditional approaches to network security no longer adequately responding to the emerging threat landscape. At the time, most organizations followed a "trust but verify" approach to security that "trusted" users and devices by default. Historically, this approach made sense. Most people could only access corporate resources if they were

- Located in a corporate-controlled building.
- Using a corporate-owned device.
- Connecting to a corporate network with an actual, physical wire.

Since people could only connect to a corporate network when located in a building that the company owned, the network was "the perimeter," or the technology that protected sensitive data. Firewalls allowing traffic into and out of the network acted as a barrier because there was only one access point to the network.

As organizations began adopting internally owned wireless networks, the network itself was no longer the perimeter, changing organizational IT's ability to "trust" users and devices. Even when

DOI: 10.1201/9781003128588-5

located in a company-owned office, people began accessing corporate resources using

- A corporate-owned device.
- Login ID.
- Password.

Organizations still used firewalls to limit incoming and outgoing traffic. However, anyone with the username and password could also access the corporate networks.

Corporate IT environments continued to evolve as technology changed. People could connect their personal smartphones to corporate networks. Employees could connect to corporate resources while traveling, using airport or hotel wireless networks. Each step away from the physical cord moved the perimeter further away from the corporate-owned office location.

With remote work and cloud-based technologies the norm, the network perimeter no longer really exists. Organizations continue to use firewalls to monitoring network traffic, but the real threats come from stolen credentials or malware-infected devices.

In response, organizations need a new security model that manages these different risks. The zero-trust architecture (ZTA) addresses these new threats and risks. With ZTA, security and IT teams "assume compromise," meaning that they treat every user as a threat actor and every device as infected. From here, they assume that their networks and systems already have malicious actors stealing information.

As with everything else in cybersecurity, organizations establishing standards discuss ZTA differently. To make things more confusing, cybersecurity technology vendors tend to oversimplify zero trust in their marketing materials, hinting that a single tool will respond to the complexity inherent in zero-trust strategies. Across the different standards and implementation guides, the most "reader friendly" is the Cybersecurity & Infrastructure Security Agency (CISA) Zero-Trust Maturity Model (ZTMM).[2] Released in June 2021, the predecisional draft defines the five pillars of zero trust as follows:

- **Identity and access**: Attribute or a set of attributes uniquely describing an agency user or entity.

- **Device/endpoint**: Hardware asset connecting to a network, including Internet of Things (IoT) devices, mobile phones, laptops, servers, and others.
- **Network**: Open communications medium for transporting messages, including internal networks, wireless networks, and the public internet.
- **Application workload**: Systems, computer programs, and services that execute on-premises or in a cloud environment.
- **Data**: Structured and unstructured digital information.

Organizations must implement controls across all five pillars as part of their zero-trust strategies. Maturity is not about how many pillars an organization manages. It focuses on how well-integrated the controls are across the pillars. The CISA ZTMM defines its maturity stages based on

- Visibility and analytics.
- Automation and orchestration.
- Governance capability.

Even an immature organization must have controls across all five pillars. An organization in the early stages of zero-trust implement might look like this:

- **Visibility and analytics**: Disconnected tools limit visibility into potential control gaps and mean that organization cannot correlate security data between pillars.
- **Automation and orchestration**: The organization manually sets and monitors controls across the disconnected tools, which creates human error risk and means that discovering problems takes longer.
- **Governance capability**: Internal teams need to collect documentation from each tool to manually compare and review data.

A mature implementation would look like this:

- **Visibility and analytics**: Well-integrated, deeply connected set of tools correlates security data across multiple pillars to show control overlaps and provide visibility into security gaps.

- **Automation and orchestration**: Integrated tools continuously monitor for changes that would impact security posture and automate changes across the IT environment to remediate issues.
- **Governance capability**: Audit documentation from all tools is stored in a central repository so that the organization can track remediation to adjust technical and administrative controls as quickly as possible.

As SMBs implement controls that enable compliance, they can start by focusing on the most important basic cyber hygiene controls across the five pillars. Once they have these controls in place, they can start to iterate their programs by adding automation that matures their posture.

The Types of Controls: What They Are and Why They Matter

Most SMBs leverage cloud-based technologies, especially Software-as-a-Service (SaaS) applications. As they start implementing controls that ultimately establish ZTA, they see overlaps between them.

Identity and Access Management

Compliance mandates and frameworks usually aggregate these controls under the term "managing access" or "access management." Setting access controls means thinking like a reporter and answering the questions:

- Who is accessing resources?
- What resources are they accessing?
- What can they do with the resources?
- When are they accessing resources?
- Why are they accessing resources?
- How are they accessing resources?

Organizations need to follow the principle of least privilege meaning that they must ensure the right person has only the right access to the right resource needed to complete their job function at the right time and for the right reason.

Most people have a basic understanding of access management. Personal Google Drives offer an excellent example. When using a Google Doc, people can

- **Set restrictions**: Anyone with a link versus access or only people with access can open the link.
- **Set privileges**: Owner, editor, comment, or view.

People can decide to limit who can access the resource by limiting access to only specified email addresses. Then, they can limit more precisely what the person can do with that access.

Looking at access management through a compliance lens means considering different types of unauthorized access.

Starting with the cybersecurity compliance lens, organizations need to prevent

- Malicious external actors from gaining unauthorized access networks, devices, applications, systems, and data.
- Malicious internal actors from using the access they have to engage in illegal behavior.
- Internal users from accidentally sharing sensitive information with people who should not have access to it.

When putting on the privacy glasses, organizations need to consider the security risks and the following:

- Too many internal users having access to resources that they do not need for their jobs.
- Internal users sharing data with one another when one party does not need to access sensitive information.

The subtle difference between these two is important. With security, the concern involves data leaving an organization's systems. With privacy, the data stays in the systems but not everyone who sees it should see it.

As the fundamental zero-trust pillar, setting access controls can be one of the most important security activities a company undertakes.

Unique Username Every user needs a unique username, just like every person has a unique social security number. The IT and security teams use the username for monitoring security and investigating incidents.

Strong Password Policy Today, people use passwords for nearly everything they do. Passwords really should be called passphrases. A strong password should

- Be a minimum of eight to ten characters.
- Include uppercase and lowercase letters.
- Include at least one special character.
- Unique to the application or login.

For a stronger password, people can create passphrases with

- Sentences.
- Spaces between words.

Multifactor Authentication (MFA) Authentication means that a company knows the person associated with a login is who they say they are.

MFA combines two or more of the following:

- Something someone knows, like a password.
- Something someone has, like a token or smartphone.
- Something someone is, like a fingerprint or face ID.

With MFA, a user needs more than a password to gain access to resources. The MFA technology sends a "challenge" question to the user, either through a text message or an authentication app. This process mitigates credential-based attack risks because malicious actors are less likely to have access to the device receiving the challenge question.

Role-Based Access Controls (RBAC) RBAC establishes the "access needed to complete a job function." With RBAC, companies typically create a "role" that's aligned to a job title or function, like accountant or financial department. Once assigned a role, the user has all the access everyone else with that role has.

Attribute-Based Access Controls (ABAC) With ABAC, organizations add more context to the role-based access by incorporating information the company knows about the user. Some examples of ABAC include

- Geographic location.
- IP address.
- Device type.
- Operating system.
- Time of day.

By adding this context, organizations can determine whether access is abnormal for that user or not.

Privileged Access Management (PAM) Privileged access means that the user or entity can make changes beyond just standard business activities. Some examples of users with privileged access include

- **Super user**: The most privileged access available with ability to change configurations for systems, networks, and applications, add users, remove users, and delete data.
- **Domain administrator**: Can add and remove users and set privileges for others.
- **Local administrator**: Can make changes to endpoints but not across the network.
- **Emergency access**: Temporary "break glass" access used to respond to a specific issue and granted for a limited amount of time.
- **Privileged business user**: Can update sensitive data in databases.

Historically, security professionals focused on privileged user management. Today, technology and code might have the same ability to change configurations. For example, when a user selects "automatically update" on a smartphone, they give the technology super user privileges because it can change the operating system without requiring manual input from a human.

The ultimate "pot of gold" at the end of the cyberattack rainbow is gaining privileged access to systems because then threat actors can do whatever they want, usually without being detected.

Privileged access management (PAM) best practices include

- Separating privileged and standard access for privileged users.
- Limiting the number of users with privileged access.

- Only providing privileged access to internal employees.
- Requiring MFA for privileged access.

Segregation/Separation of Duties (SoD) SoD controls typically mitigate insider threat risks. When two types of access can be used for covert purposes, the same person should not have both types of access.

Typically, SoD controls focus on accounting departments. People who can create new invoices in a payment system should not also be able to pay those invoices. If someone has both types of access, the person could create fake invoices that send money to a personal account and then make the payments to that account without anyone noticing the fraud.

Baseline Normal and Monitoring for Abnormal Organizations need visibility into what "normal" access looks like across all departments. When implementing IAM, they should set baselines so that they understand

- What resources users access the most.
- Time of day users usually access resources.
- Cyclical access patterns for different departments.

Baselines provide visibility into what typical access looks like. For example, at fiscal quarter end, the finance department may be uploading and downloading more sensitive information as it prepares reports. The IT and security teams need to know this so that they recognize this as "normal" for that team.

Once the company knows "normal," it can look for abnormal access that indicates a potential security incident, especially if the organization implemented ABAC. For example, if Jane typically accesses the corporate shared drive from her home in Atlanta, Georgia, USA, then a new login from Munich, Germany, twenty minutes after her most recent Atlanta access could be a cybercriminal.

Periodic Review Nearly every compliance mandate and framework require organizations to periodically review access. While not a technical control, many companies struggle with this because they use manual processes, and people find the task time-consuming. As

a result, responsible parties often scan the access list and sign-off without really thinking about it, a problem called "rubber stamping." When reviewing access, reviews should focus on finding

- People who changed jobs within the organization.
- Access that should have been revoked, such as emergency access that should have remained limited for a short time.
- People no longer working at the company.

Devices/Endpoints

Many companies struggle with device security because they lack control over all the devices accessing their networks and systems. In some cases, people use their personal devices to do their jobs. Sometimes, they need to give contractors network or resource access. Additionally, device security also includes difficult-to-manage devices like

- **Ephemeral devices**: Short-lived, code- or hardware-based devices like virtual machines and cloud instances.
- **Network devices**: Switches and routers.
- **Internet of Things (IoT) devices**: Printers, smart devices.
- **Mobile devices**: Tablets, smartphones.

Asset Identification and Catalog Most compliance mandates and frameworks require a risk assessment that includes an asset inventory. A company needs to know what it has to make sure that it implements security for everything.

The asset inventory should include

- Device make.
- Device model.
- Operating system/firmware and version.
- Owner/responsible party.
- Location/IP address.

Baseline Configurations Configuration baselines are the software, firmware, and operating system settings that an organization defines

as "most secure." Generally, these are the most recently updated code versions. For example, if the most recent version of a laptop operating system is OSv10, then that would be the most secure.

Organizations use these baselines so that they know which devices are running outdated code versions that have vulnerabilities cybercriminals can use. For example, if OSv10 has a vulnerability that a malicious actor can use as part of an attack, then it is no longer the most secure configuration.

Antivirus Software Antivirus software blocks malware that can infect devices and spread across networks. Modern antivirus can be a software downloaded to a device, called agent-based, or agentless, meaning nothing gets installed on the device.

Most antivirus software know the types of malware code—known as signatures—already seen in attacks. Some use artificial intelligence to predict new variants. Antivirus tools update their databases with the latest threat information.

Vulnerability Scanning A network scan is really a device security control, even though it sounds like a network security tool. Network scanners provide information about all the devices connected to a company's network, documenting versions of

- **Operating systems**: Code communicating between hardware and software or device user interface, like Windows or MacOS.
- **Firmware**: Code ensuring smaller devices work as intended.
- **Software/application**: Code executing tasks on a device, like Outlook or Apple Mail.

Patch/Vulnerability Management Program When an IT team updates code to a newer version, it applies a "patch." The patch management process includes

- Discovering vulnerabilities in code that malicious actors can use.
- Assessing the risk the vulnerability poses.
- Reporting on the number of vulnerabilities detected.

- Remediating the vulnerability by installing a security update.
- Validating that all updates were successful.

Patching cadence, or how quickly an IT team installs a patch, is one of the primary security metrics that organizations track. Organizations should apply security patches within thirty to sixty days.

Network

In zero-trust architectures, network security is the first place that organizations see the integrated nature of overlapping controls. When IT professionals use the term "architecture," they mean the overall design of a system, including the relationships between components like

- Hardware.
- Software.
- Access.
- Protocols.
- Data flows.

Networks are the "digital highway" that data travels across, so companies need to make sure that they build the right on-ramps, exits, and bridges into their security plan.

Network Segmentation Network segmentation creates separate zones called subnetworks. The process can be physical isolation, meaning that the smaller networks never talk to each other because they have their own dedicated devices. Logical separation uses firewalls and virtual private networks (VPN) that control traffic.

Typically, organizations place sensitive information on one or more subnetworks, keeping it separate from other information. For example, a database with personally identifiable information might be on one subnetwork that never connects to the public internet.

Network segmentation mitigates cybersecurity and privacy risks because the network containing sensitive information has more protection. Instead of being able to cross from one subnetwork to another, a process called lateral movement, they hit a dead end.

Network Access Controls When setting network access controls, companies should

- Require MFA for all users.
- Incorporate ABAC.
- Set device security requirements.

Once organizations segment their networks, they can start to build out the technical controls that mitigate risk and enable ZTA. The network access controls show the first real "overlap" across the ZTA pillars because organizations need to ensure

- People are who they say they are.
- People are only accessing the information they need for their jobs.
- Devices are free from malware.
- Devices have updated operating systems and firmware to prevent attackers from using them.

Firewall Policies Firewalls enable network security in two ways. First, they allow or deny traffic into or out of a network which enables logical network segmentation. Second, they can be used to detect abnormal data downloads that indicate an attack.

All modern firewalls include packet inspection. Since files traveling across a network are large, the data gets broken up into smaller chunks called packets. Each packet can take the fastest route from the sender to the recipient. Packet switches recognize the packets that belong together to make sure that all the information gets where it needs to go, then the packets get pieced back together when they get to the recipient.

When firewalls inspect packets, they ensure that the final file is in its original secure form and that malicious actors never made changes to it. Firewalls that use packet inspection ensure that all these small bits, once put back together as a complete file, are secure. Deep packet inspection looks at the content within the individual packets to ensure that all the individual tiny bits are secure.

Most organizations use next-generation firewalls (NGFW) that provide intrusion protection, virtual private networks (VPN), antivirus, and encrypted traffic inspection.

Access Control Lists (ACLs) ACLs control what users, processes, or operations have access to a system objects, like directories, or file access. At a simplistic level, they combine the permissions from access management and the packet filtering from firewalls. With ACLs, the best practice is to deny all by default, and then add access back on a case-by-case basis.

For example, an IT team might deny all incoming network access to a laptop by default. Then, it would choose to write an ACL that specifies Windows and Word can have access. Simultaneously, since users do not need Windows Note App to do their jobs, the IT team would not write an ACL specifying that this application could have internet access.

Since Windows and Word can still connect to the internet, malicious actors could still use them to gain entry as part of an attack. Meanwhile, since Windows Note App is not able to connect to the internet, they cannot use that application as part of their attack. By setting the ACLs, the organization reduces the number of applications connecting to the internet, ultimately reducing the number of potential attack points.

Network Encryption (Data-in-Transit) Encryption scrambles data making it unreadable and unusable unless someone has the decryption key. Encrypting traffic protects data in-transit. For example, a VPN creates an encrypted connection so that even if attackers try to intercept data, the information will be meaningless unless they also stole the VPN's decryption key.

Application

The application layer includes software downloaded to a device- and cloud-based technologies. Again, as an organization implements controls across the ZTA pillars, many begin to overlap.

Least Privileged Access For cloud-based workspaces and applications, access controls are the first line of defense. Organizations need to ensure that they

- Use RBAC.

- Implement ABAC.
- Require MFA.

As an organization matures its security posture, it may also want to include step-up authentication. With step-up authentication, users need to reauthenticate as they move between resources. For example, someone might authenticate into a payment portal to view a vendor invoice, but they need to reauthenticate to complete the payment process.

Conditional Access Conditional access is the process of combining ABAC, device security, and application risk level to control how people access resources. Using conditional access policies enables security teams to protect data inside applications with policies that focus on when to allow, block, or limit access. In some cases, organizations may want to require additional user verification steps before providing access to an application.

Subnetworks/Network Segmentation Placing applications that contain or process sensitive data on a separate subnetwork prevents attackers from moving laterally across the network. Attackers exploit vulnerabilities in or steal credentials for low-risk assets so that they can move between applications. By placing all high-risk applications on the same network segment, organizations can implement additional controls and focus monitoring on these assets.

API Security An application programming interface (API) is the code that allows applications to talk to each other, including sharing sensitive information between applications. Fundamentally, an API acts like a bridge that information uses to travel from one application to another.

API security includes

- API identification.
- Authorization and authentication configurations.
- Encryption of data-at-rest and in-transit.
- Rate limiting.
- Web application firewalls (WAF).

