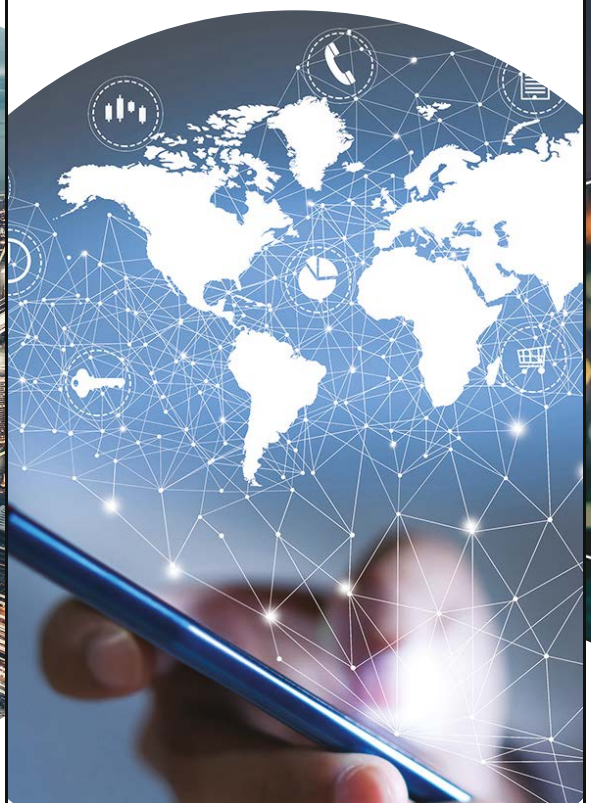
Getting Hacked: IoT and Beyond

RISK + INNOVATION | PART 10 IN A SERIES

www.aig.com/innovativetech

Foreword by:
Lex Baugh
CEO, AIG North America General Insurance



FOREWORD

CONTENTS

By Lex Baugh

In 2015, AIG and the Consumer Technology Association, the parent organization of CES, released "Internet of Things: Evolution or Revolution?," the first of what is now 10 white papers in a series on technology and risk. That first joint venture explored the promise and risks of the Internet of Things, touching on the cyber risk that technological development brings with it -- the darker side of a bright future.

"Rare will be the industry in five years that will not be changed by the IoT," we wrote then. We were wrong. Transformation is no longer on the horizon; it is happening today just 3.5 years later. As the possibilities enabled by the Internet of Things have grown, so too have the risks associated with it.

This story begins farther back, when the first cyber policy was issued in 1997.[i] Few could have predicted then the rapid and exponential growth of technology and its role in day-to-day life and business operations. At the time:

- just 39 percent of American homes had personal computers;[ii]
- the Palm Pilot was cutting edge business technology;
- President Bill Clinton was still a year away from becoming the first president to send an email;[iii] and
- monthly flat-fee unlimited Internet access from AOL was very popular.[iv]

Today, computer networks power virtually all business practices. They keep getting better, faster, and cheaper. Eighty-nine percent of enterprises "have plans to adopt or have already adopted a digital-first business strategy … to improve process efficiencies and meet and exceed customer expectations."[v] It has been estimated that by 2020, 83 percent of enterprise workloads will be in the cloud, rather than on-premises.[vi]

Recently, the broad adoption of IoT devices at both the consumer and enterprise levels has created new ways of doing business that can improve safety, efficiency, and convenience. The applications are seemingly endless, from smart-home devices such as digital assistants and smart TVs, light bulbs, locks, outlets, and more, to sensors that constantly monitor the status of assembly lines, oil pipelines, and more.

In 2016 there were 6.3 billion IoT devices (not including smartphones, tablets, and computers) in use. By 2020, Gartner estimates there will be 20.4 billion.[vii] Most of those devices will operate on their own without much involvement or oversight by humans.

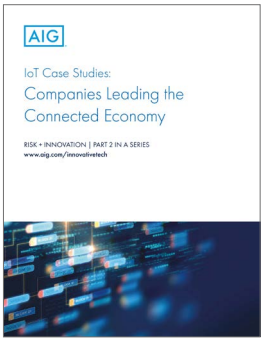
At the same time these devices improve daily life and business operations, they introduce new risks that are likely to increase along with the prevalence of the devices. IoT devices are notoriously unsecure, with the exponential growth in technology not being matched by an exponential growth in the number of resources with skills to protect individuals and enterprises from attacks.

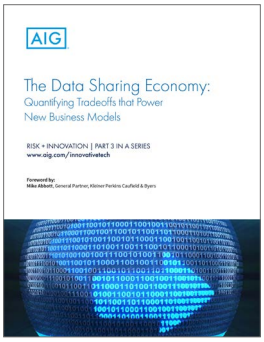
Many manufacturers overlook even basic security features -- such as unique passwords shipping with devices -- in favor of getting products to market quickly at lower cost. A high-profile study by Hewlett Packard found 25 vulnerabilities, including weak passwords and weak protection software, in each of 10 common consumer smart devices. The study concluded that nearly 75 percent of all IoT devices are susceptible to hacking.[viii]

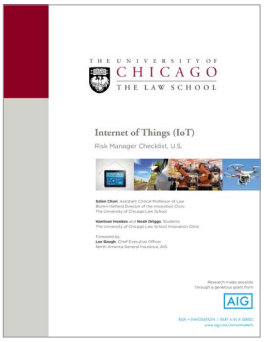
And many IoT users either don't know that they can make devices more secure or don't

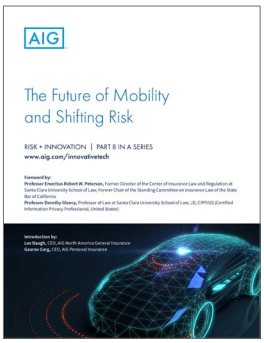
bother to do so. This is even true in business settings. A recent survey of CIOs and other IT decision makers in the United Kingdom found that 47 percent do not change default passwords in IoT devices linked to their networks.[ix] As a result, the devices become an easy access point for bad actors looking to infiltrate or attack a computer system.

