From Trunk Slammers to Guardians

How MSPs, MSSPs, and Cyber Counsel Can Lead the Way for Securing the Middle Market

Shawn E. Tuma

Visit Shawn's website: www.shawnetuma.com
Visit Shawn's Spencer Fane bio:
www.spencerfane.com/professionals/shawn-tuma/
Connect with Shawn on LinkedIn: www.linkedin.com/in/shawnetuma

Table Of Contents

Introduction

In today's digital landscape, cybersecurity has become a critical concern for organizations of all sizes, but small and mid-market companies face unique challenges in protecting their assets and data. These businesses often lack the extensive resources and expertise of larger corporations, making them attractive targets for cybercriminals. What makes it worse is they don't know what they don't know. They don't even know who they can trust that is qualified to tell them what they don't know or how to fix it. This is where I come in as I am sure you are already thinking, "why do I care what a lawyer has to say about cybersecurity?", right?

Why Would a Lawyer Write a Book Like This?

I am a practicing attorney and have been representing companies in cyber-related issues since 1999, after devoting years to preparing to become the world's leading expert on Y2K litigation. The plan was for the clock to strike Midnight on January 1, 2000, the world to come to a screeching halt, and I would spring into action as one of the rare and in-demand experts on Y2K law, propelling my career like a rocket ship to stardom and early retirement. I should have been retired and sitting on a beach somewhere a few decades ago. That was the plan, but I'm still around.

Unlike cybersecurity, Y2K was a technological problem that could be fixed with a technological solution. The problem was identified early enough, the world came together, and in one of the triumphs of our Age, we fixed the problem. The world did not come to a screeching halt, planes did not fall from the skies, there was very little (paying) demand for experts on Y2K law, my career rocket ship was a dud, and I had to adapt and focus on developing other areas of cyber-related law.

That led me to delve into issues like whether you could conduct business on or even have a contract over the Internet, which I studied and wrote scholarly articles about, had some courts cite my work, and it seemed promising. Then, in May of 2021, Texas adopted this thing called the Uniform Electronic Transactions Act which essentially said, "of course you can, move on," and there went that. By then, I had become known as the "tech lawyer" (albeit probably not in a good way) in a firm with hundreds of lawyers and I got pulled into a dispute that involved a healthcare provider and a whole bunch of patient medical records, the sensitivity of which nobody else seemed to appreciate. This led to my first work on a data breach situation.

For the next decade I spent my time working on the legal aspects of hacking, focusing heavily on the federal Computer Fraud and Abuse Act and analogous state laws, then as my understanding of hacking evolved and I developed a greater appreciation for the fact that for every "hack" there was usually someone's data involved and this brought me back to the data breach issue. In 2011, I wrote an article on whether that would be the Year of the Data Breach, and it wasn't, but 2013 was and from that time until now my practice has grown to be one hundred percent focused on cyber and privacy, and now, cyber, privacy, and AI focused.

Today, I work at the US-based law firm Spencer Fane, LLP, a full-service business law firm primarily works across the United States, and I lead a substantial team of attorneys that focus on cyber, data, privacy, and AI types of legal issues. Our team provides full service legal and advisory services on these issues. For my practice in particular, it can best be described as a general Outside Cyber Counsel role, providing legal and advisory services for all things cyber, privacy, AI, and technology-related, and can be broken down into three distinct areas:

- **Cyber Risk Management** – Proactively helping companies assess and understand their overall cyber risk and then developing, implementing, and maturing a strategic cyber risk management and compliance program that prioritizes their efforts to help minimize their cyber risk and meet practical, legal, and regulatory governance and compliance requirements, as well as advising on all aspects of cyber insurance.
- **Cyber Incident Response** – Leading companies through the cyber incident response and data breach response process as a cyber first-responder (e.g., as a "breach guide" or "breach quarterback"), crisis management, and regulatory compliance investigations and enforcement actions (e.g., by regulators such as various states' Attorneys General, Department of Health and Human Services / Office of Civil Rights (HHS/OCR), Federal Trade Commission (FTC), and Securities and Exchange Commission (SEC)). I also serve as a breach guide working with a few select insurance companies as approved panel counsel, working along with and overseeing the work of others' insurance provided counsel, as well as for self-insured companies.
- **Cybersecurity, Hacking, and Data Breach Litigation** – Representing clients in litigation involving cyber-related claims like computer and data misuse, computer hacking, data loss, data theft, and business to business disputes concerning responsibility for cyber incidents.

My ideal role is to serve as a member of a company's risk management team as general Outside Cyber Counsel to help the company proactively prepare for and minimize its risks of doing business in today's digital business world. Then, if a problem does

arise, I am there to guide the company through resolving those issues as well.

Throughout my career, I have served as a cyber first responder leading, advised on, and been a part of thousands of cyber incidents and hundreds of ransomware attack cases. When I refer to "incident response" cases, I am not referring to the routine type of incident response cases that companies, MSPs, and MSSPs deal with on a daily basis. I am referring to substantial events that have escalated well beyond routine incident response and either is or is on the verge of becoming a catastrophic crisis situation.

Candidly, I do not know how to operationally manage routine incident response for an organization. I also know, however, there are not many people working outside of the MSSP or Digital Forensics Incident Response (DFIR) firms that have similar experience with substantial incident response. That is why we make a great team! My goal is never to try and tell others how to do their job, it is only to be a part of the team and bring my perspective to bear on the situation, gained through my experience and strategic point of view, to be a part of the team and help companies understand– in the real-world that I see daily -- what risks they face, how to mitigate them, how to prepare for responding to them, and what to do if they find themselves in such a situation.

What is the Problem I am Trying to Solve?

If this isn't enough for you to care about what a lawyer has to say about cybersecurity, I have one more point that just may pique your interest. As I alluded to earlier, 2013 was a watershed moment in the world of data breach and the awareness that came with it was a tremendous boost for my business. But, do you know what else may be right up there in the top tier of things that have helped boost my business? Care to guess?

THE TRUNK SLAMMER!

Yep, it is "The IT Guy," or, the collection of "IT Guys" who see easy money to be made if they join up together, spin up a fancy website with a lot of slick graphics, complex tech-sounding gibberish, and wild promises that they have no intentions or abilities to keep – that is, the Trunk Slammer!

Just to make sure I am clear, I am not talking about the size of the providers. I know and regularly refer clients to some outstanding solo and small shop IT service providers who do a fabulous job and who I trust and respect. These people have a very valuable place in our ecosystem for the companies that need someone on their scale and level of affordability. Size or numbers is not what makes one The IT Guy or a Trunk Slammer!

No, I am talking about their abilities, their skills, their training, their experience, or any number of other intangibles that could go into making them qualified, or not qualified, to be in that very sensitive position of trust for their customers. These are not the people who would be putting in the time to read a book like this, these are not the people who would be attending conferences or reading professional publications to try and improve their skills, knowledge, and abilities to serve their customers.

The people I am talking about are the friend of a cousin of a brother-in-law who "does IT" and will come over and "do your network" on a Saturday evening for some cash and a 12 pack of beer. In fact, I feel so strongly about these people that for a few years now, after I would have to deal with them on a case, I would be so frustrated and need to vent on my blog with a series I called "***URGENT*** MEMO TO: "The IT Guy" that you can find here: https://shawnetuma.com/tag/the-it-guy-2/ These are just the few situations that I have written about but I could tell stories about them all day.

That is a big part of the problem that we face in trying to help companies – especially the small and mid-market companies – improve their cybersecurity posture: they do not know how to do it themselves, they do not know who they can trust to help them, and

when they are introduced to someone who says they can help, they do not know enough to be able to ask the right questions to even know if they are legitimate or not. You know this problem as well as or better than I do. That is why we are here.

What to Expect From this Book

This book, "From Trunk Slammers to Guardians: How MSPs, MSSPs, and Cyber Counsel Can Lead the Way for Securing the Middle Market," aims to address these challenges by exploring how we can do a better job of working together to help solve this problem.

First, let me make it clear that I do not claim to have all the answers. I don't. I continue to learn new things each day, and my ideas evolve as quickly as my perspective grows from new experiences. I view this as just a starting point for a dialogue about some areas where we can make a concerted effort to work together and use the power of collaboration between Managed IT Services Providers (MSPs), Managed IT Security Services Providers (MSSPs), and outside Cyber Counsel (Cyber Counsel) to help those companies that so desperately need qualified help.

