ProWriters™
Professional & Management Liability Insurance

Creating a Comprehensive Cyber Security Risk Management Plan

ProWriters
Professional & Management Liability Insurance

Table of Contents

Chapter One:
A Brief History of Cyber Risk Management

Cyber insurance and cyber risk management has been around a lot longer than many people think. The first cyber insurance policy dates back to the late 1970s, while the the first tech E&O policies that included cyber security insurance appeared in the 1980s.

It wasn't until the late 1990s when commercial network security coverage became more prevalent. Fears of a potential Y2K crisis led to a rise in popularity of stand-alone cyber insurance policies. Demand for cyber risk management solutions grew in the wake of the dot com crash and the 9/11 attacks. But even as public awareness surrounding cyber threats increased, cyber liability insurance was still considered a niche market.

That changed when a spike in data and identity theft breaches prompted new laws and privacy regulations. California was the first state to pass laws requiring businesses to notify customers in the event of a data breach in 2002. Many states soon followed, and today, virtually every state has notification requirements for data breaches. Companies were now

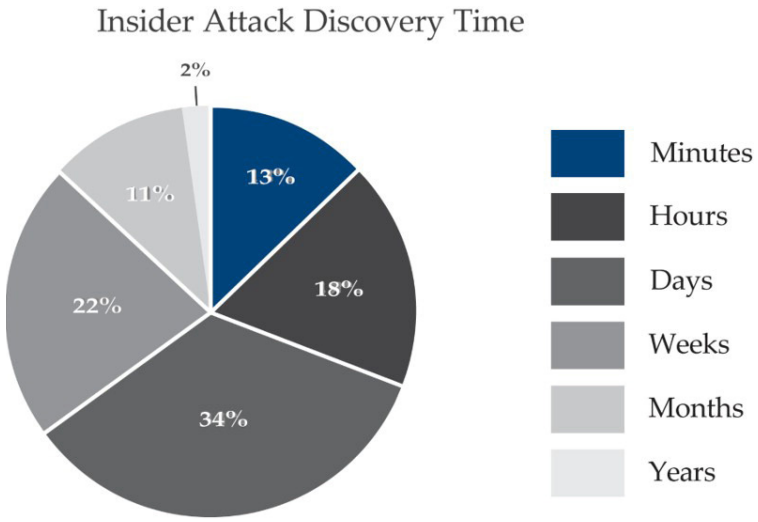
required to disclose breaches, in writing, to customers and regulators, which generated a greater demand for cyber risk management services.

As this was happening, national headlines increasingly featured stories of corporations being breached in major cyber attacks. Reputational damage, lost revenue, and regulatory fines all become more visible as direct consequences of a cyber breach. Cyber liability insurance shifted in response to these changes in the legal landscape and public perception. It started to become clear that IT security wasn't enough; cyber liability insurance was now viewed by many as a necessary part of breach risk management.

Then came 2007: a major turning point for cyber risk management.

"It started to become clear that IT security wasn't enough; cyber liability insurance was now viewed by many as a necessary part of breach risk management."

In 2007, TJX was the victim of a major cyber breach. More than 45 million customers saw their credit card and debit card information compromised in the attack. Estimates suggest the attack cost the company as much as $4.5 billion along with extreme damage to the company's reputation. The breach made clear the vital importance of cyber



Caption: "Insider attack discovery time. Source: Verizon Data Breach Investigations Report 2014."

risk management and cyber liability protection.

As cyber attacks like this became increasingly common, more research on data breaches became available. Data regarding the time it takes for a breach to be discovered made an even stronger case for cyber breach management and insurance. The Ponemon Cost of Cyber Crime Study, funded by HP, found that the average time it takes to discover a breach is 170 days. And when the attack involves an insider, this number nearly doubles.

Cyber liability insurance has changed significantly since its inception. Cyber insurance today is broader and more comprehensive than ever before and is constantly updating to respond to the ever-changing threat profile posed by increasingly sophisticated attacks. Cyber insurance at this point is only expected to grow, with some experts predicting annual cyber premiums will exceed $20 billion by 2025.

Chapter Two: The Importance of a Cyber Risk Management: Industry Exposures

When it comes to cyber security, the stakes have never been higher.