The security risk is like adding dozens of new windows to an old home in a short period of time – where some of the windows don't have locks and others don't even have glass! It creates many more ways to break in and the homeowner has to make sure all of them have the same level of security as the traditional doors and windows.





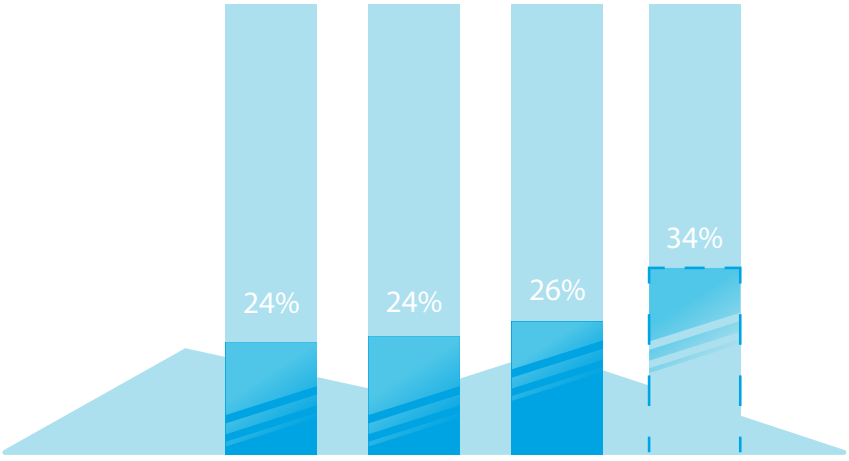




The IoT threat isn't just a consumer problem. Businesses have come a long way in understanding and addressing cyber risk since the first Chief Information Security Officer, Citi's Steve Katz, was named in the mid-1990s.[x] Given the prevalence of cyber attacks, it's no surprise cyber risk is increasingly top of mind for boards of directors.

Sixty-one percent of small and medium-sized businesses told one study they experienced a cyber attack in 2017; 54 percent said they suffered a data breach.[xi] In another study released in 2018, 82 percent of respondents predicted unsecured IoT devices will likely cause a data breach in their organization, and 80 percent say it could be catastrophic. Less than half of IT security practitioners believe they can protect their organizations from cyber threats; and only 36 percent said their senior leadership sees cybersecurity as a strategic priority.[xii]

AIG is in a unique position to observe this challenge playing out as cyber claim activity continues to rise. We have experienced increases of 24 percent, 24 percent and 26 percent in cyber claims in 2015, 2016, and 2017, respectively. As of this writing, we are on pace for a 34 percent increase in 2018 and we are approaching six new cyber claims every business day.



There's no question that cyber risk represents one of the top threats facing enterprises today, and addressing the challenge will require a coordinated effort among leaders at all levels of the organization. At AIG, we believe solving cyber risk starts with bridging the gap between Risk Managers and Chief Information Security Officers so both can fully understand the complex relationship between risk mitigation and transfer an ever-changing landscape. This white paper serves as a first step.

Less than half of IT security practitioners believe they can protect their organizations from cyber threats; and only 36 percent said their senior leadership sees cybersecurity as a strategic priority.

INTRODUCTION

As enterprises seek to address rapidly evolving cyber risks, they may discover a common challenge: a yawning gap between the person responsible for ensuring the organization is protected from cyber attacks -- usually a Chief Information Security Officer or similar position -- and the person responsible for ensuring the organization is protected from the risk of financial loss that inevitably results from those attacks -- typically a Risk Manager, Treasurer or General Counsel. Boards of Directors are increasingly responsible for oversight of both.

Cyber threats are rarely contained within a clearly defined box. They combine characteristics of multiple kinds of threats, and can create a wide range of impacts depending on the attacker's motives and the unintended consequences inherent to a viral attack.

Interconnectivity among all the systems, driven largely by the Internet of Things, is creating risks in places most people -- at least most people without a background in information security -- would never think to look. The reality today is that any device connected to a computer network -- whether it's a casino fish tank, a smart home device, or a sensor on a nuclear centrifuge -- represents a potential vulnerability. The IoT means more attack surface for criminals and raises the potential for impact because of the woeful security of IoT devices in general.

Attackers will take the path of least resistance. IoT devices usually ship with insecure configurations. Without vast improvement in consumer adoption of security best practices, they will create substantial risk for the foreseeable future. Even individuals and enterprises who practice good security basics aren't guaranteed to be safe without massive support from vendors to keep IoT updated with the latest security patches.