The cybersecurity landscape is akin to an ongoing war, where defenders must constantly evolve their strategies to counter increasingly sophisticated attacks. As Willie Sutton, the notorious bank robber, once said when asked why he robbed banks, "Because that's where the money is." This sentiment rings true in the digital age, with cybercriminals primarily motivated by financial gain. They employ a variety of tactics, from direct theft and fraud to ransomware attacks and data extortion, targeting organizations across all sectors, with a particular focus on the small and mid-market companies because they know they are easy targets.

They know these small and mid-market companies are especially vulnerable because they often have fewer resources dedicated to cyber defense and many have this misguided belief that they are not targets because they are not big enough or well-known enough. Add to this the asymmetrical nature of cybersecurity, where defenders must be right 100% of the time while attackers need only one lucky shot, and this creates an especially daunting challenge for these companies.

Moreover, cybersecurity is not a static problem that can be solved with a one-time fix. Unlike technical glitches such as Y2K, cybersecurity requires continuous adaptation and evolution. As organizations implement new defenses, cybercriminals respond by changing tactics and finding new ways to circumvent these measures. This dynamic nature of the threat landscape means that there is no such thing as being completely secure, and even robust security measures have a limited shelf life and no guarantees.

While this reality may seem disheartening, it is crucial for organizations to have a realistic understanding of the challenges they face. Only by acknowledging the true nature of the cybersecurity landscape can businesses effectively fulfill their responsibilities to customers, employees, and stakeholders. This book aims to provide that understanding and offer practical strategies for how we can work together to help them become harder targets and more resilient in the face of cyber threats.

Drawing from my extensive experience as breach counsel, advising on thousands of cyber incidents and hundreds of ransomware attacks, I try to offer my unique insights and perspective into common pitfalls and effective strategies for that we as a team can help offer to these companies to truly help them. Rather than simply reiterating standard security controls, which we all know are critical must-haves, I try to provide a strategic perspective that complements and enhances technical approaches to cybersecurity.

Throughout this book, I will explore how the collaboration between MSPs, MSSPs, and Cyber Counsel can significantly enhance a company's cybersecurity posture. This synergy brings together technical expertise, security specialization, and legal guidance, and strategic risk management perspectives based on real-world experience to create a comprehensive approach to cybersecurity that is particularly beneficial for small and mid-market companies.

Key topics covered in this book include:

1. Understanding the evolving cybersecurity landscape and the motivations of cybercriminals
2. Conducting comprehensive risk assessments and developing effective mitigation strategies
3. Implementing robust data governance and protection measures
4. Navigating the legal considerations in cybersecurity, including compliance and contractual obligations
5. Managing vendor risks and ensuring business continuity
6. Building a team-oriented approach to cybersecurity within the organization
7. Establishing a continuous process for adapting and improving cybersecurity measures
8. Learning from real-world cyber incidents and ransomware attacks
9. Understanding cyber insurance, the role of cyber insurance in mitigating financial risks, and how to effectively use cyber insurance with incident response preparation and execution

By the end of this book, readers should have a good understanding of how MSPs, MSSPs, and Cyber Counsel can work together to create a robust cybersecurity program that is uniquely tailored to the company to provide the greatest balance between effectiveness and feasibility. This collaborative approach will enable small and mid-market companies to better protect their assets and operations, comply with regulations, and effectively prepare for and respond to cyber threats in an ever-changing digital landscape.

Chapter 1: Understanding the Cybersecurity Landscape

In today's rapidly evolving digital world, the cybersecurity landscape presents a complex and ever-changing battlefield. Small and mid-market companies face unprecedented challenges in protecting their assets, data, operations, and reputation from increasingly sophisticated cyber threats. This chapter aims to provide an overview of the current cybersecurity environment, the nature of cyber threats, and the unique challenges faced by smaller organizations.

As a lawyer I am often asked, “what is reasonable cybersecurity?” My response is, “reasonable cybersecurity is a process, not a definition,” and here is why. First, every company’s risks are unique – no two companies’ risks or appropriate security solutions are alike. The only way to determine what is appropriate security for a company is to understand the company’s own unique risks, which starts with the risk assessment. How can you protect against what you don’t understand? Second, the cybersecurity landscape is characterized by its dynamic and asymmetrical nature. Cyber criminals are continuously adapting their tactics, techniques, and procedures (TTPs) to exploit new vulnerabilities and circumvent existing security measures. This constant evolution means that what was considered

secure yesterday may be vulnerable today. This means you must have a process for continually assessing your risks, the risk environment, and understanding how it is evolving and that process must be ongoing and never end. For small and mid-market companies, this presents a significant challenge, as they often lack the resources and expertise to keep pace with these rapid changes. That is where those of us engaged on the front lines of this battle daily can help.

One of the fundamental concepts in understanding the cybersecurity landscape is the cyber kill chain. Developed by Lockheed Martin, the cyber kill chain is a model that describes the stages of a cyberattack, from initial reconnaissance to the final objective. These stages typically include:

1. Reconnaissance: Gathering information about the target
2. Weaponization: Preparing malware or other attack tools
3. Delivery: Transmitting the weapon to the target
4. Exploitation: Triggering the malicious payload
5. Installation: Installing malware on the target system
6. Command and Control: Establishing remote access to the compromised system
7. Actions on Objectives: Achieving the attacker's goals, such as data exfiltration or system disruption

Understanding this model is crucial for organizations as it helps in developing comprehensive defense strategies that address each stage of a potential attack.

The asymmetrical nature of cybersecurity presents another significant challenge. Defenders must protect against all possible attack vectors and secure every potential vulnerability, while attackers only need to find a single weak point to exploit. This imbalance is often described as the defenders needing to be right 100% of the time, while attackers only need one lucky shot to be successful. For small and mid-market companies with limited resources, this asymmetry can be particularly daunting.

Cyber criminals are primarily motivated by financial gain, employing a variety of tactics to achieve their financial objectives:

1. Direct theft: Attempting to steal money directly from accounts or financial systems
2. Fraud: Using stolen information to commit financial fraud
3. Ransomware: Encrypting critical data and demanding payment for its release
4. Data extortion: Stealing sensitive data and threatening to publish or sell it unless a ransom is paid

Small and mid-market companies are particularly vulnerable to these attacks. Cyber criminals often target these organizations because they typically have fewer resources dedicated to cybersecurity, making them potentially easier targets. However, the impact of a successful attack on a smaller company can be devastating, potentially leading to significant financial losses, reputational damage, or even business failure.

For small and mid-market companies, this reality underscores the importance of adopting a proactive and adaptive approach to cybersecurity – the process. It requires ongoing investment in technology, processes, and people to stay ahead of evolving threats. The problem is, they don't know what they don't know, and they don't know who they can trust to give them good advice on where to even begin. This is where the collaboration between MSPs, MSSPs, and Cyber Counsel becomes crucial.

MSPs can provide the technical expertise needed to maintain and secure IT infrastructure, while MSSPs offer specialized security services such as threat detection, incident response, and security monitoring. Cyber Counsel helps provide practical, real-world insight to the risks companies face as well as valuable insights into the governance, risk, and compliance processes, and provides guidance on legal and regulatory requirements, helping organizations navigate the complex landscape of data protection laws and industry-specific regulations.

By leveraging the combined expertise of these partners, small and mid-market companies can enhance their cybersecurity posture,

despite resource limitations. This collaborative approach allows organizations to benefit from:

1. Up-to-date threat intelligence and security best practices
2. Continuous monitoring and rapid incident response capabilities
3. Compliance with relevant laws and regulations
4. Strategic guidance on cybersecurity investments and risk management

Understanding the cybersecurity landscape is the first step in developing an effective defense strategy. By recognizing the dynamic and asymmetrical nature of cyber threats, the motivations of cyber criminals, and the unique challenges faced by small and mid-market companies, organizations can begin to build a resilient cybersecurity posture. The key lies in adopting a realistic view of the challenges, embracing continuous adaptation, and leveraging the expertise of MSPs, MSSPs, and Cyber Counsel to create a comprehensive and effective cybersecurity program.

Chapter 2: Risk Assessment and Mitigation

In the complex landscape of cybersecurity, risk assessment and mitigation form the cornerstone of an effective risk management strategy. For small and mid-market companies, understanding and managing cyber risks is crucial to protecting their assets, reputation, and business continuity. Because every single company's risks are unique and you can't protect against what you do not understand, the risk assessment process is one of the most critical steps. This chapter explores how MSPs, MSSPs, and Cyber Counsel can collaborate to conduct comprehensive risk assessments and develop effective mitigation strategies.