Data

Data security is the final zero-trust architecture pillar. Many of the controls used across the other five pillars work together to secure data. However, a few additional security activities can help mitigate risk.

Data Governance Strategy Even SMBs want to become data-driven organizations, leveraging technologies like business analytics. To secure this vast quantity of data, organizations need to implement data governance strategies. Fundamentally, this strategy provides a "two for one" value since it enables a company to clean up its data, by ensuring data accuracy and reducing redundancy. Additionally, by implementing a data governance strategy, organizations can identify and tag sensitive information to ensure that they protect it effectively.

Data Encryption Organizations should encrypt three types of data:

- **Data-at-rest**: Data stored on servers or in repositories.
- **Data-in-transit**: Data traveling across networks.
- **Data-in-use**: Data being updated, processed, erased, accessed, or read by a system.

Encrypting data as part of network security protects data-in-transit. Encrypting data stored on a device or in a database as part of device security protects data-at-rest.

Some examples of data-in-use include

- Documents or files currently open.
- Random access memory (RAM) data.

The biggest problem companies face is that encryption makes data unusable, which is why users need to decrypt it so that they can edit documents or files.

End-to-End Encryption (E2EE) A secure communication method, E2EE encrypts data on a sender's system or device and only decrypts it when the intended person receives it. This process ensures that it remains encrypted from the time a user creates the data, providing data-at-rest encryption, through the entire transmission process, data-in-transit encryption.

Zero-Trust Architecture: Move toward Maturity

For a large enterprise, zero-trust architectures are challenging. SMBs will struggle even more because they have limited resources. However, the more cloud technologies an organization uses, the more its attack surface expands.

For SMBs, the primary takeaway lesson about zero-trust architectures should be that no single technology will provide everything the company needs. Making business and cybersecurity technology purchasing decisions should be done thoughtfully. Companies should focus on the data and users that pose the greatest security risks, then work purposefully to secure the devices, resources, applications, and networks that store this high-risk data and that the high-risk users access the most.

References

1. Kindervag, J. (2010, September 17). No More Chewy Centers: Introducing the Zero Trust Model of Information Security. Retrieved November 3, 2022, from Palo Alto Networks: https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf
2. Cybersecurity and Infrastructure Security Agency Cybersecurity Division. (2021, June). *Zero Trust Maturity Model*. Retrieved November 3, 2022, from Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

6

Continuous Monitoring

Introduction

Cybersecurity and privacy compliance is a special beast. Traditionally, people approach compliance as something they need to do once a year, a series of boxes they check off. Some types of audits remain effective as point-in-time reviews. For example, operational audits review a department's processes, procedures, and systems for effectiveness, efficiency, and productivity. Although the day-to-day activities may have variations, a point-in-time review gives the company insight into the department's performance.

In IT, this point-in-time approach is long outdated. From a privacy and security perspective, everything is always changing. Cloud technologies give organizations speed and agility. However, attackers can weaponize these benefits. Each new application or cloud resource creates a new, potentially usable attack point. In response, many laws and frameworks incorporate a continuous monitoring requirement.

Every attack uses a combination of tactics, techniques, and procedures (TTPs). These activities are the building blocks of threat actor behaviors. Just like building blocks, attackers can change the order and activity to change how they engage in an attack.

Tactics describe what an attacker did at a very high level. Some examples of tactics include[1]

- Reconnaissance.
- Initial access.
- Persistence.
- Privilege escalation.
- Defense evasion.
- Lateral movement.
- Exfiltration.

DOI: 10.1201/9781003128588-6

Techniques provide more detailed information about how an attacker behaved within the context of that tactic. For example, a technique used for reconnaissance might be[1]

- Active scanning.
- Gathering victim identity information.
- Phishing for information.
- Searching open websites/domains.

Procedures are the technical information about how an attacker implemented a technique. For example, a threat actor engaging in active scanning might engage in[1]

- **Scanning IP blocks**: Looking at a set of IP addresses connected to the organization.
- **Vulnerability scanning**: Looking at a network to try and find devices with vulnerabilities.
- **Wordlist scanning**: Looking at a company's content and infrastructure for common files extensions or software names.

When security professionals say that attackers continuously evolve their methodologies, they really mean that threat actors keep reordering the different blocks so that they can easily create something that works differently. Continuous monitoring requirements respond to these attacker activities and work to ensure that companies look for these new methodologies.

Why Continuous Monitoring Matters

For every security protection a company implements, attackers will look to find a loophole. Threat actors treat cybersecurity the way teenagers treat their curfews. A teenager may use the house's backdoor to sneak in after curfew, hoping not to get caught. Attackers do the same thing to IT systems. In fact, cybersecurity professionals use the term "backdoor" to describe any method that attackers use to circumvent security measures.

Every time an organization implements a new security protection, threat actors look for a new way to get around it. When parents lock the home's backdoor, teens might try to enter through a garage or basement, instead. Similarly, attackers keep changing their TTPs.

For example, many companies use multifactor authentication (MFA) to validate that the person trying to access an account is who they say they are. The additional challenge is usually sent to the person's device using email or SMS/text. In 2022, attackers started using MFA fatigue attacks to get around the security protection. As part of a brute force attack, they attempt to use stolen credentials to log into an account. Then, they use code that sends an overwhelming number of prompts to the account owner's device. Overwhelmed and distracted, the account owner approves the access to stop receiving the notifications.[2]

To prevent attackers from bypassing security protections, organizations need to look for potential issues all the time.

Defining Continuous Monitoring

Continuous monitoring means that organizations need to engage in real-time review of their security controls, ensuring that they remain effective.

The National Institute of Standards and Technology (NIST) outlines the following characteristics of continuous monitoring[3]:

- Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk decisions.
- Using automated procedures to keep malicious actors from circumventing security controls.
- Using automated tools to track suspicious actions.
- Noting that continuous and ongoing focus on assessing and analyzing at a frequency that supports risk-based decisions.

The good news is that the official definition of continuous may not mean every second of every day. The bad news is that unless a company is looking for problems regularly throughout the day, they could miss something.

Building the Cybersecurity Technology Stack

In a modernized, cloud inclusive environment, IT teams can no longer manage security manually. To protect their environments, most

companies adopt cybersecurity technologies that automate both the continuous monitoring and compliance reporting capabilities. Some organizations choose to purchase and deploy technologies themselves while others look for service providers who can manage the work for them.

Regardless of cybersecurity technology stack implementation, all companies need to know the fundamental tools for monitoring their environments and understand the different capabilities. Knowing the different technology types and terminologies enables SMBs to make informed purchasing decisions.

Cybersecurity technology vendors come in different flavors. As an organization plans its security technology stack, it needs to understand how it wants to build the infrastructure.

Technologies tend to fall into two categories:

- **Platform**: Aggregates multiple solutions and enables monitoring from a single console.
- **Point solution**: Solves a specific problem and may be integrated into a platform.

Every organization has a different IT technology stack, risk tolerance, and budget. Every company needs to make a cybersecurity monitoring and reporting decision that works within those constraints. Fundamentally, no "right" answer exists which can be frustrating. Some companies choose to outsource their security functions to service providers while others purchase their own security technology stacks. In either case, organizations need to understand the technologies that create a layered approach to data protection.

By understanding the different types of technologies and deployments, SMBs can make informed decisions that enable them to achieve their desired security, privacy, and compliance goals.

Platforms

A cybersecurity platform typically offers a holistic view within a "single pane of glass" so that IT or security teams have visibility into their environments and controls.

Over the last few years, the terms "cybersecurity mesh" and "cybersecurity mesh architecture" have entered the vendor vernacular. Analyst Gartner defines a cybersecurity mesh as[4]

> a collaborative ecosystem of tools and controls to secure a modern, distributed enterprise. It builds on a strategy of integrating composable, distributed security tools by centralizing the data and control plane to achieve more effective collaboration between tools. Outcomes include enhanced capabilities for detection, more efficient responses, consistent policy, posture and playbook management, and more adaptive and granular access control — all of which lead to better security.

The shortest definition of a cybersecurity mesh or platform is really a single technology monitoring activities across the various zero-trust architecture pillars with alert, response, and reporting capabilities.

Typically, SMBs contract with managed services providers (MSPs) or managed security services providers (MSSPs) who provide both the platform as their product and monitoring as their service. The MSP or MSSP purchases the security technology stack and hires security analysts who engage in monitoring, detection, investigation, and response. By distributing these costs across their customers, the MSP or MSSP business model reduces the amount of money that SMBs need to spend while providing the cybersecurity staffing and technologies needed to protect their environments.

While platforms, MSPs and MSSPs provide value, their customers often face challenges. As threat actors seek to maximize disruption with supply chain attacks, they may target these technologies or service providers.

Point Solutions

Point solutions are technologies that solve a specific cybersecurity problem. Some organizations may choose to invest in their own cybersecurity technology stack, so they need to look for tools that help them monitor their environments and manage their risks.

Since point solutions focus on a single issue, they are often less complex, meaning that they can be easily integrated into the company's environment. A good example of a point solution would be a

multifactor authentication tool. Since it specializes on sending challenge requests upon login, companies can easily integrate and deploy it across their users.

As companies grow, they often end up collecting different point solutions over time. These companies may struggle with monitoring and visibility if they have no single location for aggregating, correlating, and analyzing the alerts from the various point products.

Identity and Access

Managing identity and access is critical to any zero-trust architecture, meaning that organizations need to understand the various technologies that they can use.

Identity and Access Management (IAM) vs Identity Governance and Administration (IGA)

Although people often use these two terms interchangeably, they have a few differences.

An IAM tool enables a company to

- Manage digital identities and user access.
- Implement and maintain policies, programs, and technologies that reduce identity-related access risks.
- Focus on appropriate access and authorization.

An IGA tool incorporates similar capabilities but often includes additional functionalities by

- Managing the identity lifecycle including provisioning, self-service access requests, joiner/mover/leaver access, and deprovisioning.
- Acting as a framework and set of security solution to automate creation, management, and certification.
- Providing a policy-based centralised location of the organization of user identity management and access controls.

While an IAM tool provides a way to limit access, an IGA tool often provides a broader set of compliance and policy capabilities. The key

difference between these two technologies is that an organization uses an IGA tool as its identity system of record, aggregating everything from onboarding new users to terminating access in a single place. An IAM solution may connect with this identity system of record to control and limit access, but it does not enable the onboarding and termination.

Federated Identity Management (FIM) versus Single Sign-On (SSO)

Creating a unique password for each application can be overwhelming for many people. FIM and SSO help reduce this risk, but they do it in different ways.

An FIM acts as a hub that

- Acts as a single point of access across applications.
- Applies the same security standards and protocols across multiple applications.

An SSO enables users to

- Use a single login ID across multiple applications and services.
- Leverage one application as the way to authenticate into other applications.

If a company uses FIM, people will log into a portal and then see all their connected applications as "buttons" that they can click on. Meanwhile, if a company uses SSO, people will log into an application and then that username follows them whenever they go to the login pages for other applications. A good example of SSO is using a Google account to authenticate into a non-Google application, like a customer relationship management tool.

Passwordless

A newer technology in this space, passwordless tools leverage a device's built-in biometric capabilities to authenticate users. For example, smartphones provide either facial or fingerprint recognition capabilities. A passwordless technology ties this "something a person owns"

to the "something a person is" by sending a challenge question to the device. Passwordless technologies come in three varieties:

- **"Magic link"**: Requests a user's email then provides access by forwarding a time-sensitive link to the email
- **One-time password (OTP)**: Requests a user's email then provides access by forwarding a time-sensitive password to that email
- **Application**: Registers a user and device to become the point-of-contact for logging into a service

Privileged Access Management (PAM)

Some IAM and IGA tools manage privileged access. However, they may not always handle the full complexity of PAM. Some vendors provide tools that specialize in PAM, providing capabilities for

- Discovery across multiple systems, cloud infrastructures, and applications.
- Managing privileged account credentials.
- Delegating privileged account access.
- Establishing, managing, monitoring, and recording privileged sessions.
- Controlling elevation of commands.
- Managing secrets for applications, services, and devices.
- Providing privileged task automation (PTA).
- Remotely managing privileged access for workforce and external users.

Endpoint Security

With remote and hybrid workforces, device security is more important than ever before. Companies need to ensure that all devices, including tablets or smartphones, that connect to resources comply with their security standards.

Endpoint Detection and Response (EDR) versus Endpoint Protection Platform (EPP)

As companies moved to the cloud, traditional antivirus software was no longer enough protection. In response, EDR an EPP came into being.

EDR solutions focus on containment and response capabilities by

- Using analytics to detect suspicious behavior.
- Providing contextual information.
- Blocking malicious activities.
- Guiding remediation actions.

EPP solutions look for known and unknown threats by

- Monitoring for file-based and fileless malware.
- Using behavioral analytics that incorporate device activity, application, and user data.
- Guiding remediation activities.

The main difference between the two technologies is that EDR is a postinfection and response technology while EPP provides a proactive monitoring capability to mitigate risks arising from zero-day exploits.

Enterprise Mobility Management (EMM) versus Unified Endpoint Management (UEM)

While EMM and UEM have overlaps between their capabilities, they also have distinct differences.

An EMM tool is specific to mobile device operating systems, helping to mitigate smartphone and tablet security risks with

- Mobile app management.
- Mobile content management.
- Controlling access to and activities of applications (app wrapping).
- Isolating applications or services (containerization).

A UEM tool more broadly applies to computers, mobile devices, and Internet of Things (IoT) devices, integrating with identity, security, and remote-access tools that incorporate analytics like

- Identities.
- Apps.
- Connectivity.
- Device configurations.

Mobile Threat Defense (MTD)

As more people use mobile devices to do their jobs, threat actors find new ways to target these devices. MTD responds to these threats and supplements other mobile device security technologies by incorporating the following capabilities[5]:

- **Security management**: Devices vulnerability management, alerting, app vetting.
- **Prevention**: App vetting, signature- and analytics-based preventions, exploit prevention, preexecution behavioral analytics, app control.
- **Detection**: App control, behavioral anomaly detection.
- **Response**: Quarantining, rollback, remote wipe, sink holing.

Network Security

At the network layer, organizations need tools that help them monitor and control data access, use, and download.

Data Loss Prevention (DLP)

DLP tools can be bundled into other technologies or purchased as a standalone point product. They inspect content and track activities to prevent the loss or misuse of sensitive data from both authorized and unauthorized users.

Typically, a DLP tool

- Classified information contained in a file, email, packet application, or data store.
- Monitors data at-rest, in-use, or in-transit across storage, operation, and network.
- Dynamically applies security policies.
- Applies data rights management protections.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Although IDS and IPS tend to be aggregated into a single solution, they do provide some distinct capabilities, so understanding the

differences makes it easier to determine whether a vendor provides everything the organization needs.

An IDS tool

- Examines network traffic.
- Integrates with other security tools for overall data collection/reporting.
- Analyzes incoming network traffic.
- Monitors operating system files.
- Monitors for patterns associated with known attack types and unusual behavior to detect unknown attacks.

An IPS tool

- Examines network traffic.
- Identifies suspicious activity.
- Uses defined rules to respond to a threat.
- Analyzes protocol activity across networks, including wireless networks.
- Tracks and analyzes events on a network host.
- Analyzes network behavior for strange network flows that indicate a threat, like a DDoS attack or malware.
- Monitors packets to detect known attack types.
- Looks for abnormal patterns that indicate unknown attacks.
- Identifies abnormalities by comparing events with profiles of normal activities (stateful protocol).

Software Defined Wide Area Network (SD-WAN) Versus Secure Access Service Edge (SASE)

SD-WAN and SASE both secure remote work, but they manage networking differently.

An SD-WAN is an overlay network that connects branch offices to data centers by

- Routing traffic according to an organization's policies.
- Requiring users to go to a data center than to a resource.
- Making security decisions at the branch or headquarters.
- Requiring a third-party technology for remote access.

A SASE combines security and networking that with

- Global distribution to connect all remote users.
- Cloud-based platform with a subscription "as-a-Service" model.
- Direct endpoint connection eliminating the need for users to connect to a data center first.
- Cloud-based firewalls.
- Built-in remote access.

From a business perspective, SASE offers faster connectivity speeds for enhanced productivity. An SD-WAN sits on top of the current network architecture while a SASE builds in analytics that create the fastest routes.

Zero-Trust Network Access (ZTNA)

ZTNA wraps a SASE around a set of applications, creating additional boundaries between low-risk and high-risk applications. A ZTNA reduces the attack surface by

- Creating additional identity- and context-based requirements before providing access.
- Hiding applications from the public internet.
- Preventing lateral movement across the network.

Data Privacy and Security

At its core, cybersecurity is really data security. While technologies can manage access or prevent theft, organization still need protections at the data layer. They need to know what they have, how to protect confidentiality and privacy, and how to restore it.

Data Classification and Data Governance

Traditionally, companies manually classified their sensitive data because they were able to control where it was. However, as more companies use data lakes and business intelligence tools, the volume of data types and locations becomes overwhelming.

Data classification and governance tools automate

- Identification and labeling.
- Real-time classification.
- Review across image, text, video, and audio file types.
- Application of context across user, role, and environment.
- Classification activities like marking and tagging.