The fluidity and complexity of cyber threats highlight the critical need to align prevention and remediation efforts. The individuals working to prevent cyber attacks from occurring ultimately share the same goal as the individuals working to protect the organization from the fallout of a breach, and they will be most effective in meeting their shared goal when they work together.

Risk Managers can and should communicate closely with CISOs to better understand not only where cyber vulnerabilities exist for their enterprise, but also what is being done to prevent them, as well as the likelihood and potential impact of a cyber event, should those prevention efforts be circumvented. Similarly, CISOs can and should communicate closely with Risk Managers to better understand how cyber risk transfer can complement the CISO's efforts to prevent cyber attacks.

AIG's experience with cyber clients, however, suggests that individuals in those roles don't often have a chance to collaborate. This paper is intended to start that conversation by providing CISOs, Risk Managers and other decision-makers with questions they can ask each other to help establish and strengthen relationships and ultimately lead to stronger protections for their organizations.

Even individuals and enterprises who practice good security basics aren't guaranteed to be safe without massive support from vendors to keep IoT devices updated with the latest security patches.

QUESTIONS FOR RISK MANAGERS TO ASK

Question 1: What are our unique vulnerabilities?

A Risk Manager needs to understand the risks the organization faces and the potential impact of those risks - insight that cannot be gleaned from simple vulnerability assessment tools or response frameworks. A CISO can help a Risk Manager better understand the threat landscape, and where the organization is most at risk given its technology implementations.

As recent high-profile cyber events have shown, the range of threats extends well beyond the traditional risk of data loss. "We don't capture significant amounts of PII or payment card data" is no longer a reasonable reason not to devote attention to cyber vulnerabilities. Every entity has some amount of valuable data, but that's no longer the only target attackers are after. Any enterprise that does business online, or that has any business operations that rely on connected systems, is a potential target.

Vulnerabilities don't end at the company's servers. A business's cybersecurity is only as strong as the weakest link in its connected value chain. Fifty-five percent of industrial organizations allow third-party vendors access to their industrial control network, and those organizations are 63 percent more likely to experience a breach than organizations that do not permit third-party access.[xiii]

The Target breach of 2013 is a prime example of vendor vulnerability transfer. Though widely understood as a "traditional" data breach because it involved customer payment card data, that hack combined phishing and Internet of Things to gain access to Target's system through its HVAC vendor. Hackers used email containing malware to infect the vendor, whose connected devices that controlled Target's HVAC systems provided the hacker with privileged access to Target's network.[xiv]

In 2018, the director of cyber risk research for cybersecurity start-up UpGuard discovered a pair of publicly accessible backup hard drives owned by Ontario, Canada, robotics manufacturer Level One. The drives contained "extremely sensitive" data from Tesla, a Level One customer, including "non-disclosure agreements, pictures of Tesla's manufacturing, [and] computer-aided drafting schematics of their factories."[xv] Sensitive data from other Level One customers -- including General Motors, Ford, Fiat Chrysler, Volkswagen and Toyota -- was also available alongside PII for Level One employees.

There is no doubt all of those manufacturers maintain robust -- and costly -- security protocols to protect their trade secrets and sensitive information, but at the end of the day their programs were only as effective as their vendors'. Fortunately, the vulnerability was discovered by a "white hat" hacker who helped Level One secure the data -- but it could just as easily have been a bad actor stumbling upon a treasure trove of valuable information.[xvi]

Question 2: How do we already protect ourselves?

With a clearer understanding of where a company is potentially exposed, the Risk Manager puts himself or herself in a position to understand steps the CISO is already taking to mitigate risk, what else the organization can do to enhance those protections, and what risks still exist to be transferred.
Just as there is not only one kind of cyber risk, there is not one specific control that

THE THREAT LANDSCAPE

Three out of four IT security professionals reported experiencing a phishing attack in 2017.[xvii] While phishing attacks remain a major enterprise cybersecurity threat, they are no longer the only avenue of attack. The effects of an attack are evolving beyond data loss as well, including physical loss and business interruption in an increasingly complex threat landscape.

Data Theft

Bad actors in search of data to steal have shown an affinity for breaking into networks through openings most would overlook. Unsecured IoT devices are an appealing vulnerability, in part because of the wide range of damage that can be done when hackers gain access.

Cybersecurity firm Darktrace reported in 2017 that hackers broke into an unnamed casino through its fish tank. Hackers targeted connected sensors that monitored conditions in the tank and used it as an access point to the broader network. While the tank itself did not contain PII or sensitive financial information, other parts of the network did. The casino eventually discovered the breach, but not before data had been sent out to a device in Finland.[xviii]

The loss of data -- whether PII, protected health information (PHI), payment card data or other sensitive information, including trade secrets -- carries the risk of a wide range of financial losses, from cost associated with restoring victims, to regulatory action and potential litigation.

Physical loss

The casino fish tank is an example of a more traditional data breach occurring through an IoT vulnerability, but connected devices also pose threats with real-world implications beyond data loss. Impacts from physical loss can range from relatively minor to super catastrophic, including the end of life for a business.