The process of risk assessment begins with a thorough evaluation of the organization's IT infrastructure, network, and systems. MSPs play a critical role in this stage by leveraging their technical expertise to identify vulnerabilities and potential threats. They can perform vulnerability scans, penetration testing, and security audits to uncover weaknesses in the company's defenses. These assessments provide valuable insights into the technical aspects of the organization's cybersecurity posture.

MSSPs bring specialized security knowledge to the table, focusing on evaluating the overall cybersecurity posture of the organization. They can assess the effectiveness of existing security controls, analyze the organization's security policies and procedures, and evaluate employee training programs. MSSPs can also provide insights into industry-specific threats and compliance requirements, such as those mandated by the General Data Protection Regulation (GDPR), California Privacy Rights Act (CPRA), the Payment Card Industry Data Security Standard (PCI DSS), or litany of other regulatory compliance requirements.

Cyber Counsel plays a crucial role in the risk assessment process by providing guidance on legal and regulatory requirements as well as calling on their practical experience in dealing with real-world cyber incidents and how they impact companies. They can help identify compliance obligations specific to the organization's industry and geographic location. This legal perspective is essential for understanding the potential legal and financial consequences of cybersecurity incidents and ensuring that risk mitigation strategies align with legal obligations. Of perhaps greater importance, however, by calling on decades of experience in serving as a breach quarterback (guide, coach, first-responder) leading companies through the cyber incident investigation, recovery, and response process in thousands of

cyber incidents and hundreds of ransomware attacks, Cyber Counsel provides insights into the real-world causes of those incidents, what companies could have done to prevent them, and what the impact was on the companies. This is practical, actionable guidance for helping companies facing similar threats understand their own unique risks.

The collaboration between these three entities allows for a holistic approach to risk assessment. By combining technical, security, and legal expertise, organizations can gain a comprehensive understanding of their cybersecurity risks. This multifaceted approach ensures that all aspects of risk are considered, from technical vulnerabilities to legal compliance to real-world practical risks issues.

Once risks have been identified, the next step is to prioritize mitigation efforts. This is where the collaborative effort truly shines. MSPs can provide insights into the technical feasibility and cost of implementing various security controls. MSSPs can offer recommendations on the most effective security measures based on current threat intelligence and industry best practices. Cyber Counsel can advise on the legal implications of different mitigation strategies and ensure that proposed measures align with regulatory requirements and provide their real-world practical perspective to cyber risk and how it should be managed.

Together, these experts can help the organization develop a risk mitigation plan that balances security needs with business objectives and legal obligations. This plan may include a range of measures, such as:

1. Implementing advanced security technologies, such as next-generation firewalls, intrusion detection systems, and endpoint protection solutions.
2. Developing and enforcing robust security policies and procedures.
3. Conducting regular employee training and awareness programs.
4. Implementing data encryption and access control measures.
5. Establishing incident response and business continuity plans.
6. Regularly updating and patching systems and applications.

The collaborative approach also extends to the implementation and monitoring of these mitigation measures. MSPs can take charge of implementing technical controls and managing IT infrastructure. MSSPs can provide ongoing security monitoring, threat detection, and incident response services. Cyber Counsel can ensure that all measures are implemented in compliance with legal requirements and can assist in drafting necessary documentation and policies.

Furthermore, the risk assessment and mitigation process should be viewed as an ongoing cycle rather than a one-time event. Cyber threats are constantly evolving, and new vulnerabilities emerge

regularly. The collaboration between MSPs, MSSPs, and Cyber Counsel allows for continuous monitoring and adaptation of the organization's cybersecurity posture.

MSPs can provide regular updates on the state of the IT infrastructure and any new vulnerabilities discovered. MSSPs can offer ongoing threat intelligence and security monitoring, alerting the organization to new threats or attack vectors. Cyber Counsel can keep the organization informed about changes in legal and regulatory requirements that may impact their cybersecurity obligations as well as current threats they are seeing impacting similar businesses in their incident response work.

This ongoing collaboration ensures that the organization's risk assessment and mitigation strategies remain current and effective. It allows for rapid response to new threats and ensures that the organization's cybersecurity measures evolve in tandem with the changing threat landscape.

The collaboration between MSPs, MSSPs, and Cyber Counsel provides small and mid-market companies with a powerful framework for risk assessment and mitigation. By leveraging the diverse expertise of these partners, organizations can develop comprehensive, effective,

and legally compliant cybersecurity strategies. This collaborative approach not only enhances the organization's security posture but also provides a competitive advantage in an increasingly digital business environment.

Chapter 3: Data Governance and Protection

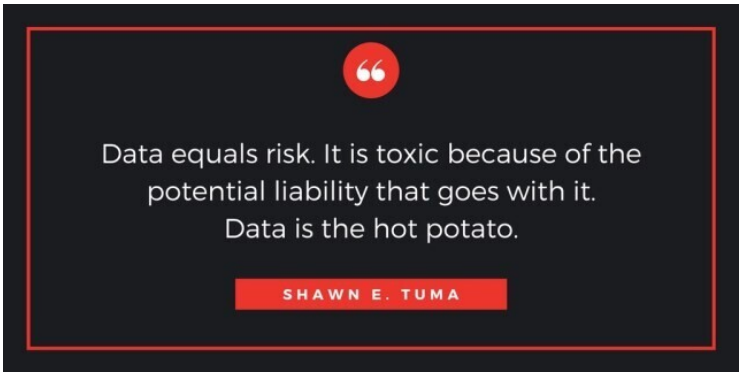
In today's digital landscape, data has become one of the most valuable assets for organizations of all sizes. For small and mid-market companies, protecting customer and employee data is not just a matter of good business practice; it's a critical component of their cybersecurity strategy and legal compliance obligations. This chapter explores the importance of data governance and protection, and how the collaboration between MSPs, MSSPs, and Cyber Counsel can help organizations effectively manage and secure their data.

“Data is the hot potato!” is one of my favorite sayings about cybersecurity and data protection. When doing presentations, I love to have the attendees chant over and over in unison, “Data is the hot potato! Data is the hot potato! Data is the hot potato!”

I introduce my professional bio by saying “Shawn Tuma helps businesses protect their information and protect themselves from their information.” On more than one occasion I have had

experienced data protection professionals who have used this bio to introduce me at events think that was a typo and did not understand what it means. But you understand my point, right?

Data equals risk. It is toxic because of the potential liability that goes with it. Data is the hot potato. When we are talking about the legal aspects of cybersecurity and data protection — the ball we usually need to keep our eye on is the data — that's what really matters.



Other than some very recent regulatory reporting obligations that the SEC implemented for public companies at the end of 2023, and that CISA is on the verge of finalizing, generally speaking, when legislators, regulators, judges, and plaintiff's lawyers talk about cybersecurity and data protection, they don't really care all that much about the security of a company's network for the company's network's sake — they care about the security of the data that is stored within or that transgresses

throughout that network — especially when that data is other people's personal information — that is what they really care about and that is where we usually need to stay focused (unless, of course, the company is in an industry with legal and regulatory requirements focusing elsewhere, which needs to be understood).

In fact, one of the most inexpensive and effective tools companies can use to exponentially reduce their potential liability exposure is likely already available to them and they just do not know it: their Data Destruction and Data Retention Policy! Most companies have one, they just do not vigorously follow and enforce it. But think about it, if data equals risk, as it does, the best way to reduce that risk is to either not collect data that is not needed or, when data is no longer needed, securely destroy it or securely archive it off of the network so it cannot be accessed by threat actors.