Data Masking versus Data Encryption

Data masking prevents people from seeing information by hiding the identifiers from view. Data encryption makes data unusable and unreadable when someone lacks the required decryption key, or "code breaking" algorithm.

Both technologies have uses, and many companies may integrate both. Data masking can mitigate privacy risks arising from authenticated users who may not need to see data. For example, data masking would redact fields that a business intelligence tool uses in a report, protecting the privacy of personally identifiable information (PII).

Meanwhile, encryption protects data from being readable or usable if someone forwards a "share with a link" to the wrong person. When implementing encryption, organizations need to protect data-at-rest and data-in-transit across

- Email.
- Databases.
- Endpoints.

Encryption solutions can be deployed as

- **Gateway**: Cloud-based technology to protect data traveling into and out a resource.
- **Software**: Installed on a device to protect data.

Data Backup

To mitigate business interruption risks, companies need to have a data backup and recovery tool. This ensures that they have a way to recover data lost as a result of a ransomware attack or a natural disaster.

A data backup tool should

- Provide a point-in-time copy of the enterprise workload.
- Write data to a secondary storage device.
- Offer a cloud-based storage and recovery option.

Data backup tools can be delivered as hardware, software, or managed service.

Additional Technologies

New business-enabling technologies ultimately create new cybersecurity risks. As the risks evolve, new tools come to the rescue. Many of these new tools do not fall into a single category, either filling a gap that exists or solving a new problem. Categorizing these technologies by function rather than protection layer is more appropriate.

Identification

The shift to cloud means that assets are no longer concretely defined. For example, a laptop is a physical object with a serial number. Meanwhile, a virtual machine or container is a code-based asset that lacks this type of long-term identifier.

Asset Inventory Asset inventories automate the process of identifying resources. Typically, these tools engage in:

- **Discovery**: Finding managed and unmanaged devices, hardware, and software.
- **Vulnerability scanning**: Integrating with configuration management database (CMDB).
- **Continuous updating**: Real-time scanning and monitoring.

Attack Surface Management (ASM)/Cyber Asset Attack Surface Management (CAASM) The primary difference between these tools and asset inventories is that ASM/CAASM tools score risk and suggest remediation actions. The key capabilities for these technologies are as follows:

- **Discovery**: Known assets in the inventory, unknown assets to detect shadow IT, and rogue assets to detect malicious infrastructure.
- **Inventory and classification**: IT asset inventory creation and asset labeling.
- **Risk scoring**: Aggregated data about assets, including exploitability and distance from the public internet.
- **Continuous security monitoring**: Monitoring for common vulnerabilities and exposures (CVEs) and misconfigurations then offering remediation actions.

Protection

These tools focus on enforcing security policies for cloud-based assets.

Cloud Access Security Broker (CASB) A CASB monitors the cloud infrastructure to enforce security policies, including

- Authentication.
- Single sign-on.
- Authorization.
- Device profiling.
- Encryption.
- Logging.
- Alerting.
- Malware detection.

Software-as-a-Service (SaaS) Security Posture Management (SSPM) A CASB focuses on an organization's infrastructure, like AWS or Azure. However, SSPM focuses on the SaaS applications that connect to and within the company's cloud. An SSPM

- Inventories cloud assets.
- Identifies misconfigurations.
- Review access controls.
- Creates an audit trail.

Detection and Investigation

Every device, user, and application generate data when something happens. For example, applications record every user login, and devices record every program running. These records are called log files or log data. Detection and investigation technologies ingest these logs and analyze them to find abnormal activity across an environment.

Centralized Log Management Many IT operations teams already use centralized log management. These tools ingest all the log data from across the environment and then normalize, aggregate, correlate, and analyze the data. Although originally used by help desk and service desk analysts to find application or system issues, IT and security teams can use centralized log management tools to create security alerts.

Many centralized log management tools now come with security analytics, data and rule sets that incorporate user behavior to help mitigate cloud-based security risks.

Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) MSPs and MSSPs usually provide a SIEM or SOAR as their technology product. Then, they offer security analyst services, known as Security-Operations-Center-as-a-Service.

Most SMBs lack the staffing necessary to implement a SIEM or SOAR tool because these technologies require specialized skills. However, if a company wants to outsource its security function, then it should know the difference between them.

Like a centralized log management tool, SIEMs and SOARs aggregate, correlate, and analyze log data. However, a SIEM will also

- Incorporate cyber threat intelligence (CTI).
- Add context.
- Leverage analytics.

A SOAR starts with a SIEM's foundational capabilities, and then adds machine learning to automate responses.

To Outsource or Not to Outsource

At first glance, outsourcing security might seem like the obvious choice for an SMB. Between data breach statistics and the long list of technologies, the idea of managing cybersecurity in-house can feel overwhelming.

The definition of SMB varies, and not every business needs to meet the same compliance requirements. Further, not every business manages the same amount of PII. To make the best decision, an organization needs to start by understanding its own data use and its use cases.

Some basic considerations include

- Does it operate in a highly regulated industry, like healthcare or financial services?
- Does it collect, store, or process consumer PII that falls under a regulation like the General Data Protection Regulation (GDPR) or the California Privacy Rights Act (CPRA)?
- Does it fall under one of the exclusions in these laws?
- How many employees does the organization have?
- What is the organization's growth plan for the next two to five years?

For example, a company with fifty to one-hundred employees may find that paying for a slightly more expensive cloud services provider business plan covers its needs. In early 2023, both Google and Microsoft offered small business subscription plans that would manage the majority of an SMB's IAM, endpoint, and data needs. The pricing models were less than $20 per user per month.[6,7]

For mid-size enterprises employing 500–1,000 employees, these services may not provide the appropriate level of security and monitoring. Meanwhile, hiring an internal security analyst and aggregating all the tools may not be cost effective. In this case, working with an MSP or MSSP might be more prudent.

For SMBs, gaining visibility into risk often means looking for technologies that can provide services. Some SMBs choose to outsource their risk monitoring with managed service providers (MSPs) or managed security services providers (MSSPs). MSPs and MSSPs are organizations that provide various services, including

- Firewall management.
- Intrusion detection.

- Virtual private network (VPN).
- Event log management and alerting.
- Vulnerability scanning.
- Antivirus and web content filtering software/services.
- Patch management.
- Security incident and response management.
- Data leak prevention (DLP).
- Information security consulting.
- Security operations center (SOC) as-a-Service.

In many ways, MSPs and MSSPs enable SMBs to reduce the negative impact lower budgets and the cybersecurity skills gap create. Increasingly, SMBs recognize the value that these services provide. *The State of SMB Security 2020* report highlights the way SMBs manage their cybersecurity risks[8]:

- 73% plan to invest more or much more in cybersecurity over the next twelve months.
- 60% plan to invest in cybersecurity to reduce risk.
- 59% predict that they will outsource the majority of or all cybersecurity activities in five years.
- 43% currently outsource the majority of or all cybersecurity activities.

No matter what direction a company chooses, it needs to start by analyzing its current and future business objectives. Security tools are expensive. If deployed haphazardly, they can add to a company's security and privacy risks rather than reducing them. Organizations should implement security programs that protect their current environments while also being flexible enough to grow with them over time.

References

1. MITRE. (n.d.). *MITRE ATT&CK®*. Retrieved from https://attack.mitre.org/
2. Abrams, L. (2022, November 15). *Comcast Xfinity Accounts Hacked in Widespread 2FA Bypass Attacks*. Retrieved from BleepingComputer: https://www.bleepingcomputer.com/news/security/comcast-xfinity-accounts-hacked-in-widespread-2fa-bypass-attacks/

3. National Institute of Standards and Technology. (n.d.). *Information Security Continuous Monitoring* (ISCM) – Glossary. Retrieved from NIST Computer Resource Center: https://csrc.nist.gov/glossary/term/information_security_continuous_monitoring
4. *Definition of Cybersecurity Mesh – Gartner Information Technology Glossary*. (n.d.). Retrieved from Gartner: https://www.gartner.com/en/information-technology/glossary/cybersecurity-mesh
5. *Gartner 2021 Market Guide for Mobile Threat Defense*. (2021, April). Retrieved from Malware.News: https://malware.news/t/gartner-2021-market-guide-for-mobile-threat-defense/48030
6. *Google Workspace*. (n.d.). Retrieved from Google: https://workspace.google.com/pricing.html
7. Microsoft. (n.d.). *Enterprise Mobility and Security Pricing Options*. Retrieved from https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/compare-plans-and-pricing
8. ConnectWise. (n.d.). *The State of SMB Cybersecurity* 2020. https://www.connectwise.com/resources/smb-research.

7

Vendor Risk Management

Securing the Supply Chain

From technologies to contractor relationships, companies outsource various business functions. Companies continue to invest in public cloud infrastructures and Software-as-a-Service (SaaS) applications because they reduce overall costs. Meanwhile, they outsource services to freelancers and contractors to fill staffing gaps.

Contract or freelance staff makes sense to most organizations. They need someone to do a job, but they may not need someone to do that job for forty hours a week. By outsourcing this task, they have someone with the right skills who can complete the work without paying for unnecessary labor or benefits.

Cloud services providers (CSPs) and SaaS applications fulfill a similar role in the corporate IT environment. The cloud infrastructures save time and money with flexible digital resources. Meanwhile, the SaaS applications enable collaboration across distributed workforces.

Problematically, every time an organization outsources a business function, it also loses some control over security and privacy, ultimately increasing risk. Recognizing this shift, compliance mandates now incorporate requirements for third-party or vendor risk monitoring.

For example, the fundamental challenge facing the Defense Industrial Base (DIB) with the Cybersecurity Maturity Model Certification (CMMC) program is that the standard includes a "flow down," making companies responsible for ensuring that their subcontractors have the appropriate certifications.

Understanding the Third-Party Risk Landscape

Third-party data breach risks fall into three general categories. First, organizations need to worry that a technology vendor's data breach

DOI: 10.1201/9781003128588-7

will impact their customers' data. Second, attackers can engage in a supply chain attack by gaining access to a technology company's source code. Third, contractors can accidentally gain access to sensitive information. When organizations understand the similarities, differences, and overlaps between these third-party risks, they can implement risk mitigation controls.

Vendor Data Breach

From SaaS applications to Internet of Things (IoT) devices, companies now have a vast, expanded digital vendor ecosystem. For every application that a company has, the organization that developed the application has just many. As people look through the supply chain, they begin to find more connections and risks. When a third-party vendor experiences a data breach, it creates a ripple effect throughout the vendor ecosystem.

For example, according to the 2022 Data Breach Investigations Report, supply chain breaches[1]:

- Accounted for 62% of System Intrusion incidents.
- Use of Stolen Credentials and Ransomware were the top two action varieties.

When malicious actors gain unauthorized access to a vendor's systems and networks, it can compromise all their customers. Some examples of a third-party data breach could include cybercriminals stealing:

- Employee account information by attacking a company's payroll vendor.
- A hospital's patient data by attacking an anesthesiologist's office.
- A college's student loan records by attacking a loan servicing system.

Case Study: Accellion and Morgan Stanley In December 2020, Accellion, a company that develops firewall technologies, experienced a zero-day exploit in its File Transfer Appliance (FTA) product. In July 2021,

Morgan Stanley announced that its third-party account maintenance service vendor Guidehouse experienced a breach arising from its use of the Accellion FTA server.[2]

The Supply Chain Attack

In a supply chain attack, threat actors gain unauthorized access to a technology company's source code, then they write malicious code that will give them access to the application when a user installs it.

Threat actors continue to deploy supply chain attacks because they gain a higher return on investment.

Similarly, the 2022 Cost of a Data Breach Report noted that supply chain attacks[3]:

- Accounted for 19% of breaches overall.
- Cost an average of $4.46 million, 2.5% more than other types of data breaches.
- Took 303 days, an average of 26 more days than other types of data breaches, to identify and contain.

Case Study: SolarWinds In December 2020, software company SolarWinds announced that attackers had compromised its Network Management System (NMS) tool, Orion. Attackers gained access to the Orion software build system, enabling them to insert malicious code into software updates that SolarWinds released between March and June 2020.[4]

Contractor Access

Of the three types of third-party data breach risks, contractor access is the one that companies have some control over. When a company hires a contractor, it often provides information that the person needs to complete the assigned task. However, this can lead to several different types of data breaches:

- The company may have failed to appropriately limit access to a shared drive, and the contractors have unnecessary access to sensitive information.

- The contractors may be able to view all data in a database, including sensitive information that they do not need.
- The company may have sent the contractor a document and no longer has control over what the contractor does with it.
- The company may have sent the contractor sensitive information necessary for the task but failed to revoke the access when the contractor finished the task.

Case Study: Toyota In late 2022, Toyota announced that nearly 296,019 customer email addresses had been leaked because a subcontractor uploaded source code from the company's T-Connect app to a GitHub repository, accidentally setting permissions as "public" instead of "private." The data breach impacted customers who used their email address to register for the app as of 2017.[5]

Analyzing Third-Party Risk

Every organization needs to implement a third-party risk management (TPRM) program. Fundamentally, the TPRM processes map to the cybersecurity and privacy risk management processes:

- Identify vendors.
- Assess vendor risk.
- Implement controls that mitigate risk.
- Monitor third-party security and privacy.

Although the steps are the same, the internal stakeholders and the processes often differ.

Identification

While the vendor risk identification process is like the traditional security risk assessment, it looks at the risks slightly differently.

Vendors The vendor identification process must include technology and services vendors. Stakeholders involved should include employees from

- IT.
- Lines of business, like marketing and sales.
- Procurement.
- Legal.
- Accounts payable.

Each stakeholder should detail the following vendors:

- Technology solutions, like Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) providers.
- Contractors, like freelance writers, accountants, law firms.
- Outsourced IT vendors, like service desk analysts or technology resellers.

Risk management teams need to remember that their focus is on people and organizations outside the organization who could impact their sensitive data. In this case, the review of technology vendors focuses less on the whether the product's code contains a vulnerability and more on whether the vendor has a robust security program of its own.

Data Upon completing this process, the organization needs to identify the sensitive information that vendors can access. This review should include all data protected by industry laws and all sensitive corporate information, including

- Personally Identifiable Information (PII), like name, address, birth date, social security number.
- Bank account information.
- Protected Health Information (PHI), like healthcare insurance data.
- Intellectual property, like patents, copyrights, and trade secrets.

Risks Identifying risks brings together the vendors and the data that they can access. For example, a freelance writer with access to a corporate blog would pose less risk than an outsourced IT administrator with privileged access to create new users in a system.

Identifying risks includes

- Reviewing vendor access to systems, networks, and software.
- Vendor access to sensitive data.
- Vendor's importance to critical business operations.

Risk Analysis

Like the IT risk analysis, the vendor risk analysis looks at the following:

- The likelihood that the vendor's access to sensitive data can lead to a breach.
- The financial or business impact a data breach arising from that vendor's access would have.
- To analyze the risks, an organization needs visibility into a vendor's security program. Before onboarding a new vendor, the risk management team needs to engage in due diligence to understand the contractor's or vendor's policies and procedures for
  - Reviewing personnel during the hiring process.
  - Managing its own security risk.
  - Handling data privacy.

Risk Tolerance

As with IT risk, companies need to decide their risk tolerance. After reviewing each vendor, they need to decide what to do about the risk. They can choose to

- **Accept**: Onboard the vendor as-is.
- **Refuse**: Decide not to go to contract.
- **Mitigate**: Implement controls that reduce the risk.
- **Transfer**: Make someone else responsible for the risk, like purchasing insurance.

Contractor and vendor relationships can be more easily terminated than an employee relationship. For example, many companies adopted SaaS applications because subscription models give them more freedom. Contractor relationships can typically be terminated with

thirty- or forty-five-day notice. Since companies should complete a vendor risk assessment annually, they can review the relationship and update their decision regularly.

Vendor Tiering

The vendor risk assessment will provide visibility into which vendors pose a high, medium, or low risk to the company. While organizations should assess and monitor all vendors, not every third party requires the same level of oversight.

Vendor tiering is the process of separating vendors into risk categories according to

- **Criticality**: Importance to business operations.
- **Data sensitivity**: Type of information the vendor accesses or processes.
- **Compliance:** Regulatory compliance requirements for vendor type or data category.
- **Access**: Vendor interaction with systems and networks.

For example, the following three vendors pose different risks that require different levels of oversight:

- **Freelance marketing writer**: Limited access to shared drive's folders and files, none of which contain sensitive information, which requires limited oversight.
- **Outsourced recruiter**: Access to employment candidate names, emails, and phone numbers which may require some oversight throughout the year.
- **External firm acting as general counsel**: Access to sensitive corporate information and some PII as required by tasks, which may require regular oversight.

Engaging in due Diligence: The Vendor Questionnaire

People in risk management jobs often bemoan the vendor questionnaire. These documents set out a series of questions that vendors need to answer, often requiring supporting documentation, so that the company

can prove it conducted the appropriate due diligence. To maintain consistent processes across departments, companies should build out a standard questionnaire that everyone uses and that procurement reviews before a vendor signs a contract. The questions in the document should align with the company's vendor risk assessment processes.

Questions about Risk

In this section, a company should ask its vendor the same questions it asks itself. The risk identification questions should align to the same categories that company reviews when analyzing its own risk.