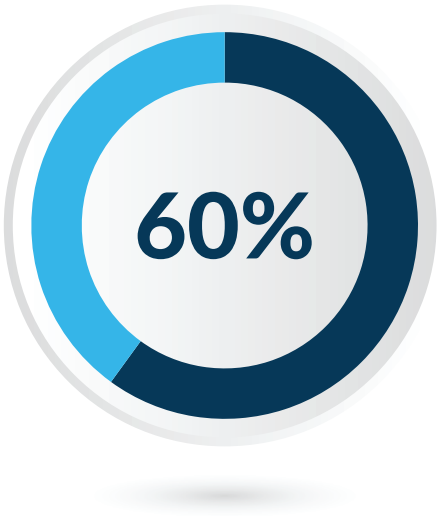
By 2021, cyber crime is expected to cost the world $6 trillion annually, which is double what it cost globally in 2015. This would make cyber crime more profitable than the entire global drug trade and would represent the greatest transfer of economic wealth in history.

Businesses of all types are potential victims of this global trend. In Q3 of 2017, nearly 80% of companies saw a severe cyber attack, with an average of 153 attacks per business.

And despite popular belief, it's not just large corporations that are targeted. In fact, small businesses are more attractive

"despite popular belief, it's not just large corporations that are targeted."

targets for cyber criminals, as they see small businesses as less secure. Hackers



Caption: "Over 60% of small businesses have experienced a cyber attack. Source: Ponemon Institute State of Cybersecurity in Small & Medium-Sized Businesses Report"

can also now largely automate cyber attacks until they successfully breach their target. According to the Ponemon Institute's 2017 State of Cybersecurity in Small & Medium-Sized Businesses report, the number of small businesses that have experienced a cyber attack rose to over 60% in 2017, and that number is only expected to grow in 2018 and beyond.

In reality, no industry is exempt from this trend, and an examination of specific industries reveals a significant deficiency in cyber risk management and security. The RSA Cyber Incident Reduction Maturity Model evaluates overall preparedness for a cyber attack by employing a quantitative assessment to determine levels of maturity in cyber risk reduction. The assessment measures five key areas, scored out of 20:

- Pre-breach Planning
- Operational Security
- Dwell Time Reduction
- Remediation
- Post-Incident Handling

Companies are evaluated in each of these categories and given a score out of 20 to create a total composite score out of 100. Overall, industries are currently scoring poorly in these areas, suggesting they are significantly exposed to cyber risk.

Financial Services

While the financial services industry is seen as being ahead of others in terms of long-term focus on security and infrastructure, there are still significant cyber risk exposures. Credit card information in particular is constantly targeted and seen as valuable to cyber criminals. A representative financial services company scored an average of 5.7 out of 20 for the five above categories, with an overall score of 28.5 out of 100.

Healthcare Services
Healthcare is an area for serious concern. The healthcare industry is highly exposed, as personal healthcare information is among the most valuable information sold on the dark web. Cyber criminals are constantly innovating and adopting new technologies to breach healthcare networks and steal data. There is also the added dimension of bodily risk with new internet-connected implant devices that are vulnerable to hacking.

Healthcare companies scored an average of 8.9 out of 20 across the five categories and got an overall score of 44.5 out of 100. While this is marginally better than the financial services industry scores, it is still classified as "Below Average-Poor" for cyber risk reduction maturity.

Legal Services
Law firms are also highly exposed with a lot of sensitive personal information that is potentially valuable for criminals. One in five law firms experienced a cyber attack in 2017—up from one in seven the year before. In the RSA assessment, law firms scored an average 5.7 out of 20 in each category. The overall score was 28.5 out of 100, on par with the financial services industry.

Every industry has unique exposures that need to be addressed by a comprehensive cyber security risk management plan. No matter what industry you're in, regardless of how large or small your company is, cyber risk affects you—and a comprehensive risk mitigation plan is the only way to limit your exposure and successfully mitigate cyber risk.

"One in five law firms experienced a cyber attack in 2017."