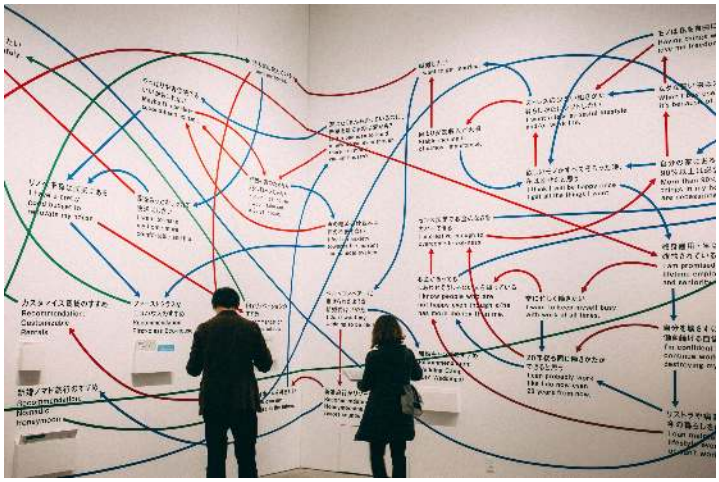
Did you notice how in a few paragraphs up I not only mentioned customer data, but also employee data? That is because in many of the data breach cases we handle, when we first talk with the client about potential exposure, the first thing they want to tell us is that they do not collect or maintain customer data. Or, that they are a business-to-business company that does not have consumer data, and that is when we have to remind them that just like all other companies, they have

employee data. Not only current employee data, but also sometimes very old archives of former employees' data, including the data of former employees who were terminated in the past and have had an axe to grind with the company ever since, just waiting for their opportunity to get their pound of flesh out of the company.

Do you want to guess who we see bring plaintiff's class action lawsuits most often following a data breach notification to individuals impacted? Yep, you guessed right: former employees who were terminated from the company who know other former disgruntled employees and are able to join together and contact a plaintiff's attorney to form a "class" to bring a class action lawsuit. That is why good data governance is critical for all companies, regardless of size or industry.

Data governance refers to the overall management of the availability, usability, integrity, and security of data within an organization. It encompasses the strategies, policies, and technologies used to ensure that data is accurate, consistent, and protected throughout its lifecycle. For small and mid-market companies, implementing robust data governance practices is essential for maintaining customer trust, complying with regulations, and mitigating the risks associated with data breaches.

The first step in effective data governance is understanding what data the organization holds. We often call this a Data Map and, when I ask new small or mid-market clients if they have one, they look at me like I'm speaking in a foreign language and are overwhelmed by the imagined complexity of something as sophisticated sounding as a "Data Map."



Then I explain to them that it doesn't have to be fancy, I don't care what it looks like, and I really don't care what they call it – we just need to know what data they collect, that transgresses through, and that is maintained in the network and where it is. Then, however, they often come back and say, "well how am I supposed to know that?" to which I respond, "well, how am I supposed to know that, I'm not clairvoyant!"

I then explain to them the bottom line which is that they are asking us for help with their cyber and data governance, risk management, and compliance obligations and that process is driven by their data and, without understanding their data, we can't really do an effective job. That means we need to drop all the pretentious sounding terminology and make sure they can figure out their data.

Ultimately, this involves conducting a comprehensive data inventory and classification exercise. MSPs can play a crucial role in this process by leveraging their technical expertise to identify where data is stored across the organization's IT infrastructure, including on-premises systems, cloud services, and mobile devices. They can use data discovery tools to scan networks and systems, identifying sensitive information such as personally identifiable information (PII), financial data, or intellectual property.

MSSPs can contribute to this process by assessing the security controls surrounding the identified data. They can evaluate access controls, encryption measures, and data loss prevention (DLP) solutions to ensure that sensitive information is adequately protected. This assessment helps identify potential vulnerabilities and areas where additional security measures may be needed.

Cyber Counsel plays a critical role in the data classification process by providing guidance on legal and regulatory requirements as well as the process for developing, implementing, and maturing governance, risk management, and compliance programs. They can help the organization understand which data elements are subject to specific regulations, such as the General Data Protection Regulation (GDPR)

for personal data of EU residents or the California Privacy Rights Act (CPRA) for California consumers. This legal perspective ensures that the data classification aligns with regulatory obligations and helps prioritize protection efforts.

Once data has been identified and classified, the next step is implementing data minimization strategies. The principle of data minimization involves collecting and retaining only the data that is necessary for specific business purposes. This approach not only reduces the organization's risk exposure but also aligns with many data protection regulations.

MSPs can assist in implementing technical controls to enforce data minimization policies. This may involve configuring systems to automatically delete or archive data after a specified retention period or implementing data masking techniques to limit exposure of sensitive information. MSSPs can provide ongoing monitoring to ensure that these controls are functioning effectively and that no unauthorized data collection or storage is occurring.

As mentioned above, Cyber Counsel can advise on the legal implications of data retention policies and help draft appropriate data retention schedules. They can ensure that the organization's data minimization practices comply with legal requirements while still meeting business needs.

Secure data handling practices are essential for protecting sensitive information throughout its lifecycle. This includes implementing encryption for data at rest and in transit, establishing secure data transfer protocols, and ensuring proper access controls. MSPs can implement and manage these technical controls, while MSSPs can provide ongoing monitoring and testing to ensure their effectiveness.

Cyber Counsel can advise on the legal requirements for data protection, such as encryption standards mandated by specific regulations. They can also help draft data handling policies and procedures that align with legal obligations and industry best practices.

Data backup and disaster recovery strategies are critical components of data protection. MSPs can implement robust backup solutions, ensuring that data is regularly backed up and can be quickly restored in the event of a system failure or cyber incident. MSSPs can assess the security of these backup systems and ensure that they are protected against potential cyber threats.

Cyber Counsel can provide guidance on legal requirements for data retention and recovery, ensuring that backup strategies align with regulatory obligations. They can also advise on the legal implications of data loss and help develop incident response plans that address data recovery procedures and lead tabletop training exercises.

Secure data disposal is another crucial aspect of data governance. When data is no longer needed, it must be securely deleted or destroyed to prevent unauthorized access. MSPs can implement technical solutions for secure data erasure, while MSSPs can verify that disposal processes meet security standards.

Cyber Counsel can advise on legal requirements for data disposal, such as specific methods mandated by regulations. They can also help develop policies and procedures for secure data disposal that comply with legal obligations.

Through all these data governance and protection efforts, the collaboration between MSPs, MSSPs, and Cyber Counsel is essential. MSPs provide the technical expertise to implement and manage data protection solutions. MSSPs offer specialized security knowledge to assess and monitor data protection measures. Cyber Counsel ensures that all data governance practices align with legal and regulatory requirements.

This collaborative approach allows small and mid-market companies to develop comprehensive data governance strategies that not only protect their valuable data assets but also ensure compliance with complex and evolving data protection regulations. By leveraging the

combined expertise of these partners, organizations can build a robust data protection framework that enhances their overall cybersecurity posture and helps maintain the trust of their customers and employees.

Effective data governance and protection require a multifaceted approach that addresses technical, security, and legal considerations. The collaboration between MSPs, MSSPs, and Cyber Counsel provides small and mid-market companies with the expertise needed to navigate this complex landscape, ensuring that their data remains secure, compliant, and available to support their business objectives.

Chapter 4: Legal Considerations in Cybersecurity

In today's complex digital landscape, cybersecurity is not merely a technical issue but a critical legal concern for all companies, especially small and mid-market companies. This chapter explores the intricate legal considerations in cybersecurity and how the collaboration between MSPs, MSSPs, and outside Cyber Counsel can help organizations navigate this complex terrain.

Recognizing cybersecurity as a legal issue is the first step in developing a comprehensive defense strategy. Cyber incidents can have far-reaching legal implications, including potential lawsuits, regulatory fines, and reputational damage. For small and mid-market companies, understanding and complying with the myriad of laws and regulations governing cybersecurity and data protection is crucial. This is where the expertise of outside Cyber Counsel becomes invaluable.

Cyber Counsel can provide guidance on a wide range of legal and regulatory requirements that impact an organization's cybersecurity practices. These may include industry-specific regulations such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare organizations, the Gramm-Leach-Bliley Act (GLBA) for financial institutions, or broader data protection laws like the General Data Protection Regulation (GDPR) for companies handling data of EU residents or the California Privacy Rights Act (CPRA) for those dealing with California consumers' data.

The collaboration between MSPs, MSSPs, and Cyber Counsel is crucial in ensuring that technical security measures align with legal requirements. For instance, when implementing data encryption or access control measures, MSPs and MSSPs can work closely with legal counsel to ensure that these technical controls meet the specific standards outlined in relevant regulations.

One of the key areas where this collaboration proves invaluable is in the development of cybersecurity policies and procedures. Cyber Counsel can draft comprehensive policies that not only address technical security measures but also incorporate legal compliance requirements. MSPs and MSSPs can then provide input on the technical feasibility of implementing these policies and help translate legal requirements into practical, actionable steps for the organization's IT team.