Data Some questions about data risk might include

- Do you collect, store, or transmit personally identifiable information (PII)?
- Do you limit your PII collection and storage?

Location Questions about location focus on where the company stores data, including

- Do you store PII in an on-premises location?
- Do you store PII in a cloud location?
- What geographic locations do you use when storing PII?

People Questions about personnel can look like this:

- How do you handle employee background verification?
- How do you provide users access to PII?
- Can users access PII remotely?

Devices This section focuses on how the vendor inventories its assets. Some questions could be

- What types of devices do your users collect, store, or transmit PII from?
- Do you monitor all devices connected to systems, software, and networks?

Compliance Understanding a vendor's compliance posture is particularly important for companies in highly regulated industries like

healthcare and financial services. For example, the questionnaire might include statement like

- List any government regulations that you need to comply with.
- List any industry standard certifications that you have achieved.
- Provide copies of the most recent internal and external audit reports.
- Provide a link to your publicly available Privacy Policy/Privacy Notice.

Questions About Policies and Procedures

Every vendor review should incorporate questions about policies and procedures because they form the foundation of good corporate governance strategies. Further, they should align to the vendor's risk assessment and tolerance.

Some questions to ask could include

- Do you have a team dedicated to information security?
- What is the information security team's composition and reporting structure?
- Do you have a formal Information Security and/or Privacy Program? Provide a copy of relevant policies and risk assessment documentation.
- Is signing a Confidentiality Agreement a condition of employment used to protect customer data?
- Do employees sign an Acceptable Use Policy? Attach a copy of policy.
- Do employees undergo cybersecurity and privacy training specific to their role in the organization?
- What is the policy exception process?
- How do you monitor for vulnerabilities and threats that impact your service?
- What are your logging and alerting mechanisms for security events?
- What are your Security Incident Response policies and procedures? Provide relevant documentation.
- How do you communicate incidents to clients/customers? Provide relevant documentation.

Questions about Technical Controls

Vendor's technical controls should align with how the organization sets its own controls. These questions can be grouped according to control category.

Identity and Access Management In this section, the questionnaire should provide insight into how the vendor manages authentication and access. Some questions in this section could include

- What is your password policy?
- Do you require multi-factor authentication?
- How do you assign access?

Network Security In this section, the vendor should supply information about the technical controls around its network. Some questions might be

- Do you segment networks? Provide a network diagram.
- Do you use firewalls?
- Do you require a VPN for remote access to network?
- How do you encrypt data-in-transit? Provide documentation.
- How do you ensure that data exchanges are secure?
- What is your network configuration change management process?

Device Security This part of the questionnaire should provide insight into vulnerability and configuration management. Some questions to include might be

- How often do you scan for vulnerabilities?
- How do you install security updates on end-user devices?
- How do you monitor for and detect malware on devices?
- How do you update firmware for network devices and Internet of Things (IoT) devices?

Applications When asking about application security, the questions should focus on both how the vendor protects the apps its employees use and how it secures the apps it develops.

Business Applications

Some examples of questions about protecting applications the vendor uses include

- How do you control access to applications?
- How do you monitor API security?
- How do you protect applications in your environment from the internet?

Application Development

Some questions to ask about how the vendor secures applications that it develops include:

- How do you assess your application's security?
- What are your secure software development lifecycle processes?
- How do you engage in code reviews, like static code analysis?
- Does the application allow administrators to enforce MFA?
- Do you engage in penetration testing for your application?
- Do you maintain a software bill of materials for third-party libraries or code used?
- How do you monitor vulnerabilities in dependencies?
- If you outsource development, how do you monitor developers' activities?
- How does your application support audit logging?
- How does your application support role-based access control?
- Does the application support API management?

Data Security and Privacy In addition to data security, companies need to understand vendor data privacy controls. Vendor technical controls should include data access and visibility. Some questions to ask might be

- How do you classify data?
- How do you anonymize data?
- How do you use data anonymization in the organization?
- How do you encrypt data? Provide documentation.
- What data processors access sensitive customer information?
- How do you control their access?

Incorporating Data Security and Privacy into Third-Party Contracts

Companies should include data security and privacy clauses in all vendor contracts. However, they may want to create more than one template to address the differences between technology product and services vendors.

Typically, vendor contracts contain the following clauses:

- **Confidentiality**: Vendor agrees to protect customer data confidentiality.
- **Non-disclosure agreement (NDA)**: Vendor agrees to maintain confidentiality of corporate intellectual property.
- **Service level agreement (SLA)**: Technology vendor agrees to certain levels of service availability and security.
- **Liability insurance**: Vendors who pose a greater security risk agree to provide insurance if they cause a data breach.
- **Breach notification**: Vendor agrees to inform the company of a data breach within a certain time frame and/or any of its clients'/customers' impacted parties.
- **Responsibility for authorized persons**: Vendor takes responsibility for employee or third-party access to sensitive information.
- **Compliance with laws**: Vendor agrees to comply with the same laws and industry standards as its client/customer.
- **Right to audit**: Vendor agrees that its clients/customers have a right to audit its security and privacy programs or review its third-party audit reports.

Complex Ecosystems Create Complex Problems

Highly connected, complex vendor ecosystems create complex security and privacy compliance challenges. Increasingly, compliance mandates recognize the impact that supply chain attacks have on customers' data. In 2018, the New York Department of Financial Services Cybersecurity Regulation was one of the first laws assigning companies' liability for their vendors' security posture. However, in 2021, the Executive Order on *Improving the Nation's Cybersecurity* incorporated a Software Bill of Materials (SBOM) mandate. As these attacks evolve, corporate responsibility for vendor security will continue to become increasingly demanding.

Unfortunately, SMBs often find themselves at a disadvantage with larger vendors. A Fortune 500 company with revenue in the hundreds of millions may be able to negotiate its CSP contract. However, an SMB with under a million dollars in revenue may be forced to sign a contract that the CSP provides. By understanding a vendor's potential risk and revenue impact, SMBs can make informed decisions, even when they lack bargaining power.

References

1. 2022 *Data Breach Investigations Report*. (n.d.). Retrieved from Verizon Business: https://www.verizon.com/business/resources/reports/2022/dbir/2022-dbir-data-breach-investigations-report.pdf
2. Page, C. (n.d.). The Accellion Data Breach Continues to Get Messier. Retrieved from TechCrunch: https://techcrunch.com/2021/07/08/the-accellion-data-breach-continues-to-get-messier/
3. Cost of a Data Breach 2022. (n.d.). Retrieved from IBM: https://www.ibm.com/downloads/cas/3R8N1DZJ
4. *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*. (2020, December 17). Retrieved from CISA: https://www.cisa.gov/uscert/ncas/alerts/aa20-352a
5. *Toyota Apologizes for Breach of User Info*. (2022, October 7). Retrieved from PYMNTS: https://www.pymnts.com/news/security-and-risk/2022/toyota-apologizes-for-breach-of-user-info/

8

Calculating the Total Cost of Compliance

As a company's IT environment becomes more complex, managing security, privacy, and compliance becomes more difficult. In the beginning, managing monitoring and documentation manually may not be that hard. With only a few policies and applications, the IT team could easily navigate across a few vendor-supplied dashboards.

As a business grows, so does its digital footprint. In the beginning, a company might use a spreadsheet on a shared drive to track its sales pipeline. At a certain point, this process becomes too time consuming, so the organization purchases a customer relationship management technology. Moving the tracking from a shared drive to a new tool adds a new data security risk and monitoring requirement. Like the sales team needed automation to streamline its pipeline tracking, the IT team may now need automation to help it manage cybersecurity.

The IT team knows it needs a new technology, but it also must provide the business use case. Meanwhile, management should understand how to calculate a solution's financial value. Leadership and technology teams need to speak a common financial language so that they can make informed purchasing decisions.

The Business Case for Cyber Resilience and Automation

Most SMBs function on tight revenue margins. Since each purchase further narrows these margins, many companies manage security and compliance manually for as long as possible. However, as businesses expand their digital footprints, investing in technologies that automate monitoring and compliance reporting ultimately reduces overhead and risk.

DOI: 10.1201/9781003128588-8

Cyber Resilience: What It Is and Why It Matters

Leadership teams are responsible for mitigating risk and protecting assets. As threat actors evolve their methodologies and deploy increasingly sophisticated attacks, cyber resilience is as important as cybersecurity.

The National Institute of Standards and Technology (NIST) defines cyber resiliency as

> The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment.[1]

While companies need to focus on preventing cyberattacks, they need to recognize that their reality will most likely be mitigating the impact an event has on their business. Risk mitigation strategies start by implementing and enforcing controls to keep attackers out of systems and networks. However, they end by detecting an attack and eradicating the threat as quickly as possible.

The key metrics that define cyber resilience are as follows:

- **Mean time to detect (MTTD)**: How long it takes the IT or security team to detect abnormal behavior indicating a security incident.
- **Mean time to investigate (MTTI)**: How long it takes to investigate a security incident.
- **Mean time to contain (MTTC)**: How long it takes to contain a threat.
- **Mean time to recover (MTTR)**: How long it takes to bring systems back to a preincident state.

Cyber resilience reduces threat actor dwell time, the amount of time spent in the company's systems and networks. The less time they spend poking around, the less damage they can do. In other words, SMBs should do their best to prevent malicious actors from gaining access, but they should adopt cyber resilient processes that enable them to reduce an attack's financial, reputation, and compliance impact.

Automation for Cyber Resilience

Security technology vendors market their products' automation capabilities because the data supports the value of artificial intelligence (AI) and machine learning (ML). While the term AI generates images of sentient robots protecting the world from cybercrimes, the reality is much less exciting and entertaining.

Understanding AI/ML AI and ML are advanced mathematical algorithms that technologies use to predict or describe events. For example, when a company says that it provides predictive analytics, it means that it has mathematical algorithms that correlate a vast amount of data giving a potential outcome that has a strong statistical probability that an event will occur. Descriptive analytics tell a company what happened using mathematical algorithms with a high degree of statistical probability. Meanwhile, diagnostic analytics use data and math to explain why something happened.

AI and ML are valuable tools in cybersecurity because they rely on pattern detection and mathematics. IT environments consist of machines that only do what people tell them to do. Generally, people have predictable daily routines. They work between certain hours. They complete certain tasks regularly, using applications and devices intended for those tasks. AI and ML are well-suited to analyzing these types of data sets.

Value of AI/ML for Cyber Resilience Most security products use some form of AI/ML because they can reduce detection and investigation times. Further, AI/ML automation is not necessarily all-or-nothing. Even partial deployments offer significant benefits.

Research found that even partial deployments offered benefits including[2]

- $2.5 million reduction in data breach costs.
- Twenty-four-day reduction in time to identify and contain a data breach.
- Twelve-day reduction for MTTD.
- Twelve-day reduction for MTTC.

Although these statistics apply to companies of all sizes, the value remains the same across them. By reducing MTTD and MTTC, companies limit an attackers' ability to disrupt business, making them more cyber resilient. Further, reducing the time it takes to detect and contain a threat equates to reducing data breach costs.

Understanding the Total Cost of Ownership

Cybersecurity technologies are expensive investments, and corporate leadership should understand how to calculate the value. As the organization grows, it needs to mature its security and privacy posture. When budgeting for technologies, leadership can focus on finding a solution with a low total cost of ownership.

Defining Total Cost of Ownership (TCO)

TCO considers all expenditures related to a technology throughout its lifespan. An investment's TCO changes based on deployment model, especially when comparing a cloud-based "as-a-Service" model to an on-premises hardware deployment.

A technology's TCO consists of

- **Purchase price**: The base cost at "checkout."
- **Deployment costs**: Money spent on hardware and consultants.
- **Maintenance**: Costs associated with updating a technology, installing patches, and monitoring service availability.
- **Depreciation/deductions**: Calculated tax savings which depend on how the technology is categorized.
- **Usage**: Time saved and staffing reductions.

An equation for calculating TCO might look like this:

$$\left(\text{Purchase Price} + \text{Deployment Costs} + \text{Maintenance}\right) - \left(\text{Depreciation} + \text{Usage}\right)$$

Overcoming the Challenges of Calculating TCO

The simplified TCO equation makes the calculation seem easier than it is. While some costs may quantitative, others are qualitative.

Further, some people become even more frustrated when they have a hard time correlating the security investment to revenue.

Often, security technologies feel more like an insurance premium than a business investment. A company purchases general liability insurance with crossed fingers, hoping it never needs to make a claim. Similarly, companies purchase security technologies hoping that they never experience a data breach. The investment feels more like a "necessary evil" than a "revenue enabler."

Predicting Revenue Impact Companies generate revenue across multiple channels, but directly relating a security tool to revenue is difficult. When trying to predict a security tool's revenue impact, companies should consider how it widens margins.

Automation enables employees to spend less time on repetitive tasks. They can spend more time focused on critical activities that require human skills and interventions. The increased productivity in one area creates a ripple effect throughout the organization, especially when applied to IT.

For example, some Identity and Access Management (IAM) tools automate the access request and approval process. A line of business employee requesting access no longer needs to wait for the IT to approve the request. The person requesting access can complete a business task faster while the IT employee focuses on investigating an application bug instead.

Budgeting Nearly every plan experiences setbacks. Delays occurring during deployment can lead to cost overruns. Maintaining the technology may require additional, unplanned staff. If a company is operating with very little financial flexibility, a subscription-based technology might be more appropriate.

Typically, organizations use cloud-delivered products because the model transfers much of the technology's maintenance back to the provider.

Prioritizing When multiple security investments have a similar TCO but solve different problems, prioritizing the purchase may be difficult,

especially without a quantitative connection to revenue. When trying to find an investment that provides the best value, companies should refer to their risk assessments.

Some considerations for prioritizing include

- Reducing risks that have the greatest financial and business operational impacts.
- Focusing on gaps in the organization's zero-trust architecture.
- Finding solutions that mitigate multiple risks.

Integrating with Current Architecture The tool proliferation struggle is real. Every new technology must integrate with the company's pre-existing business and security technology stack. For example, a tool that comes with a built-in connector can save the IT department time during implementation. If two technologies are similarly priced, the reduced deployment cost could reduce TCO.

Comparing Capital Expenditures (CAPEX) and Operating Expenses (OPEX)

Capital expenditure and operating expenses are used when filing tax returns. The security tool's categorization impacts the depreciation and deduction variable in the TCO equation.

Capital Expenditures (CAPEX) Capital expenditures are fixed assets that require an up-front payment and depreciate over time. Companies get tax deductions based on the item's depreciation over the product's lifespan. For example, when someone buys a car, the vehicle is a capital expenditure. The minute the person leaves the dealership, the car's value depreciates. Similarly, security hardware solutions, like a firewall device, are capital expenditures.

Capital expenditures come with the following benefits:

- **One-time calculated purchase**: No additional up-front costs into the future.
- **Long-term investment**: Remains in place until the device is too old to maintain.

As with everything, capital expenditures come with risks, including

- **Inaccurate forecasting**: Cost overruns from misjudgments or manual assessment processes.
- **Risk analysis**: Imprecise risk evaluations failing to consider changing economic landscape, business needs, buyer habits, supply chain security risk.

Capital expenditures are necessary, but companies need to carefully consider which ones will have the greatest impact.

Operating Expenses (OPEX) Operating expenses, also called operating costs, are fixed or variable expenditures related to a company's day-to-day core operations. The company lists OPEX as tax deductions. For example, rent is an operating expense because the company needs a physical location to conduct its core operations. However, interest charges are not an operating expense. When a company lowers its OPEX, it increases its overall business income.

Benefits of operating expenditures include

- **Cost certainty**: Low over-time variability for monthly or yearly subscription costs.
- **Shorter approval times**: Less planning with less up-front costs.
- **Flexibility**: Canceling or adjusting subscriptions.

However, OPEX solutions may not always be the best fit:

- **Lack customization capabilities**: Inability to integrate with internally designed tools.
- **Cost visibility**: Change in usage like adding new subscriptions or forgetting to cancel subscriptions.

Evaluating TCO

Most companies have a combination of CAPEX and OPEX security tools. One of the most frustrating things about cybersecurity, privacy, and compliance is that no single one-size-fits-all solution exists.

Organizations usually make their final technology decision based on how implementation will impact operating costs. Technologies exist to enable people, not to replace them. Any technologies added to the organization's security stack should enable visibility, enhance productivity, and reduce risk.

When evaluating TCO, SMBs should consider the following:

- What risk does the tool mitigate?
- Does the tool respond to a current security gap?
- What manual processes is the tool eliminating?
- How long will it take to implement/deploy the tool?
- Does the current staff have the knowledge and skills to implement or deploy the tool?
- Does the current staff have the knowledge and skills to use the tool?
- Does the current staff have time, knowledge, and skills to maintain a capital expenditure tool?
- How does the tool help with compliance reporting?

Optimizing the Total Cost of Compliance

Regardless of an organization's security, privacy, and compliance maturity level, all SMBs need to work toward optimizing their security technology stacks to help them reduce the total cost of compliance. Security tools matter because they save people time and effort. While treating compliance as a cost center is easy, preventing it from being one is difficult.

Compliance is expensive because it requires people with skills to spend time on tasks that they often feel take them away from more critical activities. With the right set of tools and processes, organizations can create more efficient programs that enhance security while optimizing compliance costs.