In 2016, attackers leveled a distributed denial of service (DDoS) attack against the heating systems in two properties in Lappeenranta, Finland. DDoS attacks overload a network with requests from a large number of hacked connected devices. In this case, the attackers didn't break into the system, but threw enough traffic at it that the system repeatedly overloaded and rebooted, eventually shutting down completely. The attack lasted for several days before it was fixed, creating risk of property damage and costly relocation of residents.[xix,xx]

A year earlier, in 2015, hackers took control of a blast furnace in a German steel mill in what media dubbed "only the second confirmed case in which a wholly digital attack caused physical destruction of equipment."[xxi] The German Federal Office for Information Security reported hackers used malicious emails to steal login credentials for the mill's control systems, which they used to damage the furnace by preventing its normal shutdown.[xxii]

Business interruption

The rapid growth of the IoT device market has led to the creation of botnets capable of bringing commercial entities to their knees. One of the most infamous botnets, called Mirai, began as a way to frustrate video-game rivals, but "evolved into an online tsunami of nefarious traffic that knocked entire web-hosting companies offline" in 2016.[xxiii] The botnet automatically scanned the internet for IoT devices with default passwords still in use.

The ready and cheap availability of botnet armies on the dark web -- one review found botnet attacks available for purchase for as little as €5 in 2017 -- is enough to cause a major disruption for many enterprises. A separate 2017 study found the average DDoS attack cost businesses $2.5 million, with disruptions reaching "beyond $100,000 an hour."[xxiv] This growing threat has led to the creation of cloud-based DDoS protection services through companies like Akamai and Cloudflare, but there is a greater potential for causing harm by just denying access to a website, and DDoS protection won't protect from ransomware.

Increasingly, bad actors are gaining access to a system for the purposes of extortion, holding data and hardware hostage for ransom. Ransomware netted attackers $1 billion in 2016, according to one estimate.[xxv] In some cases, hackers aren't motivated by money as much as by creating chaos through destroying and bricking the systems.

Strong relationships with CISOs and other cyber experts can help Risk Managers stay on top of a constantly evolving threat landscape. In close coordination with IT and security decision-makers, Risk Managers can use this insight to better protect their companies from losses.

serves as a silver bullet to prevent loss. Protection against rapidly evolving threats is about layers of defense, and can start as simply as ensuring servers -- whether on-premises or cloud-based -- have been secured with password-protected access, and that data is encrypted.

Even with robust controls, a company's cybersecurity ultimately hinges on the sophistication of its end users. For example, if a phishing attempt bypasses IT controls and makes it to a user's inbox, how likely is it that every employee will be savvy enough to recognize a security threat?

Question 3: What could those vulnerabilities cost us?

Identifying a company's vulnerabilities and steps already being taken to minimize them are key prerequisites for the Risk Manager in determining how much risk still exists. The CISO has a pivotal role to play in that determination, because he or she -- along with other IT personnel -- has the clearest understanding of how an event could happen, which scenarios are most and least likely to occur, and what data would be affected.

With a common understanding of the company's specific threat landscape, the CISO and Risk Manager should work together to develop real scenarios of what could happen if their systems were compromised -- what could happen to their data, what is the most valuable data, what could happen to lead to business down time, what ransom scenarios could occur, how a third party could access their system, what companies they most rely upon to operate their core businesses and how frequently critical data is backed up, how long it would take to restore it, how long it would take to get up and running if their systems were down? They should then measure the scenarios against a gap analysis of their insurance program so the Risk Manager can close the gaps and construct a cyber insurance program that addresses their needs based on downtime, time to recovery, amount of data collected that can be lost, etc.

Developing a full picture of an entity's specific risks -- the likelihood of an event occurring and the potential cost if it does -- is difficult if not impossible to do with a simple vulnerability assessment tool or response framework. True risk modeling includes several key elements:

- **Threat:** Models are constantly updated to make sure threats are described accurately and reflect current risks.
- **Control:** Models anticipate the likelihood of a particular type of incident occurring for a specific entity based on threats seen today and the entity's unique circumstances,
- **Impact:** Models anticipate a variety of potential business impacts, in the context of likelihood, to provide an accurate picture of possible losses.

A Risk Manager who works through these elements in partnership with his or her CISO and other experts -- including IT personnel, legal counsel, finance leadership, insurance brokers and digital forensics specialists -- will be in a position to develop actionable information.

QUESTIONS FOR CISOS TO ASK

Question 1: Why should we consider cyber insurance?

CISOs who focus on controls designed to prevent cyber attacks understand that even the best controls may be breached. Cyber insurance is designed to help make an organization whole in the event of a breach. Thus, CISOs -- while not primarily focused on insurance -- should understand the need for cyber insurance as a critical element in the broader organizational toolkit addressing cyber risk.

In an environment where human error plays as significant a role as it does in IT security, technological controls and even employee training can only protect an organization to a certain extent. CISOs invest heavily in areas of greatest threat and impact, but without the financial or human capital to completely eliminate cyber risk, the cost and business impediments make it impossible to reduce risk to zero. Insurance is a key part of a comprehensive risk management program that also includes controls to reduce risk to reasonable levels and setting a retention for how much risk the company is willing to hold. Like Directors & Officers insurance, which protects the decisions of boards for loss associated with unintended consequences, cyber insurance offers protection for those situations where -- even with good controls in place -- an organization gets breached.

At the end of the day, the CISO and the Risk Manager share the common goal of protecting the organization's interest. They're more likely to achieve that goal by working together.

Question 2: What does cyber insurance cover?