Contracts play a significant role in governing cybersecurity obligations and liability allocation. Cyber Counsel can review and negotiate contracts with vendors, customers, and partners to ensure that appropriate cybersecurity provisions are included. These may cover areas such as data protection responsibilities, breach notification requirements, and liability limitations. MSPs and MSSPs can provide valuable input on the technical aspects of these contractual obligations, ensuring that the organization can realistically meet its commitments.

In the event of a data breach or cyber incident, the collaboration between these parties becomes even more critical. Experienced Cyber Counsel plays a crucial role by calling on decades of experience in serving as a breach quarterback (guide, coach, first-responder) gained from leading companies through the cyber incident investigation,

recovery, and response process in thousands of cyber incidents and hundreds of ransomware attacks, to provide leadership and strategic insights into the real-world process and logistics required for having a coordinated team execute an effective and efficient investigation, recovery, and response. This includes Cyber Counsel guiding the organization through the legal aspects of incident response, including breach notification requirements, communication strategies, and potential legal liabilities. MSPs and MSSPs can focus on the technical aspects of containing and mitigating the incident, while ensuring that their actions align with legal requirements and preserve evidence for potential investigations.

The development of incident response plans is another area where this collaboration shines. Cyber Counsel can outline the practical, logistical, and legal steps that need to be taken in the event of a breach, while MSPs and MSSPs can develop the technical response procedures. Together, they can create a comprehensive incident response plan that addresses both legal and technical aspects of cyber incidents and test these through tabletop exercises.

Compliance monitoring is an ongoing process that benefits greatly from this collaborative approach. Cyber Counsel can keep the organization informed about changes in laws and regulations that

may impact their cybersecurity obligations. MSPs and MSSPs can then implement the necessary technical controls and monitoring systems to ensure ongoing compliance.

Employee training and awareness programs are essential components of a robust cybersecurity strategy. Here, Cyber Counsel can provide content on legal obligations and the potential consequences of non-compliance, while MSPs and MSSPs can deliver technical training on security best practices and threat recognition.

The legal considerations in cybersecurity are complex and ever-evolving. By fostering collaboration between MSPs, MSSPs, and outside Cyber Counsel, small and mid-market companies can develop a comprehensive approach to cybersecurity that not only protects their technical infrastructure but also ensures legal compliance and mitigates potential legal risks. This collaborative approach allows organizations to leverage the unique expertise of each party, resulting in a more robust and legally sound cybersecurity posture.

Chapter 5: Vendor Risk Management

In today's interconnected business environment, vendor risk management has become a critical component of an organization's overall cybersecurity strategy. For small and mid-market companies, the risks associated with third-party service providers can be particularly significant, as these organizations often rely heavily on external vendors for various aspects of their operations. This chapter explores how MSPs, MSSPs, and Cyber Counsel can collaborate to help companies effectively manage vendor risks and enhance their cybersecurity posture.

The first step in effective vendor risk management is ensuring the parties understand the need for a comprehensive assessment and providing the legal right to conduct such an assessment, especially when it involves evaluating a third party's network. Cyber Counsel plays a vital role in this process in multiple ways. First, they can ensure all parties understand the legal requirements for engaging in this process at the outset. Next, they can ensure that the company abides by and has the legal rights to comply with the general requirements of investigating the third parties' cyber risk prior to entering into the relationship, obligating them to meet certain standards, and auditing them to ensure they are complying with such obligations. This is all

accomplished through the contracts between the parties. Cyber Counsel either assists with the negotiation of such contracts or reviewing the contracts to ensure these objectives are satisfied. Next and more generally, they can ensure that contracts include appropriate security and privacy clauses, define breach notification requirements, and assign responsibilities for data protection. This legal review is crucial for establishing clear expectations and legal protections for the organization.

The next step is conducting a comprehensive assessment of the risks associated with third-party service providers. This process begins with identifying all vendors that have access to the organization's systems, networks, or sensitive data. MSPs can play a crucial role in this initial phase by leveraging their technical expertise to map out the organization's IT infrastructure and identify all points of vendor integration.

Once vendors have been identified, MSSPs can contribute their specialized security knowledge to evaluate the cybersecurity posture of each vendor. This may involve conducting technical assessments, such as vulnerability scans or penetration testing, to identify potential weaknesses in the vendor's systems. MSSPs can also review the vendor's security policies, procedures, and certifications to ensure they meet the organization's security standards.

Developing strategies to ensure business continuity in the event of a service provider breach or disruption is another critical aspect of vendor risk management. MSPs can contribute to this effort by designing and implementing redundancy measures and backup systems that can be activated if a key vendor experiences an outage or security incident. MSSPs can develop incident response plans that specifically address vendor-related security events, ensuring a rapid and coordinated response to any potential breaches.

Implementing contractual safeguards and security requirements for vendors is an area where the collaboration between Cyber Counsel and technical experts is particularly valuable. Cyber Counsel can draft contract language that outlines specific security requirements, while MSPs and MSSPs can provide input on the technical feasibility and appropriateness of these requirements. This collaboration ensures that contractual obligations are both legally sound and technically achievable.

Ongoing monitoring of vendor activities is crucial for maintaining a strong security posture. MSSPs can provide continuous monitoring services, using advanced threat detection tools to identify any suspicious activities originating from vendor connections. MSPs can assist by implementing and managing access controls and network segmentation to limit vendor access to only the necessary systems and data.

Regular vendor security assessments are essential for identifying and mitigating emerging risks. MSPs and MSSPs can collaborate to conduct periodic technical assessments of vendor systems, including vulnerability scans, penetration testing, and security audits. These assessments can help identify any new vulnerabilities or security gaps that may have emerged since the initial evaluation.

Cyber Counsel can contribute to this ongoing process by regularly reviewing and updating vendor contracts to ensure they remain aligned with evolving legal and regulatory requirements. They can also provide guidance on how to address any compliance issues that may arise during vendor security assessments.

In the event of a vendor-related security incident, the collaboration between MSPs, MSSPs, and Cyber Counsel becomes even more critical. MSPs and MSSPs can focus on the technical aspects of incident response, such as containing the breach, mitigating its impact, and restoring affected systems. Cyber Counsel can guide the organization through the legal implications of the incident, including breach notification requirements and potential liability issues.

Education and training are also key components of effective vendor risk management. MSPs and MSSPs can provide technical training to the organization's staff on best practices for working with vendors securely. This may include guidance on secure file sharing, proper

access management, and recognizing potential security risks. Cyber Counsel can contribute by educating staff on the legal aspects of vendor relationships, including confidentiality obligations and data protection requirements.

Effective vendor risk management requires a multi-faceted approach that combines technical expertise, security specialization, and legal guidance. By fostering collaboration between MSPs, MSSPs, and Cyber Counsel, small and mid-market companies can develop a comprehensive vendor risk management program that enhances their overall cybersecurity posture. This collaborative approach allows organizations to leverage the unique strengths of each party, resulting in more robust vendor security assessments, stronger contractual protections, and more effective incident response capabilities. By implementing these strategies, companies can significantly reduce the risks associated with third-party vendors and build more resilient business operations.

Chapter 6: Building a Team-Oriented Approach to Cybersecurity

In today's complex cybersecurity landscape, a team-oriented approach is essential for small and mid-market companies to effectively manage and mitigate cyber risks. This chapter explores how MSPs, MSSPs, and outside Cyber Counsel can collaborate with internal teams to create a comprehensive and robust cybersecurity strategy.

Recognizing cyber risk as an organizational risk is the first step in building a team-oriented approach. Cybersecurity is not just an IT issue; it affects every aspect of an organization, from operations and finance to legal and human resources. By acknowledging this, companies can foster a culture of shared responsibility and collaboration across all departments.

The core of a successful team-oriented approach is the identification and engagement of key team members from various departments. This typically includes representatives from:

1. Information Security
2. Information Technology
3. Legal
4. Compliance
5. Privacy
6. Audit
7. Risk Management
8. Operations
9. Human Resources
10. Communications

Each of these team members brings a unique perspective and expertise to the table, contributing to a more comprehensive understanding of the organization's cybersecurity needs and challenges.