Segment Meaningfully

Security and privacy audits focus on protected data, like personally identifiable information (PII), cardholder data, or protected health information (PHI). Optimizing the total cost of compliance

starts by segmenting networks purposefully. Network segmentation enables the organization to reduce its attack surface by placing all sensitive data and the applications that use them on a few networks. It also enables them to track data flows more effectively. Finally, it streamlines the IT or security team's activities, enabling them to focus on high-risk networks, applications, networks, and systems.

The company can consider the following investments to enable:

- **Firewalls**: Allow traffic into and out of the network.
- **Routers and switches**: Use access control lists (ACLs) to allow or deny access to the network.
- **Virtual local area networks (VLANS)**: Operate on top of a group of computers or devices in the same physical space and network to segment that network rather than creating multiple physical networks.
- **Software-defined networking (SDN)**: Enables a single location where network administrators to manage applications' activities, controllers that route requests, and network devices.

Plan Purposefully

Zero-trust architectures purposefully consist of overlapping requirements. For example, organizations need to manage how users gain access to devices, networks, and applications. Additionally, they need to ensure that devices accessing networks and applications are secure. Through a layered approach to security, organizations create overlaps between tools and capabilities.

However, often organizations purchase tools in response to a single-use case. For example, early on, an organization may have implemented a federated identity and access portal for employees. As the organization grew, it hired external contractors and required them to use a single sign-on tool because giving each contractor a unique company email was too risky. These tools provide similar capabilities without providing additional security. For every access review, the IT team and department managers need to review two different tools, one for employees and one for contractors. Further, for every audit, the company needs to get documentation from two different locations.

Between monitoring and responding to documentation requests, this overlap doubles or triples administrative costs.

As early as possible, companies should focus their security technology decisions on what they need to protect and how to streamline those activities. While managing security using spreadsheets is untenable, planning and organizing the tools on a spreadsheet can be valuable. For example, IT and senior leadership can create a spreadsheet for each zero-trust pillar, listing the technologies implemented in one column and defining their capabilities across the row. This will provide visibility into what the organization has, where overlaps exist, and what it needs to implement in the future.

Reduce Administrative Tasks

By building a security-first compliance program, companies focus policies, procedures, and technical controls focus on their unique risks. IT, security, and compliance stakeholders need to work together to streamline communications and maintain a single source of information.

Depending on the company's size, managing compliance in spreadsheets and task management systems can work. However, as the organization adds more employees and applications, this may become overwhelming. SMBs should build compliance planning into their long-term business objectives because then they can prepare in advance.

Managing documentation is usually the primary hurdle, especially when compliance personnel are not involved in the daily IT and security tasks. Stakeholders should work together from the beginning to establish a set of workflows for compliance. Even without a dedicated compliance tool, the personnel responsible for security and privacy compliance should have

- Basic reminders for critical tasks.
- A defined, authoritative source of documentation.
- Processes for changing documents and recording versions.
- Communication workflows that ensure all necessary parties know about changes.

References

1. Cyber Resiliency – Glossary. (n.d.). Retrieved from CSRC: https://csrc.nist.gov/glossary/term/cyber_resiliency
2. Cost of a Data Breach 2022. (n.d.). Retrieved from IBM: https://www.ibm.com/downloads/cas/3R8N1DZJ

9

Information Security Audit

The What, How, and Why

Companies undertake all these security and privacy activities because they need to undergo an audit. For many people, an audit can feel like experiencing a real-world version of the recurring unprepared-for-a-math-test nightmare.

In some ways, audits can feel like a high school English teacher from the 1950s trying to find some uncrossed t's and undotted i's. The auditor reviews the company's high-level strategic program and cross-references those to the low-level technical controls, assessing compliance to an external standard and internally defined policies and processes. While audits can be like tests, they are also like tutors. No organization or program is perfect, and audits provide an opportunity for companies to "check their work."

Information security audits determine whether an organization's security program meets the specific objectives outlined in a compliance. To determine this, the auditors or assessors start with a list of objectives based on the law's or framework's language. Then, they compare a company's documented activities to these requirements. Auditors use three different assessment methods:

- **Testing**: Determining whether a control works as the organization intends.
- **Examining**: Reviewing, observing, or analyzing evidence that the company provides.
- **Interviewing**: Talking to people responsible for the daily data protection activities.

While most compliance mandates require an external audit, few offer insight into what a company can expect from one. Like any other

DOI: 10.1201/9781003128588-9

assessment, passing an audit requires preparation, information, and review. While compliance mandates may focus on different specific controls, every audit follows the same basic steps:

1. Plan for the audit.
2. Prepare for the audit.
3. Conduct the audit.
4. Report audit findings.
5. Follow up on audit issues.

While security audits are time consuming and resource intensive, companies can use the outcomes to build customer confidence and iterate their programs. Although all audits consist of these five steps, each task includes various subtasks which can make audits feel even more complicated. Breaking down the audit process into discrete tasks and handling each one separately can make the audit process less overwhelming.

Plan for the Audit

The planning stage sets the course for the whole audit by defining what systems will be audited, how they will be tested, and who the auditor will be.

Audit Objectives

Audit objectives align to the organization's cybersecurity goals set by the regulation or certification framework.

For example, if the organization's security goal is "limit access according to the principle of least privilege" then the audit objectives might be

- Verify that every user is uniquely identified.
- Verify role-based access controls limit access.
- Verify timely access termination upon termination of employment.

Scoping

Scoping is the process of defining the systems that an auditor will review. This process may be the most important one because a company should clearly identify and define all covered data, devices, and

networks. The scoping process is particularly important for audits that focus on a specific data category, like

- **Payment card industry data security standard (PCI DSS)**: All systems storing, processing, or transmitting cardholder data.
- **Cybersecurity maturity model certification 2.0 (CMMC 2.0)**: All controlled unclassified information (CUI).
- **Health insurance portability and accountability act (HIPAA)**: All protected health information (PHI).

For companies using a more general security framework, like the International Organization for Standardization 27000-series, the data categorization matters because they need to protect sensitive data, but they may not face the potential fines and penalties.

When scoping the environment, the three most important actions are as follows:

- Identifying and categorizing all covered data.
- Identifying and categorizing all systems that process, store, or transmit covered data.
- Segmenting networks and limiting how sensitive data flows between systems.

To ease audit pain, the company should try to limit the scope as precisely as possible. While some auditors may look at all systems, major findings only apply to those systems containing data covered by the audit's purpose. By scoping as precisely as possible, the company

- Reduces the number of systems that the auditor needs to review.
- Reduces the amount of documentation that the auditor needs.
- Reduces the amount of time the audit takes.

Roles and Responsibilities

The security and privacy policies should define management, IT, and security team roles and responsibilities. The auditor will use this list when interviewing people, so everyone should know how to answer questions about their job and how it relates to security.

Assessor/Auditor Selection

Finally, the organization needs to choose an auditor. In some cases, the regulatory requirement will provide specifications for the auditor. For example, a CMMC-certified assessor must conduct any assessments for CMMC Level 2 and Level 3 certifications. To achieve a SOC 2 certification, organizations need to use a Certified Public Account (CPA) or an audit firm approved by the American Institute of Certified Public Accountants (AICPA).

Preparing for the Audit

Planning and preparing for the audit have overlaps and similarities. To make the process less daunting, multiple smaller tasks and milestones are helpful.

Review Previous Audits/Documentation

This step applies to companies that have already had at least one external audit. The first item on any auditor's agenda will always be previous audit findings. Even if the company responded to the findings during or directly after the previous audit, the assessor wants to ensure that the implemented remediation works and remains functional. Whether the auditor requests it or not, a company should include documentation of the control in the package it provides.

Preexamination Interviews

Before beginning the on-site activities, the auditor meets with leadership. During this conversation, the auditor will ask questions about changes to the IT environment, including new services, products, or users. Further, the auditor will likely ask for some background documentation including

- Asset inventories.
- Network diagrams.
- Credit or operating losses attributed to IT.

The auditor uses these meetings to understand the organization's IT environment, audit scope, and reporting structure.

Documentation Gathering

Gathering documentation is the most time-consuming part of the entire audit. After the initial meeting, the auditor sends a documentation request detailing all the evidence necessary to complete the assessment. The collected documentation, or audit package, provides evidence that the auditor reviews during the audit.

Policies and Procedures Policies, procedures, and any supporting documentation prove management's involvement in and governance over the program.

Some examples of documentation include

- Data flow diagrams.
- Risk assessment.
- Security and Privacy Policies.
- Incident Response Policy/Plan.
- Business Continuity and Disaster Recovery Policies.
- Data Retention and Destruction Policy.
- Acceptable Use Policy.
- Encryption Policy.
- Written procedures associated with these policies.
- Vendor Risk Management Policy, including vendor/contractor list, copies of security questionnaires and contracts.

Technical Documentation This information comes from the company's IT environment to prove that the IT and security teams have the technologies appropriately configured and aligned to the policies.

Some examples of this documentation include

- Equipment maintenance records.
- System configurations.
- Password requirements.

- Authentication server or system logs.
- Intrusion Detection System logs.
- System backup logs.
- System update logs and patch records.
- Router and switch configurations and logs.
- Application logs.
- Antivirus logs.
- Firewall configurations and logs.
- Vulnerability scanning reports.
- Network traffic logs.
- Security alert rulesets and configurations.

People and Processes Since people are responsible for managing security, the auditor needs documentation about responsibilities and organizational structures.

Some examples of this documentation include

- Organizational chart.
- Employee Handbook.
- List of roles and responsibilities related to information security and compliance.
- Employee background checks.
- Employee termination documentation.
- Security awareness training logs.
- Visitor logs.

Conduct the Audit

After receiving the audit package, the audit fieldwork begins. On-site testing supplements the auditor's off-site document review and analysis.

Off-Site Document Review With so much information in the audit package, most auditors complete their initial review and analysis off-site. This process includes policy review, comparing documentation to written policies and procedures, and comparing documentation to the regulatory or compliance framework checklist.

On-Site Testing During the on-site testing, the auditor will review physical safeguards, samples of the IT environment's current state, and interview staff.

In some cases, the auditor may ask staff to demonstrate control effectiveness. For example, if the access policy requires multi-factor authentication for a remote login, the auditor can request to see the mechanism in practice, looking to ensure that the access and authentication logs document the process appropriately.

Report the Findings

The audit report is the underlying reason the whole audit exists. Typically, the auditor meets with management before providing the final report and explains any issues discovered during the audit. In some cases, the company may be able to remediate small problems before the auditor issues the final report. The report will indicate what the finding was and how the organization remediated it.

Executive Summary

The audit report includes the following sections:

- **Executive summary**: High level who conducted the audit, reason for the audit, audit scope, and any audit findings.
- **Background**: Overview of the company undergoing the audit and regulations/certifications associated with the audit, previous audits conducted by the assessor.
- **Objectives, scope, methodology**: Definition of systems audited, assessment methods used, and processes involved.
- **Findings and recommendations**: Summary of each system tested that includes controls and processes observed and tested as well as comment on whether the auditor had findings or opportunities for improvement incorporating management response when applicable.

Findings

For most companies, the findings and recommendations section is the most important part. The findings are the final "grade" that the

company achieved. Every company hopes its audit report has no findings, but the good news is that not all findings are equally problematic.

For each system audited, the findings and recommendations section will list:

- **No finding**: Nothing was wrong, and the system passed the test.
- **Observation/opportunity for improvement**: The company could do something to improve a control in this area, but it meets the baseline for compliance.
- **Minor nonconformance:** The system has an issue that prevents complete compliance, but the issue does not impact its ability to achieve intended results.
- **Major nonconformance**: The system has an issue where a control does not exist or is not working as intended, ultimately leaving the system at risk. This could also describe several minor nonconformance issues that indicate a governance failure.

Management Response

Management needs to provide a response to any observation/opportunity for improvement, minor nonconformance, and major nonconformance. The management response should

- Acknowledge the issue.
- Identify a corrective action.
- Provide a timeline for implementing the corrective action.

Follow up on Audit Issues

After the audit concludes, management must implement any corrective actions for issues defined as minor or major nonconformances. Management should also implement any remediation plans for observations/opportunities for improvement, but this is not an immediate requirement.

These steps might include

- Re-assessing risk.
- Purchasing a new tool.

- Implementing a new process or procedure.
- Hiring additional staff.

Depending on the regulation or certification framework, the company should complete the corrective action within sixty to ninety days. Once the company implements the corrective action, it needs to submit documentation to the auditor.

The Business Case for Audits: Liability Risk Mitigation

In highly regulated industries, companies need audits so that they can continue to do business. For example, if a financial institution's audit has a material finding, the federal regulator can impose fines or file a Memorandum of Understanding (MoU). An MoU sets out requirements and timelines for correcting a major nonconformance issue. If the financial institution fails to comply with the MoU, it may not be able to continue conducting business operations. While these outcomes are rare, they highlight the impact that an audit can have on businesses operating in industries like healthcare and financial services.

While other companies may not need to engage in third-party, independent audits, many still choose to complete them. For example, many organizations require a vendor to provide a SOC 2 report as a part of their third-party risk management process. Audits and compliance enable revenue growth for these business-to-business organizations.

However, audits also help organizations prove that they have an effective security and privacy program. An audit acts as objective, third-party validation proving that a company has implemented appropriate data protections. From a liability standpoint, this offers value by proving that the organization is following best practices.

Understanding Civil Law, Negligence, Contracts, and Fiduciary Duty

When people get into a car accident, the first question they ask is "who was at fault?" Someone driving too fast may not be able to bring the car to a stop in time. Someone who makes an illegal right turn may not have been able to see an oncoming vehicle. If one driver failed

to follow the law, the other person can file a lawsuit in civil court. Data breach lawsuits work similarly, and compliance can mitigate the amount of money it has to pay.

Civil Lawsuits

Increasingly, privacy laws give consumers the right to file civil lawsuits. Unlike criminal lawsuits that can lead to prison, civil lawsuits can force companies to pay plaintiffs money. However, audits can help mitigate a civil lawsuit's financial impact.

When people file civil lawsuits, they need to prove five things to win their case:

- **Duty**: The defendant being sued had a responsibility to the plaintiff, the person who filed the suit.
- **Breach**: The defendant failed in their responsibility.
- **Cause**: The failure caused harm.
- **Damages**: The plaintiff suffered damages, like physical injury, lost income, or property damage.

Through the lens of privacy, these four things could look like this:

- **Duty**: Did a privacy law or contract make the company responsible to the plaintiff?
- **Breach**: Did the company fail to protect the data for which it was responsible?
- **Cause**: Did that failure cause harm to the person whose data was stolen?
- **Damages**: Can the plaintiff be "made whole" if the company pays them money?

When discussing breach and cause, the plaintiff needs to show that the defendant was negligent. When lawyers talk about negligence, they use the standard of care concept. Standard of care can be defined in two different ways:

- What a reasonably prudent person would do.
- Conduct according to a legally established standard.

Negligence means that a person or company fails to act as a reasonably prudent person or to conduct business according to a legally

established standard. While the reasonably prudent standard of care can be qualitative, conduct outside a legally established standard is more quantitative. For example, if the speed limit is 55 MPH for safety purposes, someone driving at 65 MPH who gets into an accident is not following the legally established standard. By speeding, a person can be proven negligent for not following the law.

Laws establish a legal baseline for privacy and security. Compliance frameworks establish minimum baseline best practices for how a reasonably prudent company should act. When companies achieve compliance certifications or pass audits, they can use this documentation to counteract a plaintiff's claim that they were negligent.

Negligence and Contracts

In business relationships, companies sign contracts that define the parties' responsibilities. In response to third-party data breaches and privacy laws, most vendor contracts now include data security and privacy requirements.

A typical contract will define

- Type of data a vendor needs to protect.
- Industry regulations that apply to the contract.
- State or federal law that applies to the contract.
- What constitutes a security incident.
- When and how the vendor will supply a data breach notification.

Under these clauses, a vendor data breach becomes a breach of contract, meaning it failed to do what it promised to do. When a vendor breaches a contract clause, the customer can either immediately terminate the contract with no consequences or seek monetary damages.

Two types of contract breaches exist:

1. **Material breach**: The party receives something substantially different than the contract said they would.
2. **Minor breach**: The party receives mostly what it expected even though it was not exactly what the contract required.

In law school, contracts professors typically teach the story of the farmers and the milking cows. Farmer A wants to buy Farmer B's spotted

milking cow. The two agree on a price and sign a contract. Farmer A pays Farmer B. A material breach occurs if Farmer B replaces the spotted milking cow with a spotted cow that fails to provide milk. Farmer A paid for a cow whose milk he could sell, so the similar-looking replacement is substantially different than expected. A minor breach is when Farmer B replaces the spotted milking cow with a brown milking cow. The brown milking cow differs from the one described in the contract, but it provides the same amount of milk. This substitution is a minor breach of contract because Farmer A gains the agreed-upon benefit.

When considering breach of contract materiality, most courts consider the following:

- The benefit that the nonbreaching party received.
- Whether the nonbreaching party can be adequately compensated for damages.
- The breaching party's performance of the rest of the contract.
- Hardship to the breaching party.
- The breaching party's negligence or willful behavior.
- Whether the breaching party will perform the rest of the contract.