As cyber insurance has evolved over the years, what is covered and how it is covered have shifted. While it's not necessary for a CISO to understand the difference between silent and affirmative coverage, or the differences between covering cyber loss in a property & casualty policy vs. a cyber policy, it may be helpful to review with the Risk Manager the kinds of things covered in the company's cyber policy.

Common myths about cyber coverage fuel a perception that makes people less likely to believe that cyber insurance will help them. These myths can erode the relationship between the company and its insurer, making adversarial what should be a collaborative partnership where the company shares what it's doing to reduce its risk, and the insurance company rewards that. Some basics it may be helpful to review with the Risk Manager include:

- Cyber insurance may include first-party protection, which covers the costs of responding to a cyber event; these costs might include ransom, forensics, restoration, lost revenue, etc.
- Cyber insurance may include third-party protection, which covers the cost of litigation related to the impact of an event, as well as regulatory fines and penalties.
- Cyber insurance may cover the cost of an investigation, even if the investigation reveals there was no breach or unauthorized access.
- Cyber insurance may cover the ransom and resulting business interruption incurred by ransomware.
- Cyber insurance is broader than "cyber risk;" it extends to privacy risk and system failures as well as to human error and malicious acts.

- Cyber insurance may cover a breach even if the company hasn't kept up with updates and patches.
- Cyber insurance may cover the company even if it was not the intended target of an attack.
- As cyber risks continue to evolve, AIG is constantly monitoring the landscape to stay at the forefront and offer tailored coverage options so insureds can promptly respond and prevent future or more costly damage.

1999

AIG writes its first data breach policy, covering financial costs associated with a breach, including event response, data restoration, financial costs to third parties, network interruption and cyber extortion.

2014

AIG writes its first Cyberedge PC® policy, which sits excess of property and casualty program to broaden coverage and fill gaps so those policies cover losses related to cyber risk.

2016

AIG offers its first Cyberedge Plus(SM) policy, which covers losses in the physical world caused by a cyber event, including primary coverage for business interruption, first- and third-party property damage, physical injury to third parties, and products/completed operations coverage.

Today

Cyber is no longer a product; it is a peril that affects a multitude of coverage lines. In our interconnected world, a cyber attack may cause property damage, loss of life, broad business interruption, or harm to customers. Cyberedge Plus provides an affirmative grant of primary coverage for a broad range of cyber risks.

CYBERWAR: COLLATERAL DAMAGE

In addition to direct attacks on enterprises, businesses must also be aware of the growing threat of the collateral damage from cyberwar. The indiscriminate nature of worms like Stuxnet and malware like NotPetya means their impacts are felt far beyond the intended targets. They can disrupt critical infrastructure, interrupt business and expose companies to the costs associated with data loss and physical impacts.

Stuxnet, a 2010 worm believed to be a joint American/Israeli attack on Iranian nuclear facilities, highlights the potential for cyber attacks to result in physical loss. The worm targeted programmable logic controllers used in a wide variety of manufacturing applications, from assembly lines to nuclear centrifuges, giving attackers the ability to take control of the machinery and eventually destroy an estimated 984 centrifuges.[xxvii]

In 2017, the NotPetya malware had far-reaching impacts beyond what is believed to be its intended target. The U.S. Central Intelligence Agency attributed NotPetya to a Russian-led attack on Ukraine,[xxviii] but the malware — which mimicked ransomware but was intended to disrupt rather than extort -- affected thousands of users across Europe, the United States and South America.[xxix]

These and other incidents that straddle the line between cyberwar and "normal" cyber attacks — including a 2014 hack of Sony Pictures believed to be carried out by North Korea and an Iranian attack on The Sands casino's IT systems in 2014[xxx] —raise complicated questions of insurance, because acts of war are usually not covered events.

Question 3: How is the legal landscape going to change the IoT?

Until now, much of the onus for security of connected devices has fallen to consumers and the enterprise users who control their implementation, but that may be changing as lawmakers and regulators begin addressing the issue.

In September 2018, California became the first state to enact legislation regulating smart devices. SB-327 requires manufacturers to include "reasonable" security features on any devices that connect to the Internet. Those security features include unique passwords for each device or a requirement for users to set a new password.[xxvi]

AIG Head of Cyber Risk Consulting Phil Kibler called the measure "a good first step," but it remains to be seen how many other states will follow suit, and what the ultimate impact will be on security and liability. Staying abreast of the legal landscape with the Risk Manager can help the CISO stay in front of these issues.

THE IMPORTANT ROLE OF INTERNAL AND EXTERNAL LEGAL COUNSEL IN SECURITY INCIDENT INVESTIGATION AND RESPONSE

By Jennifer Coughlin
Founding Partner
Mullen Coughlin LLC

The bulk of this white paper focuses on the importance of establishing and strengthening relationships between Risk Managers and Chief Information Security Officers, and that relationship is vital to the success of a cyber risk mitigation and transfer program. But there are two additional parties who brings important insight into the conversation: both internal and external legal counsel.

Just as the CISO brings expertise on the information security program and the Risk Manager brings expertise on the role insurance plays in risk transfer, a company's internal legal counsel will bring a unique expertise on the legal responsibilities an organization has to secure data in its possession and control, and its legal and contractual obligations when a potential or confirmed compromise in the security of that data occurs.