MSPs play a crucial role in this collaborative approach by providing technical expertise and support. They can work closely with the internal IT team to implement and maintain robust security measures, conduct regular system updates and patches, and monitor the organization's IT infrastructure for potential vulnerabilities. MSPs can also assist in translating technical jargon into language that non-technical team members can understand, facilitating better communication across the organization.

MSSPs bring specialized security knowledge to the team. They can provide advanced threat detection and response capabilities, conduct regular security assessments, and offer guidance on emerging threats and best practices. MSSPs can work closely with the internal information security team to develop and implement a comprehensive security strategy that aligns with the organization's risk profile and business objectives.

Experienced Cyber Counsel plays a crucial role by providing guidance on legal and regulatory requirements as well as calling on their practical experience in dealing with real-world cyber incidents and how they impact companies. They can help identify compliance obligations specific to the organization's industry and geographic location. This legal perspective is essential for understanding the potential legal and financial consequences of cybersecurity incidents and ensuring that risk mitigation strategies align with legal obligations.

Of perhaps greater importance, however, by calling on decades of experience in serving as a breach quarterback (guide, coach, first-responder) leading companies through the cyber incident investigation, recovery, and response process in thousands of cyber incidents and hundreds of ransomware attacks, Cyber Counsel

provides insights into the real-world causes of those incidents, what companies could have done to prevent them, and what the impact was on the companies. This is practical, actionable guidance for helping companies facing similar threats understand their own unique risks.

Promoting cross-functional collaboration and information sharing is key to the success of this team-oriented approach. Regular meetings and workshops can be organized where MSPs, MSSPs, and Cyber Counsel can share their insights and expertise with the internal team. These sessions can cover topics such as:

1. Recent threat intelligence and emerging cyber risks
2. Updates on relevant laws and regulations
3. Best practices for incident response and business continuity
4. Employee training and awareness programs

Establishing clear roles and responsibilities for each team member is crucial for effective collaboration. This includes defining:

1. Who has decision-making authority in various cybersecurity matters
2. Who is responsible for implementing and maintaining security controls
3. Who should be notified in the event of a security incident
4. Who is responsible for coordinating with external partners (MSPs, MSSPs, and Cyber Counsel)

MSPs and MSSPs can assist in defining these roles by providing insights into industry best practices and helping to develop clear communication channels and escalation procedures.

Cyber Counsel can contribute to this process by ensuring that roles and responsibilities are clearly documented and align with legal and regulatory requirements. They can also help draft internal policies and procedures that outline these roles and responsibilities.

To further enhance collaboration, organizations can consider implementing a Cyber Risk Committee. This Committee, comprising key internal team members along with representatives from the MSP, MSSP, and Cyber Counsel, can meet regularly to discuss cybersecurity strategy, review incident reports, and make decisions on major security initiatives.

Regular tabletop exercises and simulations, facilitated by MSPs, MSSPs, and Cyber Counsel, can help test and refine the team's collaborative approach. These exercises can simulate various cyber incidents, allowing the team to practice their response and identify areas for improvement. Cyber Counsel can lead these exercises to provide real-time legal guidance and ensure that the response aligns with legal and regulatory requirements as well as share customary practices and insights gained through guiding companies through thousands of cyber incidents and hundreds of ransomware attacks.

Building a team-oriented approach to cybersecurity requires the active participation and collaboration of internal teams, MSPs, MSSPs, and Cyber Counsel. By leveraging the diverse expertise of these stakeholders, small and mid-market companies can develop a more comprehensive and effective cybersecurity strategy. This collaborative approach not only enhances the organization's ability to prevent and respond to cyber threats but also fosters a culture of cybersecurity awareness throughout the organization.

Chapter 7: Continuous Process and Adaptation

In the ever-evolving landscape of cybersecurity, small and mid-market companies must recognize that effective protection requires an ongoing and continuous process. This chapter explores how MSPs, MSSPs, and Cyber Counsel can collaborate to help organizations develop and maintain a robust, adaptive cybersecurity strategy.

The foundation of a successful continuous cybersecurity process lies in implementing a recognized framework. The National Institute of Standards and Technology (NIST) Cybersecurity Framework and ISO 27001 are two widely adopted standards that provide a structured approach to managing cybersecurity risks, though there are other popular ones as well. MSPs, MSSPs, and Cyber Counsel all play a crucial role in helping organizations implement these frameworks by:

1. Conducting initial assessments to determine the organization's current cybersecurity posture
2. Developing a roadmap for implementing the chosen framework
3. Assisting in the implementation of technical controls and processes
4. Providing ongoing monitoring and reporting to track progress and compliance

Cyber Counsel contributes to this process by ensuring that the implemented framework aligns with relevant legal and regulatory requirements. They can review the organization's policies and procedures to ensure they meet legal standards and help draft any necessary documentation required by the chosen framework.

Regular assessment and updating of security controls is another critical aspect of the continuous cybersecurity process. MSPs and MSSPs can provide valuable services in this area, including:

1. Conducting regular vulnerability scans and penetration testing
2. Implementing and managing patch management processes
3. Reviewing and updating access controls and user privileges
4. Monitoring for new threats and vulnerabilities that may impact the organization

Cyber Counsel can contribute by providing regular updates about changes in the threat environment we are seeing through our ongoing incident response work as well as keeping the team informed about changes in laws and regulations that may require updates to the organization's security controls or policies. They can work with MSPs and MSSPs to ensure that any changes to security controls are documented and comply with legal requirements.

Staying ahead of cyber criminals requires continuous adaptation and the leveraging of emerging technologies. MSPs and MSSPs can help organizations in this endeavor by:

1. Providing threat intelligence services to keep the organization informed about emerging threats
2. Recommending and implementing new security technologies as they become available
3. Offering advanced security services such as Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR)
4. Conducting regular security awareness training for employees to keep them informed about new threats and best practices

Cyber Counsel can assist by reviewing contracts for new security technologies and services, ensuring that they comply with data protection laws and other relevant regulations. They can also help develop and review policies related to the use of new technologies within the organization.

Fostering a culture of cybersecurity awareness is essential for maintaining an effective continuous cybersecurity process. MSPs, MSSPs, and Cyber Counsel can collaborate to develop comprehensive training programs that cover both technical and legal aspects of cybersecurity. This might include:

1. Regular phishing simulations conducted by MSPs or MSSPs
2. In-person or online training sessions on cybersecurity best practices
3. Legal training on data protection laws and regulatory compliance
4. Executive-level briefings on cybersecurity risks and responsibilities

To ensure the effectiveness of the continuous cybersecurity process, it's important to establish regular communication and collaboration between MSPs, MSSPs, and Cyber Counsel. This can be achieved through:

1. Monthly or quarterly security review meetings
2. Joint development of cybersecurity strategies and roadmaps
3. Collaborative incident response planning and testing
4. Shared access to relevant threat intelligence and legal updates

Maintaining an effective cybersecurity posture requires a continuous, collaborative effort between the organization, MSPs, MSSPs, and Cyber Counsel. By leveraging the technical expertise of MSPs and MSSPs, combined with the real-world incident response experience and legal guidance of Cyber Counsel, small and mid-market companies can develop a robust, adaptive cybersecurity strategy that evolves with the threat landscape. This collaborative approach ensures that organizations can stay ahead of cyber criminals, comply with legal requirements, and protect their valuable assets in an increasingly complex digital world.

Chapter 8: Lessons from Cyber Incidents and Ransomware Attacks

The landscape of cybersecurity is constantly evolving, with new threats emerging and existing ones becoming more sophisticated. This chapter draws upon the wealth of experience gained from Cyber Counsel's leading companies through thousands of cyber incidents and hundreds of ransomware attacks, offering invaluable insights from the perspective of a breach counsel. By providing insight gained through guiding clients through real-world cases and analyzing common vulnerabilities and attack vectors, we can better understand how to prevent and respond to cyber incidents effectively.

One of the key lessons learned from numerous cyber incidents is the critical importance of a well-prepared incident response plan. MSPs and MSSPs play a crucial role in developing and testing these plans. They can work closely with organizations to create detailed, step-by-step procedures for detecting, containing, and mitigating various types of cyber incidents. These plans should be regularly updated and tested through tabletop exercises and simulations to ensure their effectiveness.

Cyber Counsel contributes significantly to incident response planning by ensuring that the procedures align with legal and regulatory requirements. They can provide guidance on breach notification obligations, evidence preservation, and communication strategies with law enforcement and affected parties. This collaborative approach ensures that the organization's response to a cyber incident is not only technically sound but also legally compliant.