Companies that experience a data breach can use their compliance and audit documentation in a breach of contract lawsuit, too. In this case, the court will again review whether the company was negligent when handling sensitive information. Again, having documentation that proves it met the basic standard of care can help mitigate financial losses from the lawsuit.

Fiduciary Duty and Professional Negligence

For senior leadership members, compliance and audits may offer some liability protection. In recent years, prosecutors and regulators have brought lawsuits against senior leadership after their company experienced a data breach. In October 2022, the Federal Trade Commission (FTC) took action against the CEO of online drink delivery service Drizly for the company's security failures.[1] Every compliance mandate includes a governance component, requiring senior leadership oversight.

Senior management owes the organization a fiduciary duty, a legal and ethical responsibility to act in its best interest. In the context of privacy and security, two fiduciary duties can apply:

- **Fiduciary duty of care**: Exercising reasonable prudence when carrying out their duties to achieve the company's best interests.
- **Fiduciary duty of good faith and fair duty**: Acting with honesty, good faith, and fairness when engaging in daily tasks and operating the organization.

Compliance mandates formalize these duties within their governance requirements. Some examples of management requirements in compliance mandates include

- **International Organization for Standardization (ISO) standard 27002:2022 Clause 5.4 Management Responsibilities**: Management should demonstrate support of the information security policy, topic-specific policies, procedures, and information security controls.[2]
- **American Institute of Certified Public Accountants (AICPA) Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy CC1.3**: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.[3]

Since these governance requirements define reasonable prudence and good faith in daily tasks, organizations can choose to engage in a third-party audit to prove that senior management team has fulfilled its fiduciary duties.

The Benefits May Outweigh the Costs

Security and privacy audits are time-consuming, expensive undertakings. For example, an SMB can budget anywhere from $12,000 to $20,000 to complete a SOC 2 audit as it scales and needs to supply one to potential customers. However, as an organization scales its business, it also increases its potential liability.

Whether through certifications or shareable reports, the audit outcomes are fundamental to revenue growth for many businesses. Even companies outside of regulated industries need to consider the farther-reaching liability mitigation use cases, especially as new privacy laws provide consumers a legal right to sue companies after a data breach. While completing an expensive audit may not be necessary for the first few years, all organizations should incorporate these costs and processes as part of their overall strategic business plans.

References

1. *FTC Takes Action against Drizly and Its CEO James Cory Rellas for Security Failures That Exposed Data of 2.5 Million Consumers*. (2022, October 24). Retrieved from Federal Trade Commission: https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million
2. ISO. (2022, March). *ISO/IEC 27002 Information Security, Cybersecurity and Privacy Protection – Information Security Controls*.
3. AICPA. (2020, March). TSP Section 100 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

10

Cyber Liability Insurance

Controls mitigate risks. Cyber liability policies give companies a way to transfer the risk. Like auto policies give people a way to pay for car repairs after an accident, cyber liability policies give companies a way to pay for some data breach costs.

Increasingly, compliance mandates reference cyber insurance policies as a risk management strategy. For example, the International Organization for Standardization (ISO) 27002:2022 mentions the provision of insurance as a security measure that companies should consider when implementing controls to protect information when personnel work remotely.[1] Cyber risk insurance enables companies to mitigate financial losses arising from

- Business interruption.
- Hardware and software replacement.
- Legal fees.

New data protection laws give people the right to sue companies in civil court. For example, under the California Privacy Rights Act (CPRA) consumer may file a lawsuit in civil court if a data breach is the result of a company's violation of the duty to implement and maintain reasonable security procedures and practices.[2] With cyber liability insurance, companies can reduce the lawsuit's financial impact.

Most companies purchase Commercial General Liability (CGL) policies that cover property damage and bodily injury arising from an "occurrence" or an accident. However, these policies include specific language that excludes coverage for access or disclosure of confidential or personal information. These exclusions remove the following data-related liability payments from the CGL policy's coverage:

- Damages related to access to or disclosure of confidential business or personal information.
- Damages arising from data integrity issues or data unavailability.

DOI: 10.1201/9781003128588-10

Although the CGL policy eliminates these coverages, companies can add them to their policies for an additional fee. Not every company needs to have a cyber liability policy. For example, a freelancer who does graphic design might never have access to any sensitive corporate or customer personal information. However, a company with an e-commerce platform might need to purchase the cyber insurance coverage because it manages cardholder account data.

While cyber risk insurance can help SMBs manage their risk, they do not replace a robust security posture. Further, many insurers require companies to provide audit documentation when applying for coverage. The ever-changing threat landscape means that insurers need to understand their policyholders' security program.

Further, a cyber liability policy does not provide a blanket protection. Companies need to understand the coverages in their policies and the limitations of these coverages.

The Cyber Liability Policy

Like people purchase healthcare insurance to offset the costs of an emergency surgery, companies purchase insurance to offset the costs of an unforeseen event. The company, also called the insured, pays a premium, the cost of the insurance policy. The insurance policy is the contract that defines each party's responsibility to the other. Business leadership should understand how to read the policy and what it typically contains.

Declarations Page

The Declarations page provides a high-level summary of the coverage. It typically includes:

- **Policy period**: The policy's effective and expiration dates.
- **The policy limits**: The most amount of money that the company will receive from the insurance company.
- **The deductible**: The amount of money that the company must pay out-of-pocket before the insurance company has to pay for anything.

- **Sublimits**: The most amount of money that company will receive for the extra insurance coverage it purchased.

Most cyber insurance policies include two basic coverages:

- Response expenses.
- Defense and liability.

Companies can pay extra for the following additional coverages:

- Business income and extra expense.
- Extortion threats.
- Fines and penalties.
- Payment Card Industry Data Security Standard (PCI DSS).

Insuring Agreement

For each coverage type, the insurance policy will include an Insuring Agreement. This defines the insurer's and policyholder's responsibilities.

Some typical policyholder responsibilities include

- Data breach must occur during the policy period.
- Insured learns about the data breach after the policy's effective date.
- Insured did not know about the breach when it purchased coverage.
- Insured reports the data breach within thirty days of discovering it.
- Data breach occurs in a geographic area that the policy covers.

Limit of Insurance

This section references the amount of money outlined on the Declarations page as the most money that the insurance company will pay for any single data breach.

Definition of Insured

The definition of insured includes the person or entity listed on the Declarations page. However, this section provides additional

definitions based on different business models, limiting the coverage to only conduct related to the business:

- **Sole owners**: The individual and spouse.
- **Partnerships and joint ventures**: Members, partners, and their spouses.
- **Limited liability companies**: Owners, members, and managers.
- **Organizations**: Executive officers and directory.
- **Trust**: Trust and trustees.

Deductibles

This section formalizes the requirement that the policyholder must pay the entire deductible before the insurance company pays any money.

Duties in the Event of Loss

The insurer's responsibility is paying money. However, the insured also has responsibilities other than paying the premium, and this section of the policy defines them.

Some typical requirements include

- **Notification**: Reporting the data breach within thirty days of discovery.
- **Cooperation**: Helping the insurance company with the investigation, pursuing action against the perpetrator, preserving and permitting access to evidence, and providing a statement under oath.
- **Documentation**: Providing information like how the data breach occurred, when it occurred, number of compromised files, description of compromised data, encryption information, law enforcement notification, and geographic location of impacted parties.
- **Obligations**: Not voluntarily assuming obligations or making payments without insurance company approval.

Exclusions

Cyber liability insurance is not a blanket coverage, and companies need to know what the insurer removes from the policy.

Typically, the policy excludes coverage for

- Insured's malicious actions, including intentional or knowing violations of law.
- Costs to correct a system deficiency, including data security or storage issues.
- Costs associated with computer system shortcomings that the insured knew about prior to purchasing the policy including design or maintenance issues.
- Costs from a data breach caused by failure or improper security update installations.
- Fines and penalties.
- Costs from a failure to meet stated, federal, foreign, or self-regulatory minimum data security requirements.
- Intentional or knowing violations of the company's privacy policy.
- Breach of contract.

Insurance supports a company's security program; it does not act as a replacement. Equally important, the exclusion clearly discusses the need to comply with "self-regulatory" requirements. The policy only applies if the company complies with its own policies and processes. If the company has a defined security program but fails to follow its own rules, then the insurance company can deny the claim.

Conditions

The Conditions section contains everything the insurer wants to include in the contract that do neatly fit in one of the other categories. Some examples of what this section includes are as follows:

- Insured paying premium on time.
- Insured using a third-party provider that the insurer approves or designates.
- Consolidation of data breaches arising from the same event or at the same time.

The last condition about consolidating the data breaches focuses on limiting the how much money the insurer pays. If each individual person or entity with compromised data consisted of a different data breach, then the insurance company would have to pay the full policy

limits for each person or entity. By aggregating all of them as a single data breach, the insurer limits its payout.

For example, if a company has a $100,000 policy limit and ten people file lawsuits arising from the same event, the insurance company aggregates payments across all ten people until it pays a total of $100,000. It does not pay $100,000 to each person.

Definitions

Since insurance policies are contracts, both parties need to have a shared understanding of what the important terms mean. In this section, the policy typically defines

- Data breach.
- Data breach claim.
- Data breach expenses.
- Legal and forensic services.
- Loss.
- Personally identifiable information.
- Regulatory proceeding.

The Difference between Defense and Indemnification

Insurance policies typically include two types of coverage, defense costs and indemnification. Defense costs are legal costs associated with a lawsuit that the impacted parties file. Indemnification is the payment that impacted parties received for damages they suffered.

Typically, the duty to defend is broader than the duty to indemnify. Insurers often pay legal defense costs based on what plaintiffs write in the lawsuit. If even one allegation is something the policy covers, then the insurer will pay for the lawyers and legal fees. However, the insurer bases its indemnification decision on the facts uncovered during the investigation. The investigation may prove that the insured's negligence led to the data breach.

For example, a plaintiff might include the following allegations in the lawsuit:

- Cybercriminal accessed PII when the insured's third-party vendor experienced a data breach.

- Cybercriminal used an unpatched laptop to gain access to the insured's environment to steal PII.

In this case, the first allegation may be covered by the policy, requiring the insurer to pay the policyholder's defense costs. However, the second allegation appears to fall under the policy exclusion saying that the insurer has no obligation if the data breach arose from failure or improper security patch installation. Whether the lawsuit goes to trial or not, the insurer will likely argue that it does not have to pay the plaintiffs because the failure or improper security patch installation caused the data breach. It does this for two reasons:

- To reduce its payment to the plaintiff.
- To protect its right to deny indemnification if the insured caused the data breach.

Since insurers have a contractual obligation to protect their insured's interests, they may choose to pay the plaintiffs, or settle the lawsuit, before the case goes to trial. While trial might prove they have no duty to indemnify, it could hurt their insured's reputation, creating other legal problems for the insurer.

The Evolving Cyber Insurance Landscape

The insurance industry is risk averse because it only generates revenue when it can adequately predict losses arising from risk. The industry typically uses data analytics to price policies so that sales will always be greater than losses arising from claims. However, since 2020, the industry has increasingly struggled to price cyber risk policies, making them more expensive and less accessible.

Ransomware Attacks Led to Increased Premiums

Ransomware attacks increased by nearly 93% in 2021.[3] With many of these attacks, financially motivated cyber criminals recognize that companies purchase insurance to cover these attack types. Knowing this, they often make ransom demands that fall within a typical cyber liability policy's limits.

However, insurance carriers struggled to adequately price their policies because they lacked historical data about the costs and likelihood of these attacks. In response, cyber liability carriers increased premiums over 2021 and 2022. A review of cyber insurance costs for small business noted that policy premiums increased approximately 25%, with some companies seeing increases over 80%.[4] Further, the average cost for a cyber liability policy increased from $1,485 in 2020 to $1,589 in 2021.[4] While these increases protect insurance companies from reporting financial losses, they can outprice SMBs from the market.

Insurance Companies Reduce Their Exposure

Insurance companies not only increased premiums, but they also began writing fewer policies and reducing the amount of risk they were willing to take on. In 2021, insurers decreased available cyber insurance limits. For example, a company renewing a policy might find that its limits went from $3 million to $1 million.[3] The policy's terms, conditions, and exclusions stayed the same, but the organization received less financial risk protection. Many companies needed to look for additional insurance to get the same amount of financial coverage.

While raising premiums alleviates the problems associated with inadequate pricing models, reduced policy limits protect the insurance company's financials. In this case, the companies wanted to limit their financial responsibility to prevent one large loss from undermining their entire cyber liability business.

Nation-State Actors Change the Coverage Landscape

Sophisticated nation-state actors turned warfare into cyber warfare. In 2017, threat actors deployed the NotPetya ransomware, primarily affecting Ukrainian companies and companies with strong ties to the Ukraine. In November 2018, United States and British government officials linked the attacks to the Russian military.[5] With government officials linking these attacks to a foreign military, several insurance carriers invoked the "war exclusion." This declaration gave rise to two different lawsuits, ultimately leading to changes in policy language.

Merck v. Ace American In 2018, Merck sued its insurance carriers Ace American Insurance Company. Merck alleged that the malware resulted in $1.4 billion in damages. The company had purchased $1.75 billion in property insurance that covered "all risks" for loss or damage arising from destruction or corruption of computer data and software.[6]

Ace denied coverage citing its war exclusion, which stated:

> i. Hostile/Warlike Action Exclusion Language
>
> A. 1) Loss or damage caused by hostile or warlike action in time of peace or war, including action in hindering, combatting, or defending against an actual, impending, or expected attack:
>
> a. By any government or sovereign power (de jure or de factor) or by any authority maintaining or using military, naval or air forces;
>
> b. Or by military, naval, or air forces;
>
> c. Or by an agent of such government, power, authority or forces;
>
> This policy does not insure against loss or damaged caused by or resulting from Exclusions A., B., or C., regardless of any other cause or event contributing concurrently or in any other sequence to the loss.

In December 2021, the New Jersey court decided in favor of Merck, noting that

- No court had ever applied the war exclusion to a cyberattack.
- Both parties were aware that cyberattacks can come from nation-state actors.
- The insurer gave no previous notice that it intended to apply the war exclusion this way.
- Merck had every right to anticipate that the war exclusion only applied to traditional warfare not cyberattacks.

Mondelez v. Zurich On October 10, 2018, Mondelez International, a victim of the NotPetya malware attack, sued its insurance carrier, Zurich American Insurance Company. According to the lawsuit, Mondelez incurred $100 million in damages and submitted an insurance claim to Zurich under a policy that included coverage for

> actual Loss Sustained and EXTRA EXPENSE incurred by the Insured during the period of interruption directly resulting from the failure of the Insureds electronic data processing equipment or media to operate.[7]

On June 1, 2018, Zurich denied coverage, citing the policy's war exclusion, which stated as follows:

> This Policy excludes loss or damage directly or indirectly caused by or resulting from any of the following regardless of any other cause or event, whether or not insured under this Policy, contributing concurrently or in any other sequence to the loss:
>
> 2) a) hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any:
>
> (i) government or sovereign power (de.jure or de facto);
>
> (ii) military, naval, or air force; or
>
> (iii) agent or authority of any party specified in i or ii above.[7]

In November 2022, Mondelez and Zurich settled the case for an undisclosed amount of money.[8] From a legal perspective, the settlement made sense. If the Ohio court ruled in Zurich's favor, different states would have different legal precedent, which creates an additional legal headache for future claims. If the Ohio court ruled in favor of Mondelez, Zurich would have to pay the full damages claimed, at minimum. While the legal issues remain unresolved, Zurich saved money overall, especially since the Ohio court could have looked to the New Jersey ruling since it is the only current legal precedent.

Lloyd's of London Changes Policy Language In November 2021, Lloyd's of London drafted four separate "Cyber War and Cyber Operation Exclusion Clauses."[12] Lloyd's of London is a re-insurer, an insurance company for insurance companies. While the company drafted four different versions of the exclusion, all contain the following language:

> **Attribution of a cyber operation to a state**
>
> 3. The primary but not exclusive factor in determining attribution of a cyber operation shall be whether the government of the state (including its intelligence and security services) in which the computer system

affected by the cyber operation is physically located attributes the cyber operation to another state or those acting on its behalf.

4. Pending attribution by the government of the state (including its intelligence and security services) in which the computer system affected by the cyber operation is physically located, the insurer may rely upon an inference which is objectively reasonable as to attribution of the cyber operation to another state or those acting on its behalf. It is agreed that during this period no loss shall be paid.

5. In the event that the government of the state (including its intelligence and security services) in which the computer system affected by the cyber operation is physically located either:

5.1. takes an unreasonable length of time to, or

5.2. does not, or

5.3. declares it is unable to attribute the cyber operation to another state or those acting on its behalf, it shall be for the insurer to prove attribution by reference to such other evidence as is available[9]

This policy language was only the first step. In August 2022, Lloyd's released a Market Bulletin requiring that standalone cyberattack policies written by its members must include a cyber war exclusion beginning in March 2023.[10] In the Market Bulletin, Lloyd's specifically notes that while it supports providing cyber liability coverage, state sponsored cyberattacks must be managed differently.