Chapter Three: Identifying Cyber Risks and Threats

In order to have an effective cyber security risk management plan, you need to be able to identify the threats when they occur. Cyber crime is constantly evolving and developing new ways to attack businesses. However, being able to anticipate and prepare for the most common threats will go a long way to making your business more secure.

Phishing

This is one of the most prominent cyber threats today. Phishing involves a cyber criminal sending a fraudulent email that appears to be from a legitimate source. The goal is to deceive the recipient of the email to divulge personal or confidential information, such as passwords, login credentials, or credit card information, or to trick the recipient into downloading malicious software.

Phishing emails use social engineering to appear legitimate. Cyber criminals will use social networks such as Facebook, LinkedIn, or Twitter to gather personal and work details about their target. They will include true details about their

target's life, such as names of coworkers or the person's place of business, to make the email believable. Increasing sophistication of phishing emails has made it more and more difficult to distinguish them from emails originating from legitimate sources.

According to PhishMe's Enterprise Phishing Susceptibility and Resiliency Report, 91% of cyber attacks and data breaches start with a phishing email. Given their prevalence, it is crucial for businesses and employees to carefully review any email they receive before opening any attachments or volunteering any personal information. Most reputable institutions, such as banks, will not ask for sensitive information like passwords or social security numbers via email.

"91% of cyber attacks and data breaches start with a phishing email."

Ransomware

Ransomware is a type of malicious software that infects a computer or network and holds its data hostage until a ransom is paid. These attacks often include threats to either delete vital data or publically release sensitive and/or potentially embarrassing data.

This malicious software can be downloaded onto a computer in several ways, such as from a phishing email or from malicious, false advertisements known as malvertisements. Once downloaded, the virus will either lock the whole computer screen or encrypt certain files.

Ransomware has enormous potential to cause significant financial and reputational damage. The money directly lost in making a payment often only represents a fraction of the damages that come from lost productivity and data destruction. While it is encouraging that awareness of this type of attack is on the rise, this threat won't be going away any time soon. According to Cisco's Annual Cybersecurity Report, ransomware attacks are increasing at a rate of 350% per year.

"...ransomware attacks are increasing at a rate of 350% per year."

Mobile Security Threats

Mobile technology can be a significant asset to businesses in every industry. However, it can also increase cyber security risk by exposing businesses to potential breaches. Hackers will use mobile devices to gain access to networks and steal data. They do this in a variety of ways, including getting mobile users to connect to malicious wifi, which is a compromised wifi network that allows hackers to take control of any device that connects to it.

The BYOD & Mobile Security Report found that one in five organizations have suffered from mobile security breaches, many from employees connecting their devices to malicious wifi. Verifying the wifi network you are connecting to and keeping company devices off of public wifi are effective ways to avoid mobile device breaches.

Being able to identify these threats is a crucial part of limiting exposures in every industry. Every cyber security risk management plan should address these threats and exposures to mitigate cyber risk and decrease the chance of a major data breach.

> ***"...one in five organizations have suffered from mobile security breaches"***

Chapter Four:
A "How-to Guide" to Cyber Risk Management

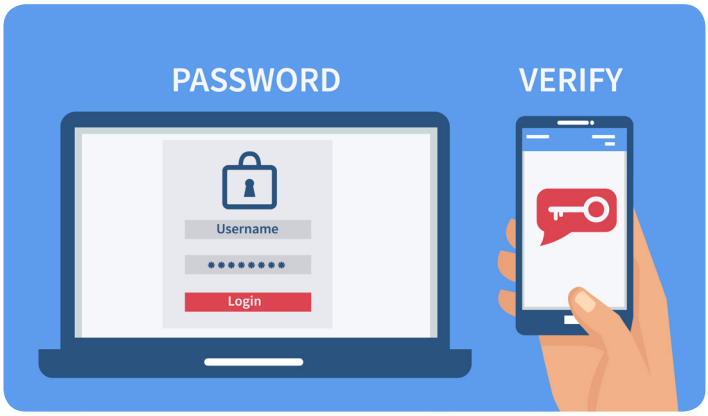
Knowing some of the history behind cyber risk management, learning about industry exposures, and identifying different threats are all important pieces of information that can inform a cyber risk management strategy. But what should actually go into a cyber risk mitigation plan? While some policies will be industry-specific, there are a few things every risk mitigation plan should have:

- Authentication controls
- Asset management
- User awareness
- Malware prevention and response
- Mobile device management

These simple recommendations will help you build a comprehensive cyber security risk management plan that mitigates your risk and limits your exposure.