One often overlooked aspect of cyber incident response is communication strategy. Cyber Counsel plays a crucial role in developing communication plans that balance transparency with legal protection. They can guide organizations on what information should be disclosed, to whom, and when, helping to maintain trust with stakeholders while mitigating legal risks.

Another critical lesson from past incidents is the importance of proactive vulnerability assessments and penetration testing. MSPs and MSSPs can conduct regular assessments to identify potential weaknesses in an organization's IT infrastructure before they can be exploited by attackers. These assessments should go beyond automated scans and include manual testing to uncover complex vulnerabilities that automated tools might miss.

Ransomware attacks, in particular, have highlighted the need for robust backup and recovery strategies. MSPs can work with organizations to implement comprehensive backup solutions that are regularly tested and verified. This includes implementing the 3-2-1 backup rule: maintaining at least three copies of data, on two different types of media, with one copy stored off-site. MSSPs can further enhance this strategy by ensuring that backups are immutable, protected against ransomware attacks and by implementing secure, isolated recovery environments.

The role of employee training and awareness cannot be overstated. Many successful attacks exploit human vulnerabilities through social engineering tactics like phishing. MSPs and MSSPs can collaborate to develop and deliver comprehensive cybersecurity awareness training programs. These programs should be ongoing and include simulated phishing exercises to test and reinforce employee vigilance. Cyber Counsel can contribute by sharing lessons learned from their past cases guiding clients through incident response and providing content on legal obligations and the potential consequences of data breaches, adding weight to the importance of following security protocols.

Threat intelligence sharing has proven to be a powerful tool in combating cyber threats. MSSPs can provide organizations with access to up-to-date threat intelligence, helping them stay informed about emerging threats and attack techniques. This intelligence can be used to proactively update security controls and incident response plans. Cyber Counsel can advise on the legal implications of sharing threat intelligence and ensure that any sharing practices comply with data protection laws.

The importance of network segmentation and least privilege access principles has been underscored by numerous incidents where attackers were able to move laterally through networks after gaining initial access. MSPs and MSSPs can work together to implement robust network segmentation strategies and enforce least privilege access controls, significantly limiting the potential impact of a breach.

Finally, the value of continuous monitoring and rapid incident detection cannot be overstated. MSSPs can provide 24/7 security monitoring services, leveraging advanced technologies like Security Information and Event Management (SIEM) systems, User and Entity Behavior Analytics (UEBA), and tools like Endpoint Detection & Response (EDR), Managed Detection & Response (MDR), eXtended Detection & Response (XDR), and Network Detection & Response (NDR) to detect and respond to threats in real-time. This rapid detection and response capability can significantly reduce the impact of cyber incidents.

The lessons learned from past cyber incidents and ransomware attacks highlight the importance of a collaborative approach to cybersecurity. By leveraging the technical expertise of MSPs and MSSPs, the legal guidance of Cyber Counsel, and the organization's own knowledge of its business processes, small and mid-market

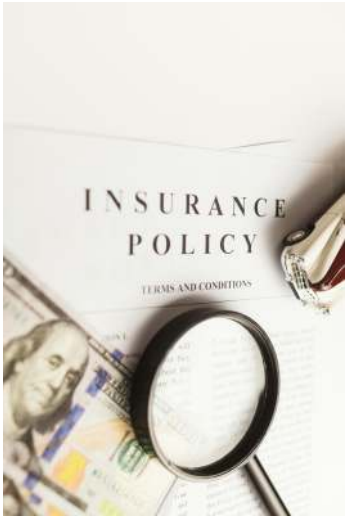
companies can significantly enhance their cybersecurity posture. This collaborative effort, combined with a commitment to continuous improvement and adaptation, is key to staying ahead of evolving cyber threats and minimizing the impact of potential incidents.

Chapter 9: Cyber Insurance and Financial Considerations

In today's digital landscape, cyber insurance has become an essential component of an organization's overall risk management strategy. This chapter explores how MSPs, MSSPs, and Cyber Counsel can collaborate to help small and mid-market companies navigate the complex world of cyber insurance and financial considerations related to cybersecurity.

Understanding the role of cyber insurance is crucial for mitigating financial risks associated with cyber incidents. Cyber insurance policies can provide coverage for various aspects of cyber incidents, including:

1. Data breach response costs
2. Business interruption losses
3. Cyber extortion payments
4. Regulatory fines and penalties
5. Legal expenses related to cyber incidents



The collaboration between MSPs, MSSPs, and Cyber Counsel is particularly valuable when it comes to selecting and evaluating cyber insurance policies. Each party brings unique expertise to the table.

Cyber Counsel plays a critical role in sharing experiences on how different insurance carriers approach handle the claims process as well as reviewing and interpreting policy terms and conditions. They can:

1. Analyze policy language to ensure it aligns with the organization's specific risks and needs
2. Identify potential coverage gaps or exclusions that could leave the company exposed
3. Negotiate with insurers to modify policy requirements and conditions when necessary (such as obtaining pre-approval of vendors)
4. Ensure that the policy complies with relevant laws and regulations
5. Assisting in the development of incident response plans that align with insurance policy requirements

MSPs and MSSPs contribute their technical expertise by:

1. Assessing the organization's current security posture to determine appropriate coverage levels
2. Implementing and maintaining security controls required by insurers
3. Providing documentation of security measures in place, which can support insurance applications and potentially lead to more favorable premiums
4. Assisting in the development of incident response plans that align with insurance policy requirements

The collaborative effort extends to the claims process as well. In the event of a cyber incident:

1. Cyber Counsel can guide the organization through the claims process, ensuring compliance with policy requirements and maximizing potential coverage
2. MSPs and MSSPs can provide technical documentation and evidence to support the claim, such as logs of security measures in place and details of the incident response
3. Together, they can work to demonstrate the organization's adherence to required security standards, which is often crucial for claim approval

Another important aspect of this collaboration is in helping organizations meet and maintain the cybersecurity requirements set by insurers. Many cyber insurance policies now require specific security measures to be in place for coverage to be valid. MSPs and MSSPs can:

1. Implement and manage required security technologies, such as multi-factor authentication, endpoint detection and response (EDR) systems, and regular backups
2. Conduct regular vulnerability assessments and penetration testing as mandated by the policy
3. Provide ongoing security monitoring and incident response capabilities

Cyber Counsel can review these requirements from a legal perspective, ensuring that the organization's implementation aligns with both the insurance policy and relevant laws and regulations.

The collaboration also extends to financial planning related to cybersecurity. MSPs and MSSPs can provide insights into the costs associated with implementing and maintaining various security measures. Cyber Counsel can advise on potential legal and regulatory fines and other costs and consequences that could result from non-compliance or data breaches. Together, they can help the organization develop a comprehensive budget for cybersecurity that balances risk mitigation with financial constraints.

The collaboration between MSPs, MSSPs, and Cyber Counsel is invaluable when it comes to cyber insurance and financial considerations. By leveraging their combined expertise, small and mid-market companies can ensure they have appropriate and adequate cyber insurance coverage, meet policy requirements, and effectively manage the financial aspects of their cybersecurity program. This collaborative approach not only helps in mitigating financial risks associated with cyber incidents but also contributes to the overall strengthening of the organization's cybersecurity posture.

Conclusion

In today's rapidly evolving digital landscape, cybersecurity has become a critical concern for small and mid-market companies. Throughout this book, we have explored the complex challenges these organizations face and the invaluable role that collaboration between MSPs, MSSPs, and outside Cyber Counsel plays in addressing these challenges.

We began by acknowledging the harsh reality of cybersecurity: it is hard; it is an ongoing battle where defenders must be right all the time, while attackers need only one successful attempt. The small and mid-market companies, in particular, faces heightened risks due to

the financial motivations of cybercriminals and relative ease of circumventing their defenses. We emphasized that cybersecurity is not a static problem but an ever-evolving landscape that requires continuous adaptation and vigilance.

The collaboration between MSPs, MSSPs, and Cyber Counsel has emerged as a powerful strategy for small and mid-market companies to enhance their cybersecurity posture. This partnership brings together technical expertise, specialized security knowledge, and legal guidance to create a comprehensive approach to cybersecurity.