Take for example a scenario that recently played out in a health care organization being hit with a ransomware demand for $5,000. The CISO had budgetary authority to incur expenses up to $5,000 without prior approval, and utilized this authority without notification to any other

department within the organization to pay the ransom, obtain the decryption key, and regain access to the previously encrypted protected health information.

Six months later, at an executive meeting attended by the CISO, the Risk Manager, and legal counsel, the CISO reported on the event and learned two important facts that, had he known six months prior, would have changed the course of his actions and placed the organization in a defensible position with no financial loss. Unbeknownst to the CISO, the organization had cyber insurance coverage that provided extortion coverage, with a $0 retention. Also unbeknownst to the CISO, per the 2016 directive from the U.S. Department of Health and Human Services, the encryption of protected health information via ransomware is presumed to be a breach unless the organization takes steps to investigate the incident and, per HIPAA, conclude the incident posed a low probability of compromise of the protected health information.

Because the CISO did not communicate with legal counsel or the Risk Manager, the health care organization not only incurred the out-of-pocket expense for the ransom payment, but also lacked the evidence to demonstrate a low probability of compromise of the protected health information and had failed to satisfy its reporting obligations pursuant to federal law, resulting in a risk of fines and penalties and a duty to provide notice to its patients, HHS, and other parties.

External legal counsel also plays a vital role, and it is critical for Risk Managers, CISOs, and internal legal counsel to engage with external legal counsel as soon as they suspect a breach may have occurred. External legal counsel well-versed in security incident investigation and response will ensure that:

- As much of the response effort as possible is covered by attorney-client privilege, putting the organization in the best possible position to defense any claims that arise as a result of the incident.

- The organization engages with vendors whose services will be covered by the company's insurance policy, reducing out of pocket expenses.

- The organization engages with vendors capable of responding appropriately and quickly. A vendor that has cryptocurrency available immediately, for example, can get the ransom paid and the company's system back up and running quicker than one that needs to convert dollars or other currency into bitcoin first.

- The investigation and response efforts align with reporting requirements, and that evidence that may be needed in the course of the response or in defending the organization from litigation is preserved.

Addressing cyber risks before they become reality is critical to preparing for events that are, in many cases, inevitable. It's important that Risk Managers, CISOs, and internal legal counsel develop their relationships and common understanding of (1) the benefits of the organization's cyber insurance policy, which can provide coverage for some or all out-of-pocket costs associated with security incident investigation and response, such as ransom payment, forensic investigation firm fees, legal fees, notification costs, credit and identity monitoring and restoration services, and public relations fees; (2) the organization's security risks and legal and contractual posture; and (3) the need to engage with experienced external counsel as early as possible after detecting a potential security incident. These efforts will ensure a smooth, cost-effective and compliant response effort and place the organization in the best defensible position possible.

Jennifer Coughlin is a founding partner of Mullen Coughlin LLC, a law firm specializing in data privacy and information security events.

PRACTICING FOR THE WORST - UNDERSTANDING THE CLAIMS PROCESS

If a building catches fire, the owner's first call is to the fire department, which will put the fire out. Only after the event is over does the owner contact his insurer to assess the damage and begin the restoration process. A similar scenario is true for most losses that would traditionally be covered by property and casualty policies. The loss occurs in a single, one-time, brief event and the insurer enters the picture after the fact to provide restoration.

Cyber events, by contrast, are usually ongoing, long-term events, and the insurer plays a critical role at every step: prevention before an event, support during an event, and restoration after a loss occurs. The complex and ongoing nature of most cyber attacks makes appropriate and timely response critical, and that starts with two phone calls:

Step 1: Call Legal Counsel

When an attack is suspected, AIG recommends a company's first call, once the CISO and internal cyber response team have been notified, be to legal counsel who can advise on the legal ramifications of the suspected breach and engage with forensic analysts who can pinpoint the problem, end the breach, and begin the process of restoration. AIG, like most insurers, provides insureds with a list of pre-approved legal experts who can provide this critical advice.

Step 2: Call Your Insurer

If there is a silver lining to the frequency and profile of cyber breaches in recent years, it is the removal of the stigma that had been associated with becoming a victim. The fact is that being the subject of a cyber attack is becoming more commonplace -- and reporting a claim allows a company to take advantage of the protection it has secured in insurance.

Ideally, a company's first conversation with its insurer's claims processors won't be when a breach is suspected to have occurred. As is the case with relationships between CISOs and Risk Managers, establishing relationships between insureds and claims agents before a breach occurs is one of the most effective ways to ensure a claim is processed quickly and efficiently. Additionally, AIG maintains a 24/7 hotline, powered by IBM, to expedite the response to suspected cyber events.

PREPARATION IS THE BEST PROTECTION

The relationship between the CISO and the Risk Manager is critical to the success of a cyber risk program. Each brings a different skill set and knowledge base that is vital to the other's understanding of the threat landscape as well as mitigation and transfer solutions. Establishing a relationship and maintaining open lines of communication are among the most important steps either can take in addressing the cyber challenge.

But neither individual is in a position to unilaterally make strategic business decisions that guide cyber mitigation and risk transfer. Risk Managers and CISOs are part of a network of leaders and decision-makers from the broader business, and it's important to involve those leaders in pre-breach conversations.