Offering Security Monitoring Services

Recognizing that robust policyholder security ultimately reduces losses, cyber liability insurers increasingly offer security monitoring services as part of their policy packages. Some insurance companies partner with security ratings technologies. These technologies take an "outside-in" approach to monitoring, giving customers insight into potential security weaknesses. The insurers then suggest remediation strategies that mitigate policyholders' risks, ultimately reducing the likelihood that the insurer will need to pay a claim.

Other companies work to provide a combination of cyber insurance policy and continuous monitoring solution. Targeted at SMBs, these products offer a range of capabilities that help companies improve their

security posture and protect against unknown, unexpected financial losses arising from data breaches.

Everything New Is Nothing New

Insurers are starting to understand cyber liability risk better. Although still in its infancy, the cyber liability market is rapidly maturing, with underwriting becoming more sophisticated. According to one report, companies under $100 million in revenue have options for lower limits with reduced insurance carrier expectations around controls.[11] Underwriters recognize that threat actors target certain industry verticals more heavily and price their policies accordingly. As they gain a greater understanding of different security vulnerability and risk mitigation strategies, they have new requirements during the underwriting process or additional exclusions in the policies.

However, the insurance industry faced a similar situation in the physical realm before and adapted accordingly. In the 1970s and 1980s, new regulations from the Environmental Protection Agency (EPA) created a new set of losses. Companies found themselves facing lawsuits for pollution events like leaking underground storage tanks, landfills, or chemical waste associated with manufacturing. As they filed claims, the insurance industry sought to exclude coverage. For example, many of these events took place over time, as chemicals slowly leaked into the environment. Insurers attempted to argue that they were excluded from being covered because they failed to fall under the policy's definition of "occurrence." However, like the war exclusion and cyberattacks, courts felt that the contract language was vague, requiring insurers to pay the claims. Today, CGL policies contain pollution exclusions drafted in response to this coverage litigation and redefined occurrence to exclude these long-tail events.

As evidenced by changes since 2020, insurers are applying these physical environmental lessons to digital environments. While the coverage may change or companies may need to pay more for the insurance they want, cyber liability insurance will remain a valuable source of insurer's income, especially as they collect more historic data to better understand risk and likelihood.

References

1. ISO/IEC 27002 Information Security, Cybersecurity and Privacy Protection – Information Security Controls. (2022, March). International Organization for Standardization.
2. *The California Privacy Rights Act of* 2020. (n.d.). Retrieved from Californians for Consumer Privacy: https://www.caprivacy.org/cpra-text/
3. *Report on the Cyber Insurance Market*. (2022, October 18). Retrieved from National Association of Insurance Commissioners: https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf
4. Chen, P. (2022, July 13). Cyber Insurance Market Update. Retrieved from AdvisorSmith: https://advisorsmith.com/business-insurance/cyber-liability-insurance/market-update–2022/
5. *UK and US Blame Russia for 'Malicious' NotPetya Cyber-Attack*. (2018, February 15). Retrieved from BBC News: https://www.bbc.com/news/uk-politics-43062113
6. *Merck & Co, Inc and International Indemnity, Ltd v Ace American Insurance Company*. (n.d.). Retrieved from https://s3.documentcloud.org/documents/21183337/merck-v-ace-american.pdf
7. *Mondelez International, Inc. v. Zurich American Insurance Company, Circuit Court of Illinois, Cook County*. (n.d.). Retrieved from https://s3.documentcloud.org/documents/23257972/397265756-mondelez-zurich-1.pdf
8. Adriano, L. (2022, November 8). *Zurich, Mondelez Settle Longstanding Lawsuit over $100 Million Claim*. Retrieved from Insurance Business Magazine: https://www.insurancebusinessmag.com/us/news/cyber/zurich-mondelez-settle-longstanding-lawsuit-over-100-million-claim-426741.aspx
9. *Lloyd's Market Association Bulletin LMA21–042-PD*. (2022, November 25). Retrieved from Lloyd's Market Association: https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx
10. *State Back Cyber-Attack Exclusions*. (2022, August 16). Retrieved from Lloyd's of London: https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf
11. 2023 *U.S. Cyber Market Outlook*. (n.d.). Retrieved from Risk Placement Services:https://www.rpsins.com/learn/2022/nov/2023-us-cyber-market-outlook/
12. Rundle, J. (2022, August 18). *Lloyd's to Exclude Catastrophic Nation-Backed Cyberattacks from Insurance Coverage*. Retrieved from The Wall Street Journal: https://www.wsj.com/articles/lloyds-to-exclude-catastrophic-nation-backed-cyberattacks-from-insurance-coverage-11660861586

11

Cybersustainability

Ethical Data Handling for Corporate Responsibility

Cybersecurity professionals use terms like "environment," "ecosystem," and "data leakage" when discussing IT infrastructures and cyber threats. Modern cloud-based strategies mean that organizations must create proactive security programs that not only address today's risks but can also protect from tomorrow's threats. With the cybersecurity and privacy industries increasingly borrowing terms traditionally focused on the physical, companies can take lessons from the environmental movement to create long-term, sustainable digital transformation strategies.

In physical ecosystems, organisms coexist symbiotically to maintain the habitat. For example, the coral reef houses the algae, and in turn, the algae nourish the coral. Similarly, modern IT environments consist of interconnected, symbiotic relationships between technology partners. A customer relationship management (CRM) technology enables the customer to streamline its sales pipeline, ultimately enhancing revenue outcomes by reducing operational costs. The customer's subscription supports the CRMs continued innovation and revenue.

The relationships in these digital ecosystems increasingly mirror the relationships in physical ecosystem. For digital transformation to remain sustainable, organizations of all sizes must build out security and privacy programs that protect sensitive data. Much like the habitats consist of finite resources, digital business models rely on customer data, a finite resource.

The General Data Protection Regulation (GDPR) was a landmark law in many ways. Significantly, it was the first law to declare personal data protection a fundamental right, and it declared this in the first sentence of the first recital.[1] While companies should understand the

DOI: 10.1201/9781003128588-11

revenue and business value of data protection, they should also view it as part of being an ethical, socially responsible business.

Definition of "Cybersustainability"

Although no official definition of cybersustainability exists, the constant comparison between modern systems and physical environments creates an opportunity to use definitions drawn from environmental sustainability research. The research into environmental sustainability focuses on avoiding resource depletion to maintain ecosystem balance.

From a digital transformation standpoint, cloud migration strategies need to maintain data privacy and security to prevent the depletion of both financial and data resources. Costly data breaches undermine the business and financial value that digital ecosystems create. For example, when companies establish their risk tolerance, they really create a cost–benefit analysis between the positive business and revenue impacts and the negative financial, reputation, and compliance outcomes.

Within that context, cybersustainability means

- Adopting/maturing digital transformation strategies.
- Establishing access and governance policies that promote cyberhealth.
- Continuous monitoring to maintain data privacy/security.
- Communicating across stakeholders.
- Promoting operational resiliency.

While these principles come from various natural systems sustainability theories, they also apply to business and IT. For example, cyber resilience relies on operational resiliency. As a company's physical footprint grows, it invests in Environmental, Social, and Governance (ESG) because investors increasingly incorporate these factors to their analysis processes. Similarly, companies should architect systems or design applications to promote operational resilience.

Building on a Foundation of Environmental Sustainability Theory

Several sustainability theories act as the underpinning for cybersustainability. Integrations between applications create an interconnected digital

ecosystem. If a single point of failure can lead to a data breach, then the organization has not built a sustainable security and privacy program.

Sustainable Development Theory

Environmental scientists use sustainable development theory to describe practices for protecting natural systems and ecosystems while still providing the resources people need, like food, water, and electricity.

Within the environmental movement, sustainability development theory focuses on[2]

- Economic value.
- Healthy ecosystems.
- Building community.

Mapping these principles to cybersecurity and privacy looks like this[3]

- **Economic value**: Adopting/maturing digital transformation strategies.
- **Healthy ecosystems**:
  - Establishing access and governance policies that promote cyberhealth.
  - Continuously monitoring to maintain data privacy/security.
  - Promoting operational resiliency.
- **Building community**: Communicating across stakeholders.

Cybersustainable practices apply the core principles of physical sustainable development to designing and architecting digital transformation strategies. For example, when developing business models that ensure natural system sustainability, companies try to prevent them from increasing their overhead. Similarly, organizations adopt digital transformation strategies because they provide economic value by eliminating hardware costs and enabling scalability.

Complex Adaptive Systems (CAS)

Ecosystems are dynamic and constantly evolving. CAS responds to the complex behaviors within these systems, like learning and

adaptation. While not all the principles apply to technology, several offer key takeaways for cybersecurity and privacy programs[4]:

- **Self-organization**: Interactions and interrelationships not imposed by hierarchical structures.
- **Emergence**: New patterns and ideas arising from interactions, interconnection, independencies.
- **Co-evolution**: Dynamic and continuously changing adaptation.
- **Path dependence**: Changes tied to systems and history lacking universal causes and truths.
- **Feedback loops**: Changes from individual behaviors create critical formal or informal communication networks.

As companies design cyber resilient systems, they incorporate these principles:

- **Self-organization**: Collaboration tools and integrated applications within the ecosystem democratize data and resources.
- **Emergence**: New connections and interdependencies within cloud environments.
- **Co-evolution**: Dynamic technologies like artificial intelligence and machine learning analytics models.
- **Path dependence**: Ripple effect of third-party data breaches and vulnerabilities in code repositories.
- **Feedback loops**: Continuous monitoring informing evolving risk and program changes.

For example, the collaboration technologies that enable remote workforces also create new risks, like people sharing documents within the tool leading to a data leakage. Mapping the CAS components to digital transformation means that companies can use these principles to protect their digital systems.

Adaptive Governance

In environmental sustainability theory, adaptive governance focuses on creating a core set of terms, understandings, and collaboration across groups that have otherwise diverse interests. For example, local

governments institute recycling programs, but people complain about or refuse to separate out recyclables. These different interests create a disconnect between policy and performance.

In security, similar disconnects exist. For example, companies can set secure configuration requirements for their networks, but employees may not install security updates because the process gets in the way of completing tasks.

The core principles of adaptive governance focus on[5]

- **Complexity and scale**: interactions within and across location and time.
- **Resilience**: Reorganizing or adapting while retaining foundational functions and characteristics.
- **Networks**: Self-organizing multilevel networks to enabling learning, trust, and information sharing.
- **Institutions, adaptation, and social learning**: Structures of rules, laws, policies, and norms that incentivize people's actions.
- **Power and agency**: Transformation through powerful actors championing transformation, providing leadership, generating trust, managing conflicts, preparing for change, and establishing educational opportunities.
- **Outcomes**: Evaluation of whether desired outcomes occurred.

In security and privacy compliance, the principles can be applied like this:

- **Complexity and scale**: Companies use multiple public clouds, on-premises servers, and Software-as-a-Service (SaaS) applications.
- **Resilience**: IT and security teams need to adjust their security detections and alerts in response to changing attacker methodologies.
- **Networks**: Companies and governments need to collaborate and share security information, like vulnerabilities and threat intelligence, so they can coordinate responses to new risks.
- **Institutions, adaptation, and social learning**: Cybersecurity and privacy laws update best practices to adapt to new technology risks and incentivize corporate compliance.

- **Power and agency**: Security professionals and senior management work together to promote digital transformation by providing security awareness training and technologies, like password managers, that enable people to change their behaviors.
- **Outcomes**: Audits provide assurance over whether security controls function as desired.

Risk-based, security-first compliance programs are the IT equivalent of adaptive governance. When companies continuously monitor their environments, they uncover new risks and detect new threats so that the programs become cyber resilient.

SMBs: The Whole Is Greater Than the Sum of Its Parts

While an individual SMB may have fewer than 5,000 employees, they globally represent 90% of all companies and provide 70% of all employment.[6] The World Economic Forum (WEF) notes that new companies often drive radical technology and innovation cycles, especially since these innovations support the global sustainability agenda.[6] In its report, WEF notes that SMBs need to[6]

- **Boost organizational resilience**: Use governance as an explicit business strategy.
- **Digitally transform operations**: Digitize process and product innovation to transform business models.
- **Embrace sustainability**: Understand and capture data about energy consumption across the business lifecycle.

All three of these components translate to data security and privacy, yet the report only briefly mentions cybersecurity by noting that policymakers should have cohesive national strategies to combat cybersecurity issues that could undermine SMB digital transformation strategies.

SMBs sit in a unique position. Large enterprise organizations may manage high volumes of sensitive information, but their IT environments often include internally designed applications that prevent them from truly innovating their cybersecurity programs. For large organizations, building a cybersustainable infrastructure becomes an afterthought. Meanwhile, SMBs can build cybersustainability into their digital transformation strategies and their organizational cultures.

Applying Sustainability Development Theory for Cybersustainable Digital Strategies

The fundamental tenets of sustainability theory directly map to digital strategies. At its core, digital transformation uses an ecosystem of technologies that improve revenue by enabling workforce collaboration and connecting the brand with customers. As SMBs develop their digital strategies, they need to incorporate cybersecurity and privacy risks.

Use Case: Customer Experiences and Applications Consumers want digital customer experiences like applications that enable loyalty rewards. By their nature, these applications collect personally identifiable information (PII) like

- Customer name.
- Email.
- Password.
- Credit card number.

Data security and privacy should be considered when software developers define the project's requirements to design the application around these issues. By incorporating security and privacy before developers write a single line of code, these qualities are built into the application's DNA.

Use Case: Business Analytics Business analytics enable data-driven business plans. Many companies use business intelligence applications to analyze

- Customer buying behaviors.
- Customer product/service usage patterns.
- Market trends.

While these metrics digitize the organization's business model, they increase privacy risks. Before deploying a data lake, organizations need to clearly classify and tag all sensitive data. Through this activity, they build their business intelligence capabilities on a foundation of data protection.

Applying Complex Adaptive System Theory to Embrace Cybersustainability

CAS enables organizations to embrace cybersustainability by enabling them to capture, understand, and analyze security data across their digital ecosystems and business lifecycles. SMBs implement technologies to enable workforce independence and productivity, but with each new connection, SMBs increase their risk. As they evolve their security and privacy programs, they collect, aggregate, and analyze data to detect changes in their IT environments. They use this information to inform the next iteration of the program.

Use Case: Cyber Threat Intelligence and Security Alerts Cyber threat intelligence (CTI) provides information about changes to threat actor attack methodologies, including

- Industries targeted.
- Vulnerabilities exploited.
- Vendors compromised.

This information enables IT and security teams to focus their activities. For example, if they know that a chat technology employees use to share documents has a known vulnerability and threat actors are actively exploiting it, they know to look for abnormal activities connected to this application. As risks arising from these interconnections emerge, they adapt their response to this third-party ecosystem risk.

Use Case: Conditional Access Controls With conditional access, user authentication to a network or application ties to the person's device security and/or location. For example, if someone attempts to connect to a critical application that processes sensitive information, conditional access controls would prompt a multi-factor authentication challenge question.

Conditional access recognizes the emergence of a new risk and adapts to it. The automated process recognizes the path dependencies between sensitive data, applications, and users. It provides feedback about the risk change then when the user is back in a recognized location, reverting to the original authentication requirements and creating a feedback loop.

Applying Adaptive Governance as a Business Strategy for Cyber Resilience

Adaptive governance offers an integrated and flexible model upon which organizations can build a cyber resilient business strategy. Cyber resilience focuses on reducing an attack's impact on critical business operations. Leveraging the principles of adaptive governance, SMBs can work with threat intelligence sharing groups to help them establish adaptable incident response plans to help mitigate the risks associated with their IT environment's complexity and scale. By collaboration, business, IT, and security leadership can create a culture of security rooted in employee knowledge, ultimately mitigating risk and enhancing resilience.

Use Case: Risk Analysis Every security and privacy compliance program begins with a risk assessment that should incorporate a network of cross-functional stakeholders. When completed meaningfully, a risk assessment analyzes the corporate IT environment's complexity and scale by identifying the business-critical assets and the interdependencies between them.

The risk assessment enables IT and security teams to architect cyber resilient systems because they know which assets require the most protection. As risks change, the security control implementations, detection alerts, and monitoring capabilities evolve. Since senior leadership must approve the security and privacy policy, the organization establishes a governance model that focuses security on operational resilience with audits evaluating whether the program is effective.

Use Case: Tabletop Exercises A tabletop exercise simulates a security incident so that security teams work through their incident response processes. Seen as professional education, the exercises give the teams experience so that they can find weaknesses in the incident response process before having to respond to a real incident. Teams make changes to processes or fine-tune their security detections, ultimately mitigating business disruption risks.

When business, IT, and security leadership sets a strategy that regularly includes tabletop exercises, they create a collaborative culture built on social learning and knowledge sharing that gives incident

response teams the power and agency to improve operational and cyber resilience by reducing key metrics like mean time to detect (MTTD) and mean time to contain (MTTC).

Future-Proofing Data Protection

Protecting personal data is a company's social responsibility. In the same way that companies seek to limit their carbon footprint, they should be limiting their digital footprint. The Industrial Revolution's environmental impact is still being assessed. Nearly 200 years after the first factories were built, their impact on climate change is becoming a public concern.