Authentication Controls

More than any other vector, single-factor authentication is increasingly easy for cyber criminals to compromise. Single-factor authentication refers to a security procedure that only requires a username



and password. Using increasingly sophisticated techniques, hackers today can easily gain access to personal and sensitive data that is only protected with single-factor authentication.

Businesses need to strengthen their authentication controls by implementing two-factor authentication across their entire enterprise. Two-factor authentication adds an extra layer of security by adding an additional step beyond entering a username and password. The extra step involves a piece of information only the user knows and has access to. For instance, users may need to log in with their computer using a username and password for the first step and verify their identity using a code sent to their cell phone for the second step.

"Businesses need to strengthen their authentication controls by implementing two-factor authentication across their entire enterprise."

Two-factor authentication makes it more difficult for hackers to gain access to sensitive information. Businesses need to implement two-factor authentication controls to protect all of their data, without exception.

Asset Management

Many businesses don't take an accurate inventory of all of their assets, making it easier for cyber criminals to steal it. Furthermore, many businesses don't keep their assets properly patched across their entire enterprise.

It's critical to keep all software patched and up-to-date to protect assets from cyber breaches. "Patching" involves installing updates to fix vulnerabilities in existing software. As many companies have learned, there's a high cost to not patching. The 2017 Equifax breach is one such example. Hackers stole the personal data of more than 140 million Americans by exposing a software vulnerability. Some two months before the company was first breached, a developer patch that addressed the vulnerability was issued. However, Equifax failed to patch,

and hackers were able to breach their systems.

Keeping all assets patched and accounted for is a crucial part of any cyber risk management plan.

User Awareness

Many company breaches occur because an employee fell for a phishing email or unknowingly downloaded ransomware. For this reason, any approach to cyber security needs to go beyond software and policies and take a more holistic approach.

"For this reason, any approach to cyber security needs to go beyond software and policies and take a more holistic approach."

All employees should be made aware of cyber threats, especially those outlined in Chapter Three. This involves training employees in both cyber breach prevention and cyber breach response. In addition to training, everyone should be assessed on their ability to respond to cyber threats. Chapter Five includes more details and tips on employee training and awareness.

Malware Prevention and Response

There's no doubt malware is here to stay for the long-term. At the very least, businesses should have client-based antivirus software to defend against malware. However, not even the best antivirus software is a silver bullet, so companies should take extra steps to supplement their antivirus software, including:

Configuring content filtering

To reduce the risk of being compromised by malicious software, set controls for filtering internet traffic and email attachments. Employees are less likely to accidentally download malicious software with properly configured filtering solutions in place.

Installing intrusion detection software

According to a study conducted by

the malware researchers at Lastline Labs, only about half of antivirus software applications will detect malicious software on the day it's introduced. This is especially troubling when you consider recent research released by Cisco, which found that that 60% of data is stolen within the first few hours of attack. Adding intrusion detection software allows businesses to react to a breach in real time and limit their losses by blocking malicious software from further infecting their network.

"...60% of data is stolen within the first few hours of attack."

Implementing information rights management (IRM)

Because malicious software is often contained in an executable file, it may need privileges to run the program. IRM involves encrypting files to limit access to and interaction with sensitive information. Most employees don't need this kind of elevated access to carry out day-to-day tasks, and IRM will protect sensitive files even if an employee downloads malicious software.

Mobile Device Management

Most breaches start with a compromised device, and increasingly, these devices are mobile devices. Businesses should encrypt all mobile devices without exception. They should also be aware of the Bring Your Own Device (BYOD) policies that are becoming more and more popular each year.

BYOD policies allow employees to bring their own devices from home and use them for work. This offers convenience to both employees and business owners who don't need to worry about separate personal and work devices. Many businesses have embraced this, with a recent survey indicating nearly 40% of businesses have a formal BYOD policy.