Ultimately, it's a business choice to decide what is important to protect and what is not, or the total value to use in setting insurance coverage. Neither the Risk Manager nor the CISO makes those decisions independently; instead they must be made in collaboration with business leaders at the highest levels.

Table-top exercises are a valuable way to bring all these decision-makers together to work through potential incidents, answer one anothers' questions, and explore broader strategic decisions that must be made. Scenarios to explore could include:

- Ransomware locks up 10,000 machines for three days and the attackers are demanding a $100,000 payment.
- An ongoing breach is discovered in which hackers have gained access to PII and PCI
- A disgruntled employee steals or damages sensitive company information such as employee or customer data, trade secrets or financial information.
- A DDoS slows down or cripples the network, making customers unable to access products and services.
- A "perfect storm" scenario that combines numerous risk elements into one event and represents an all-hands-on-deck situation.

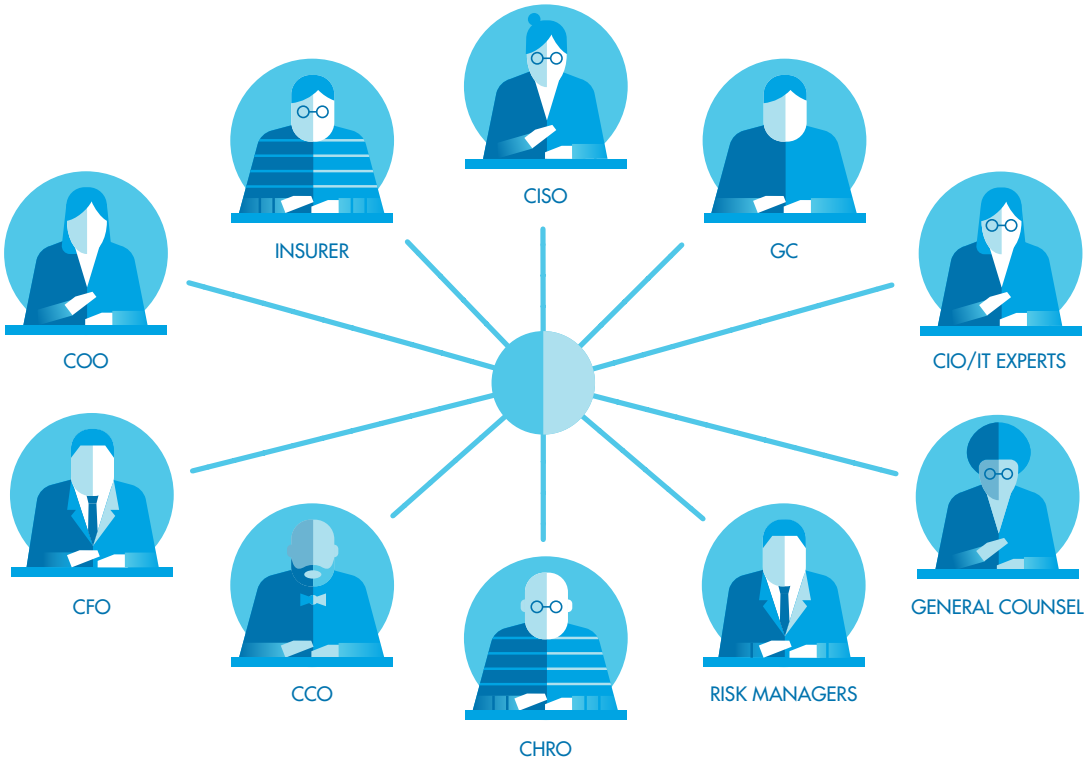
All scenarios will follow a similar underlying response framework that unfolds in phases, beginning with detection of a threat; followed by assessment of the state of the breach and its impact; containment, eradication, and recovery; incident closure; and a review of feedback and lessons learned that can be applied to preventing or more effectively responding to similar incidents in the future. Depending on the scenario, questions to address in table-top exercise could include:

- How will systems alert us to a threat?
- What is the process for assessing the state of the breach and its impact.
- What will it cost the business if the network is down for 1 day, 2 days, or more?
- Under what cyber attack circumstances would we disconnect our servers from the network?

- Would we pay a cyber ransom?
- Who are our third parties? What are each party's notification responsibilities in the event of a breach? What service level do we expect from them?
- What is our liability in the given scenario?
- What reporting requirements apply?
- Do we contact law enforcement? If not, why not?
- Can IT guarantee that if some systems are down, backups are safe and secure. Have we tested them or can we test them in a safe environment before restoring?
- If the scenario is multi-national, are we aware of foreign rules and regulations and are we prepared to comply?

A comprehensive Cyber Security Incident Response Plan will identify roles and responsibilities on the Cyber Security Incident Response Team, but in most cases the people at the table include

- Chief Information Security Officer brings insight on the risk landscape and mitigation efforts in place.
- Chief Information Officer and other IT experts bring insight into the company's broader information technology strategy, including third-party relationships, as well as the kind of information stored and the potential impact of a loss.
- General Counsel and other legal experts bring insight into liability and regulatory/compliance requirements.
- Risk Manager brings insight on current and available insurance coverages on particular risks.
- Chief Human Resources Office brings insight into company policies related to risks around rogue employee threats and/or employees as third-parties affected by a breach.
- Chief Communications Office brings insight into public relations fallout and how to communicate with internal and external audiences to minimize negative impacts.
- Chief Operations Officer and other business leaders bring insight into potential impact of a breach on business operations.
- Chief Financial Officer brings insight into potential impact of a breach on finances.
- Board member (depending on the size of the organization) can help answer questions about decisions the organization would or should make during a breach.
- Insurer brings insight into risk severity and likelihood, response procedures, etc.