The digital Industrial Revolution remains in its early stages. Although companies have seen the fallout from data breaches, the long-term impacts may not be visible for decades. To prevent the digital equivalent of climate change, SMBs must consider their future data protection responsibility when developing digital transformation strategies.

References

1. *Recital 1- Data Protection as a Fundamental Right*. (2019, September 2). Retrieved from General Data Protection Regulation (GDPR): https://gdpr-info.eu/recitals/no–1/
2. Quieroz, M., Tallon, P., Coltman, T., & Sharma, R. (2018). Corporate Knows Best (Maybe): The Impact of Global versus Local IT Capabilities on Business Unit Agility. *Hawaii International Conference on System Sciences (HICSS)*.
3. Walsh, K., & Raschke, J. (2019, September 1). *Sustainable Development for Digital Transformation, Part 1*. Retrieved from ISACA Journal: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/sustainable-development-for-digital-transformation-part-1
4. Naudé, M. (2012). Sustainable Development and Complex Adaptive Systems. Corporate Ownership & Control, https://pdfs.semanticscholar.org/6c65/79fdb8dd7be13deef3ce766d6b9569906c99.pdf
5. Preiser, R., Biggs, R., De Vos, A., & Folke, C. (2018). Social-Ecological Systems as Complex Adaptive Systems: Organizing Principles for Advancing Research Methods and Approaches. Ecology and Society, 23(4), https://www.ecologyandsociety.org/vol23/iss4/art46/.
6. *Future Readiness of SMEs and Mid-Sized Companies: A Year On*. (2022, December 2). Retrieved from World Economic Forum: https://www.weforum.org/reports/future-readiness-of-smes-and-mid-sized-companies-a-year-on/

12

Magic 8 Ball Says "Yes"

Some things, like death and taxes, are certain. In a digital world, people can add cyberattacks and data breaches to the list. Unless the world devolves into a dystopian, postapocalyptic, preindustrial society, technology companies will continue to innovate, meaning people will continue to adopt them.

Large, historic enterprise organizations are the Boomer generation of business. Their business models existed in analog form, and they built IT infrastructures over time. They accrued legacy technologies and built internally designed applications or systems. While innovative at the time, their IT infrastructures now become digital behemoths, weighing them down with technical debt. These organizations often focus on securing what they have because they cannot afford to rebuild from scratch. As they take a backward-looking approach to security, they view it as a hindrance and cost center.

SMBs are the Zoomer generation of businesses. Their business and operating models have always been digital, so they have a freedom that the large enterprises often lack. SMBs are either new-to-market firms or have a nascent IT ecosystem. Instead of trying to wedge security and privacy into their current operating models, forward-thinking SMBs can build their business and revenue objectives around security and privacy. Born in an era when customers look for data privacy and security, these firms have an opportunity to build data protection into their business and operating models from the beginning. They are the organizations that can leverage privacy and security as revenue enablers.

Forward-thinking SMBs that understand data protection set themselves up to create cyber resilience as part of their products and services. They derive value from data protection because they understand it.

DOI: 10.1201/9781003128588-12

Business Models for the Fourth Industrial Revolution

Predicting new technologies is impossible. Think tanks and digital historians already view the current era as the fourth industrial revolution. In his book *The Fourth Industrial Revolution*, Klaus Schwab argued that this new era consists of simultaneously occurring breakthroughs fusing technologies and their interactions across the physical, digital, and biological domains.[1]

Schwab explains the main impacts the fourth industrial revolution has on businesses, regardless of industry, are[1] as follows:

- Shifting customer expectations.
- Data-driven product enhancements.
- New partnerships arising as companies collaborate in new ways.
- New digital operating models.

Schwab defined this term in 2016, three years before the onset of the COVID-19 pandemic. Since global lockdowns, the fourth industrial revolution's impact has become even more pronounced. The pandemic shifted business models and changed lifestyles.

SMBs must incorporate this shift into their business models. Traditional operating models taught in business schools may no longer apply to new organizations. The future of privacy and security is embedded into the fourth industrial revolution's impact.

Shifting Customer Expectations: Privacy-by-Design

Customers—both corporate and consumer—want digital experiences. They want on-demand information and services delivered electronically. Companies supply these services by collecting sensitive data. Malicious actors will keep stealing data to profit from it. In response, governments will continue to enact increasingly stringent data laws.

Businesses that provide personalized customer experiences cultivate brand loyalty. One study found[2]

- 64% of customers would rather purchase from a brand that knows them.
- 34% of customers would spend more money for this experience.
- 49% of customers were more likely to purchase from a brand that personalizes well.

Customers want the personalization that comes with data analytics, but they also want companies that protect their data. These seemingly contradictory desires mean that SMBs must consider privacy at every inflection point.

Meanwhile, organizations need to view their workforce members as their internal customers. Employees want remote work opportunities, and SMBs need to IT infrastructures that support them.

Successful business models will natively incorporate privacy-by-design. Updated in 2011, *Privacy by Design: The 7 Foundational Principles* sets out the following definition of the model[3]:

1. **Proactive not reactive; preventative not remedial**: Anticipate and prevent privacy risks.
2. **Privacy as the default setting**: Provide privacy through IT system and business practices so people do not have to do anything to protect themselves.
3. **Privacy embedded into design**: Design and architect IT systems and business practices with data privacy as an integral component.
4. **Full functionality—positive-sum, not zero-sum**: View privacy through a "win-win" mentality to accommodate all legitimate interests.
5. **End-to-end security—full lifecycle protection**: Design secure system before collecting data, secure retained data, securely destroy data.
6. **Visibility and transparency—keep it open**: Prove to all stakeholders that business practices and technologies operated as intended, subject to objective verification.
7. **Respect for user privacy**: Keep designs user-centric with strong privacy default, appropriate notice, and user-friendly options.

Privacy is a universal human right. People have a right to give companies their data and rescind that gift. When companies collect customer data, they become responsible for what happens to it. Privacy must be embedded into all decisions, including product development and business workflows.

An SMB's relative IT immaturity is a bonus. They can seek out business and security technologies simultaneously. For each technology

added to their business IT infrastructures, companies must ask and answer the following:

- To function as intended, what data does this application or device need to store, transmit, or access?
- To achieve the intended return on investment, what resources does this application or device need to connect to?
- To streamline business operations, what users need access to this application or device?
- To secure these data flows, what security technologies must be in place?
- To protect data privacy, what operational processes need to be implemented?
- Are these security and privacy controls user-friendly for customers or workforce members?

By asking and answering these questions before implementing a new technology, SMBs build data security and privacy directly into their organizations' DNA.

Customer-Centric, Data-Driven Product and Service Enhancements: Solving Data Protection Problems through Automation

Every modern company is an IT company. Across all industry verticals, organizations provide customer-focused technologies. For example, even a small business selling handmade items provides an e-commerce option for customers. Technology sits at the center of modern operational models, meaning that all organizations need to carefully consider every digital experience's data protection requirement.

As customers shift their expectations, organizations adopt data-driven decision-making strategies enabled by these IT decisions. A customer-centric business strategy analyzes external and internal customer needs and expectations to

- Help solve problems.
- Build relationships.
- Provide value.

To truly be customer-centric, companies need to make data-driven decisions about product and service enhancements across their business

and security technology stacks. Protecting this mission-critical data while maintaining these business-critical work models requires companies to adopt zero-trust architectures. SMBs need operational and security technologies that work together, especially since they have limited budgets compared to large enterprises.

The External Customer Technology

Having a robust data culture enables a business to understand what products or services customers consume so that the organization can predict what additional products and services customers might want. To collect this data, they need customer-facing technologies. As companies build out their data collection infrastructure, they need to apply customer-centric questions to their implementations.

SMBs should engage in the following assessment prior to implementing an external customer-focused technology:

- What customer problem does this solve?
- What customer data risk does this create?
- How does this technology help build a stronger customer relationship?
- How could a data breach arising from this technology damage the customer relationship?
- How does this technology provide a value to customers even before they spend money?
- How will data security and privacy enhance this value?

For example, a business may offer shopping options through social media. As part of the decision-making process, the business needs to understand the following:

- **Customer problem solved**: Customers like purchasing from social media applications because this is where they connect with the brand.
- **Customer data risk**: A social media platform's API collects, processes, and transmits sensitive information, including geographic location and contacts.
- **Stronger customer relationship**: The social media platform's algorithms enable customers to have a more personalized brand experience.

- **Data breach damage**: Customers expect brands to understand how social media platforms collect too much data and to limit their use of this overcollection as precisely as possible.
- **Customer value**: Customers learn about new products and services that align with their interests and needs because the social media platform's algorithms highlight them.
- **Enhanced value with data privacy and security**: The brand limits the way that the social media platform's API can create and send customer data when people interact with their page.

This cost-benefit analysis, like a risk assessment, enables organizations to implement customer-facing automation in ways that also align with consumer data protection concerns. Customers following the brand's social media account provide data through likes and follows so the company can use this to inform its new offerings. Meanwhile, by focusing on the data that it needs and telling customers how it plans to limit its collection, the company leverages privacy-by-design principles that build customer trust and enable revenue.

The Internal Customer Technology

Most companies implement security technologies without considering how workforce members use them. Companies that view their workforce members as internal customers think about how people will use these new technologies. By taking the same data-driven approach to its security stack that it takes to its customer technology implementations, a company gains higher levels of end-user adoption.

When purchasing a security technology, SMBs should engage in the following assessment that follows a similar model to the one they use before implementing customer-facing technologies:

- What workforce problem does this solve?
- How many additional steps does this add to a task?
- How does this technology help workforce members collaborate more effectively and efficiently?
- How could this technology become too cumbersome for workforce members?

- How does this technology provide a value to workforce members?
- How will this technology help workforce members view data security and privacy as valuable?

Identity and Access Management (IAM) tools provide an excellent example. Multifactor authentication (MFA) is critical to security but requires people to take additional steps before gaining access to resources. Often, this frustrates workforce members and leads them to creating workarounds. As part of the decision-making process, organizations need to understand the following:

- **Workforce problem solved**: Security risks arising from stolen credentials or password-based cyberattacks.
- **Additional steps**: Technology incorporates at minimum two additional steps, likely requiring access to two devices.
- **Enable collaboration**: Workforce members can share access to resources without having to share a login credential.
- **Technology can be cumbersome**: Requiring unique MFA for each resource during each login requires two additional steps as people access different resources throughout their workdays.
- **Technology value**: An MFA tool that automates authentication challenges across the business technology stack saves people time.
- **Enhanced value with security and privacy**: Workforce members adopt better cyber hygiene across all activities by learning that data protection does not always mean more work.

When companies view workforce members as valuable internal customers, they make security technology purchasing decisions that incentivize cyber hygiene.

New Partnerships and Collaboration Models: Transparency and Education

Similarly, SMBs build new partnerships with external and internal customers through transparency and education. In both cases, SMBs need to create clear data protection policies and make them available.

Further, they need to educate both groups about what data protection means.

Partnering and Collaborating with Customers

Organizations post their privacy policies on their websites, providing customers with visibility but little control. For example, many organizations post their General Data Protection Regulation (GDPR) cookie notice on their website, as required by law, but fail to give customers real options. Too many websites have a general notice advising visitors that by clicking yes and continuing to view content, they are giving consent. These policies are not transparent, nor do they educate visitors.

Organizations need to provide true transparency. They must go beyond the bare minimum to help customers understand how they collect and use data. They must collaborate with customers by providing accessible ways for them to control their data. Customers should be able to provide valuable feedback, not only about the data companies collect but about how they want the company to use data.

At minimum, companies in both the business-to-business and business-to-consumer spaces should have the following on their websites:

- Easy-to-use cookie policy with options that include
  - A simple "deny all" option.
  - A list of cookies and what providing them means.
- Way to opt-out for all marketing materials.
- Easy-to-find page explaining the company's data protection philosophy.
- Information about the company's data breach communication policy.

Companies should view their customers as partners and collaborators. Since data is mission critical to business success, customers who share data are business partners. They deserve transparency because they provide business value, even without purchasing products or services.

Partnering and Collaborating with Workforce Members

Internally, IT and security teams need to partner and collaborate with employees more. Cybersecurity training programs often fail to provide

meaningful experiences that help people learn better practices. IT and security teams need to partner with the rest of the company by explaining how the technical controls reinforce the training program's materials to build meaningful educational experiences.

The primary educational gap existing in most cybersecurity awareness training and end-user resistance to IT controls lies in the lack of creating clear connections between the two. Security professionals within the organization can help explain how their technical security controls reinforce the organization's cybersecurity awareness.

By collaborating with workforce members, IT and security teams can build educational experiences based on how people learn. For example, the six principles of adult learning theory are[4] as follows:

1. **The need to know**: Provide context and explain the benefit of the lesson.
2. **The learner's self-concept:** Adult learners often resist didactic—or bossy—teaching approaches.
3. **The role of the learner's experience:** Using experiential learning enables adult learners to incorporate their work and life experiences into the process.
4. **Readiness to learn**: Adults learn better when the situation or psychological reason builds on previous knowledge.
5. **Orientation to learning**: Problem-based or task-centered exercises work best.
6. **Motivation**: Internal factors such as goal setting, career ambitions, or self-esteem drive adult learners

By building new internal learning partnerships between technology teams and workforce members, companies can create educational experiences that lead to cultures of security. Leveraging adult learning theory and collaborating could look like this:

1. **The need to know**: Explaining the connection between technical controls and awareness training provides context and shows how the lesson relates to their experience as an end user who may feel frustrated by controls in day-to-day activities.
2. **The learner's self-concept**: Reinforcing how the controls align to the awareness training removes some of the didactic

approach by giving them experience with how the technical controls work.

3. **The role of the learner's experience**: Understanding the way that the controls work and how they support better cyber hygiene offers experiential learning that enables adult learners to incorporate their work experiences into the process
4. **Readiness to learn**: Building on the basics of the cybersecurity awareness program gives adult learners a way to apply their previous knowledge gained from training to the situation more effectively.
5. **Orientation to learning**: Offering real-world examples of how the technical controls work and asking them to engage in conversations with security teams provide problem-based exercises.
6. **Motivation**: Knowledge is always power so working with security teams to discuss how technical controls work can increase end-user confidence and self-esteem which is an internal driver.

This collaboration creates cross-functional transparency. When technology teams explain the technical controls and their purposes, business teams understand their roles better. Further, by partnering together, the business teams can articulate their struggles more clearly, giving technology teams the data that helps them make future purchasing decisions.

Digital Operating Models: Security-First Compliance

To secure the digital fourth industrial revolution, legislative bodies and industry standards organizations will continue to focus on zero-trust, security-first requirements. Every regulation enacted and framework updated since 2020 has focused on the layered defense-in-depth approach to security that zero-trust architectures seek to create.

Information security compliance professionals have long held that by securing IT environments organizations will achieve better audit outcomes. Slow-moving bureaucracies now reinforce these statements.

Architecting cyber resilient systems for digital operating models is critical. SMBs need to build systems with security at the forefront, meaning that they recognize from the start that the initial implementation will need continuous monitoring and iteration. They need to build continuous assurance technologies into their business IT infrastructure from the start.

To do this, they need to ensure that for every single technology deployment they have technologies that enable them to

- **Assess, assess, and assess again**: Cyber resilient systems operationalize the risk assessment process by building continuous monitoring into the digital business model.
- **Automate assurance**: Compliance requires continuous documentation, so organizations need the set of solutions that automate these processes efficiently and cost-effectively.
- **Communicate consistently**: Everyone within the company needs a shared vocabulary for consistently talking about security and privacy.

Organizations need to stop viewing security and privacy as problems that technologies can solve. They need to think about them as problems that people solve when they have the right enabling technologies. They need to adopt the set of business and security technologies that work for their needs while simultaneously recognizing that those needs will evolve as the business grows.

Data Protection: Incentivizing Not Penalizing

Compliance can be viewed as a necessary evil or a business enabler. Unfortunately, most compliance mandates penalize rather than incentivize. They exist because some companies refused to engage in the bare minimum security and privacy activities.

The organizations that internally incentivize security and privacy will be the ones to become leaders within their industry verticals. They will be the ones who reward workforce members who have good cyber hygiene. They will be the ones that effectively communicate with customers.

With internal data protection incentivized, these organizations will create the cultures of security that drive cybersustainability. They will see data protection as a fundamental part of everything they sell, regardless of whether they are business-to-business, business-to-consumer, product, or service model. These organizations will be the ones to derive revenue value from their data security, privacy, and compliance programs.

References

1. Scwab, K. (2016). *The Fourth Industrial Revolution*. New York: Currency.
2. Nash, J. (2022, February 9). *Avoid a Customer "Break Up" this Valentine's Day*. Retrieved from RedPoint Global: https://www.redpointglobal.com/blog/avoid-a-customer-break-up-this-valentines-day/
3. Cavoukian, A. (2011, January). *Privacy by Design the 7 Foundational Principles*. Retrieved from Information and Privacy Commissioner of Ontario:https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf
4. Halpern, R., & Tucker, C. (n.d.). Leveraging Adult Learning Theory with Online Learning ModulesLearning Modules. *Library Instruction West 2014*. https://pdxscholar.library.pdx.edu/cgi/viewcontent.cgi?article=1007&context=liw_portland: Portland State University.

Index