However, there are significant cyber risks involved; as stated in Chapter Three, one in five businesses have suffered a cyber attack from a compromised mobile device. If even one employee brings an infected device into work, it can compromise the entire network.

This is not to say businesses should not

allow employees to use their personal devices for work. However, businesses should be aware of the risks involved with BYOD. Have a formal policy in place that includes mandatory antivirus protections, a continually monitored and secured network, and employee awareness.

"businesses should be aware of the risks involved with BYOD."

Chapter Five:
Training and Staff Awareness

As mentioned in previous chapters, staff awareness is a crucial part of cyber risk management. Many cyber breaches happen because of avoidable errors that can be addressed with comprehensive cyber security training. These recommendations will strengthen any cyber security training program and make your business more secure from a cyber attack.

> ***"cyber security and threat awareness will always be a part of their job, regardless of their official job description."***

Include training on day one

One of the most important aspects of cyber security is not what you teach employees, but when. Establish early on that employees need to adopt a mindset of cyber security. You can

do this by clearly communicating to employees on their first day that cyber security and threat awareness will always be a part of their job, regardless of their official job description. If employees hear it from day one, they are more likely to practice good cyber hygiene.

Institute live drills

Learning by doing is one of the best approaches to cyber security training. Simulated cyber attacks allows employees to apply what they've learned and also learn from their mistakes. Some companies have their IT team continually send out fake phishing emails to gauge how employees respond. "Live fire" training like this provides invaluable insight into where vulnerabilities are and how to improve training in the future.

> ***"Learning by doing is one of the best approaches to cyber security training."***

Conduct Evaluations

This applies to both your employees and your systems. Systematically review your business' preparedness for a cyber attack by testing its strength to identify vulnerabilities. Some experts recommend evaluating your cyber security program every 90 days.

Implement continuous training

> ***"Since cyber threats are constantly evolving, your employees should, too."***

Cyber security training should start on day one, but it shouldn't end there. Since cyber threats are constantly evolving, your employees should, too. This training should be specific to the employee's job and needs to happen at all levels. Buy-in from management is just as important as buy-in from average employees, and continuous training can help keep everyone on the same page and keep your risk mitigation plan on track.

Create a culture of cyber security

The companies with the most successful cyber security records make this a top priority. Every company should foster a culture where cyber security awareness is second nature. There are multiple ways to do this, including appointing cyber security culture advocates

in each department who continually encourage good cyber hygiene and keep employees motivated.

Encourage communication

Communication is key to security. If one employee gets a phishing email, they should feel welcome to report it, especially because they likely aren't the only ones who got it.

If an employee feels they made a mistake and may have downloaded malicious software, it's important they work in an environment where they feel they can report it. Once a cyber breach occurs, the only thing that matters in the first minutes of the attack is how quickly you identify and stop it. Encouraging communication with your employees gives you more opportunity to catch mistakes right when they happen.

Make security a priority outside of work

Communicating the importance of cyber security at home is especially important if your business has a Bring Your Own Device (BYOD) policy. Furthermore, explaining how employees can apply their training at work to their personal lives gives them an extra incentive to stay engaged in cyber security and risk mitigation planning.

Recognize and incentivize employees

Employees who do things like flag malicious emails should be recognized and rewarded. It demonstrates they take the training seriously and proves they are an asset to your company in terms of cyber security. It also helps encourage a culture of cyber awareness and keeps employees motivated to remain vigilant at work.

Cyber risk management has come a long way since the first insurance products were introduced in the 1970s. Insurance products today cover a wide range of exposures across every industry. Industries like finance, healthcare, and law face significant exposures, and businesses need a comprehensive cyber security risk management plan to manage their cyber risk and limit their exposure.

The right insurance policy, coupled with the tips for risk mitigation plans in Chapter Four and the training strategies in Chapter Five, can create a powerful and effective cyber security risk management plan. Putting all of these pieces in place can be daunting, but you never have to do it alone. Reading materials like this ebook is an important first step. The next step is seeking out professionals like the experts at ProWriters who can give you the confidence secure your business and manage your cyber risk in the long-term.

ProWriters™

Professional & Management Liability Insurance