We explored how MSPs contribute their technical proficiency in implementing and managing IT infrastructure, while MSSPs provide advanced security monitoring, threat detection, and incident response capabilities. Cyber Counsel adds the crucial legal perspective, ensuring that cybersecurity practices align with regulatory requirements and helping organizations navigate the complex legal landscape surrounding data protection and privacy.

Throughout the chapters, we delved into various aspects of cybersecurity, including risk assessment and mitigation, data governance and protection, legal considerations, vendor risk management, and the importance of a team-oriented approach. In each of these areas, we highlighted how the collaboration between

MSPs, MSSPs, and Cyber Counsel can provide small and mid-market companies with a level of expertise and protection that they might struggle to achieve on their own.

We emphasized the importance of continuous process and adaptation in cybersecurity. The partnership between MSPs, MSSPs, and Cyber Counsel enables organizations to stay ahead of evolving threats by providing ongoing monitoring, regular assessments, and up-to-date legal guidance. This collaborative approach ensures that cybersecurity strategies remain effective and compliant in the face of changing threats and regulations.

Drawing from real-world experiences and case studies, we shared valuable lessons from cyber incidents and ransomware attacks. These insights, combined with the expertise of MSPs, MSSPs, and Cyber Counsel, provide a powerful foundation for developing robust incident response plans and enhancing overall cybersecurity defenses.

Finally, we explored the role of cyber insurance in mitigating financial risks associated with cyber incidents. The collaboration between technical experts and legal counsel is crucial in selecting appropriate coverage and ensuring that the organization meets policy requirements.

As we conclude, it's important to reinforce that there is no such thing as perfect security. However, by fostering collaboration between MSPs, MSSPs, and Cyber Counsel, small and mid-market companies can significantly enhance their cybersecurity posture. This partnership provides a comprehensive approach that addresses technical, security, and legal aspects of cybersecurity, enabling organizations to better protect their assets, data, and reputation.

The key takeaway is that cybersecurity is an ongoing process that requires continuous effort, adaptation, and collaboration. By leveraging the combined expertise of MSPs, MSSPs, and Cyber Counsel, small and mid-market companies can build a strong foundation for cybersecurity that evolves with the threat landscape.

We encourage readers to implement the strategies discussed in this book, prioritize cybersecurity efforts, and embrace the collaborative approach. Remember that cybersecurity is not just an IT issue but an organizational imperative that requires commitment from all levels of the company.

As cyber threats continue to evolve, so too must our defenses. By fostering a culture of cybersecurity awareness, maintaining ongoing education, and staying informed about emerging threats and best practices, organizations can build resilience against cyber-attacks.

While the challenges of cybersecurity may seem daunting, especially for small and mid-market companies, the collaborative approach outlined in this book provides a powerful framework for addressing these challenges. By working together, MSPs, MSSPs, Cyber Counsel, and organizations can create a robust, adaptive, and compliant cybersecurity strategy that protects against current threats and prepares for future challenges.

About the Author

Shawn Tuma helps businesses protect their information and protect themselves from their information. He is an attorney internationally recognized in cybersecurity, incident response, cyber risk management, cyber insurance, and data privacy law, areas in which he has practiced for over two and a half decades. He is a Partner and Co-Chair of the Data Privacy, Cybersecurity, AI & Emerging Tech Practice Group at Spencer Fane LLP where he regularly serves as cybersecurity and privacy counsel advising a wide variety of businesses ranging from small and mid-sized companies to Fortune 100 enterprises, across the United States and globally.

Shawn counsels his clients with cybersecurity, data privacy, data breach and incident response, cyber risk management, cyber insurance, regulatory compliance, and computer fraud related legal issues, and cyber-related litigation. He is frequently sought out and hired by other lawyers and law firms to advise them when these issues arise in cases for themselves and for their own clients.

While this area of the law has evolved greatly in the decades Shawn has been practicing, he continues to evolve with it as a practitioner representing his clients, academically as an author and instructor, and as an analyst for the national media.

In 2016, Shawn was selected by the National Law Journal as a Cybersecurity Law Trailblazer and Texas SuperLawyers for the Top 100 Lawyers in DFW. He is regularly selected for D Magazine's Best Lawyers in Dallas and Texas SuperLawyers.

Shawn's practice can be described as a general Outside Cyber Counsel role for his clients, providing legal and advisory services for all things cyber, privacy, AI, and technology-related, and can be broken down into three distinct areas:

- Cyber Risk Management – Proactively helping companies assess and understand their overall cyber risk and then developing, implementing, and maturing a strategic cyber risk management and compliance program that prioritizes their efforts to help minimize their cyber risk and meet practical, legal, and regulatory governance and compliance requirements.

- Cyber Incident Response – Leading companies through the cyber incident response and data breach response process as a cyber first-responder (e.g., as a "breach guide" or "breach quarterback"), crisis management, and regulatory compliance investigations and enforcement actions (e.g., by regulators such as various states' Attorneys General, Department of Health and Human Services / Office of Civil Rights (HHS/OCR), Federal Trade Commission (FTC), and Securities and Exchange Commission (SEC)). Tuma serves as a breach guide working with a few select insurance companies as approved panel counsel, working along with and overseeing the work of others' insurance provided counsel, as well as for self-insured companies.
- Cyber Security, Hacking, and Data Breach Litigation – Representing clients in litigation involving cyber-related claims like computer and data misuse, computer hacking, data loss, data theft, and business to business disputes concerning responsibility for cyber incidents.

Shawn's ideal role is to serve as a member of a company's risk management team as general Outside Cyber Counsel to help the company proactively prepare for and minimize its risks of doing business in today's digital business world. Then, if a problem does arise, he is there to guide the company through resolving those issues as well.

Shawn has served the Bar and Profession in many capacities and has been selected for several current and past professional honors:

- The National Law Journal selected as a Cybersecurity Trailblazer (2016)
- National Advisory Board Member of the Year, SecureWorld (2019)
- SuperLawyers Top 100 Lawyers in DFW (2016)
- SuperLawyers (2015 – 2024)
- D Magazine Best Lawyers in Dallas (2014 – 2024)
- Past Chair, Computer and Technology Section, State Bar of Texas
- Practitioner Editor, Bloomberg Law's Texas Privacy & Data Security Law
- Council Member, SMU Cybersecurity Advisory Council
- Executive Advisory Board, Northwestern State University School of Business
- Board of Advisors, Security Advisor Alliance
- Board of Advisors, Cyber Future Foundation
- Policy Council, National Technology Security Coalition
- Past Board Member, Collin County Bench Bar Conference
- Past Chair, Collin County Bar Association Civil Litigation & Appellate Section
- College of the State Bar of Texas
- Texas Bar Foundation
- Privacy and Data Security Committee of the State Bar of Texas
- Litigation, Intellectual Property, and Business Sections, State Bar of Texas
- North Texas Crime Commission, Cybercrime Committee
- Information Systems Security Association (ISSA)
- International Association of Privacy Professionals (IAPP), CIPP/US
- Editor, Business Cyber Risk Blog

Shawn is an accomplished author with several published works on various legal-technology topics. He is a frequent speaker on business cyber risk issues such as cybersecurity, computer fraud, data protection, privacy, AI, and social media law. You can reach Shawn by telephone at 972.324.0317, or email him at stuma@spencerfane.com.

A list of Shawn's recent presentations and publications is available here: https://shawnetuma.com/about-the-author/presentations-publications/

From Trunk Slammers to Guardians: How MSPs, MSSPs, and Cyber Counsel Can Lead the Way for Securing the Middle Market

This book provides a guide for how Managed IT Services Providers (MSPs), Managed IT Security Services Providers (MSSPs), and outside cyber legal counsel (Cyber Counsel) can work together in a collaborative manner to help small and mid-market companies enhance their cybersecurity posture and resilience.

The book begins by highlighting the challenging nature of cybersecurity, especially for smaller organizations that are prime targets for financially motivated cybercriminals. It emphasizes that cybersecurity is an ongoing process requiring continuous adaptation, not a static problem that can be permanently solved.

The book concludes by reinforcing the importance of a realistic understanding of cybersecurity challenges, encouraging ongoing education, and emphasizing the need for continuous improvement of cybersecurity measures through collaborative efforts between internal teams and external partners – especially MSPs, MSSPs, and Cyber Counsel.

By leveraging the combined expertise of IT solutions providers and Cyber Counsel, small and mid-market companies can build a strong cybersecurity foundation to protect their assets, data, and reputation in an increasingly complex threat landscape.