CONCLUSION

Connectivity enabled by the Internet of Things is creating new risks for enterprises. It is critical for those enterprises to close the gap between the person responsible for ensuring the organization is protected from cyber attacks and the person responsible for ensuring the organization is protected from the risk of financial loss stemming from attacks that do occur.

The collaboration between Risk Managers and CISOs, and among them and other business leaders from across the company, should mirror the complexity and interconnectedness of attacks themselves. Only when leaders work together will businesses be well positioned to prevent attacks that can be prevented, respond as quickly as possible to attacks that do occur, and achieve restoration in a timely manner that minimizes long-term fallout.

It all starts with a conversation.

CITATIONS

i. Wells, Andrea. "What Agent Who Wrote First Cyber Policy Thinks About Cyber Insurance Now." Insurance Journal. March 1, 2018. Accessed online Nov. 29, 2018. https://www.insurancejournal.com/news/national/2018/03/01/481886.htm

ii. "39 percent of U.S. homes have PCs." CNET. May 21, 1996. Accessed online Nov. 29, 2018. https://www.cnet.com/news/39-percent-of-u-s-homes-have-pcs/

iii. Sandre, Andreas. "What's the first ever presidential email?" Medium.com. Nov. 7, 2017. Accessed online Nov. 29, 2018. https://medium.com/digital-diplomacy/whats-the-first-ever-presidential-email-324ddcd82fca

iv. Ryan, Joal. "This was the hottest tech 20 years ago … in 1997." CNET. Jan. 11, 2017. Accessed online Nov. 29, 2018. https://www.cnet.com/pictures/this-was-the-hottest-tech-20-years-ago-in-1997/15/

v. Columbus, Louis. "The State of Digital Business Transformation, 2019." Forbes.com. April 22, 2018. Accessed online Nov. 30, 2018. https://www.forbes.com/sites/louiscolumbus/2018/04/22/the-state-of-digital-business-transformation-2018/#38675c205883

vi. Columbus, Louis. "83% of Enterprise Workloads Will Be In The Cloud By 2020." Forbes.com. Jan. 7, 2018. Accessed online Nov. 30, 2018. https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/#7c1e3b836261

vii. Press Release. "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent From 2016." Gartner. Feb. 7, 2017. Accessed online Nov. 29, 2018. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

viii. Nelson, Katie. "70 Percent of Internet of Things Devices Are Vulnerable to Hacking, Study Says." Mashable.com. Aug. 2, 2014. Accessed online Nov. 30, 2018. https://mashable.com/2014/08/02/internet-of-things-hacking-study/#rRHWbpUBKaqz

ix. Jay, Jay. "46% CIOs & IT decision makers have no control over IoT devices in their networks." TEISS. April 5, 2018. Accessed online Nov. 30, 2018. https://www.teiss.co.uk/iot/iot-devices-enterprise-networks/

x. Security Current biography of Steve Katz. Dec. 21. 2017. Accessed online Dec. 6, 2018. https://securitycurrent.com/steve-katz/

xi. "2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)." Ponemon Institute LLC. September 2017. Accessed online Nov. 29, 2018. https://csrps.com/Media/Default/2017%20Reports/2017-Ponemon-State-of-Cybersecurity-in-Small-and-Medium-Sized-Businesses-SMB.pdf

xii. "2018 Study on Global Microtrends in Cybersecurity." Ponemon Institute Research Report. February 2018. Accessed online Nov. 29, 2018. https://www.raytheon.com/sites/default/files/2018-02/2018_Global_Cyber_Megatrends.pdf

xiii. "The State of Industrial Cybersecurity 2017." Business Advantage. Accessed online Nov. 30, 2018. https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf

xiv. "Target Breach: How it Happened and how to Prevent." SecureLink. Sept. 21, 2015. Accessed online Nov. 29, 2018. https://www.securelink.com/blog/target-breach-how-to-prevent/

xv. Niedermeyer, Edward. "All in a day's work: How a hacker found a massive customer data breach through a robotics supplier in Canada." Automotive News Canada. Oct. 1, 2018. Accessed online Nov. 29, 2018. http://canada.autonews.com/article/20181001/CANADA01/310019993/all-in-a-days-work

xvi. Ibid

xvii. Bisson, David. "Three-Quarters of Organizations Experienced Phishing Attacks in 2017, Report Uncovers." Tripwire. Jan. 24, 2018. Accessed online Dec. 6, 2018. https://www.tripwire.com/state-of-security/security-data-protection/three-quarters-organizations-experienced-phishing-attacks-2017-report-uncovers/

xviii. Schiffer, Alex. "How a fish tank helped hack a casino." The Washington Post. July 21, 2017. Accessed online Dec. 7, 2018. https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

xix. Saarela, Matti. "Hackers hit the Lappeenranta property in the boiler room." [Translated] Etela-Saimaa. Nov. 6, 2016. Accessed online Dec. 7, 2018. https://esaimaa.fi/uutiset/lahella/64208f0e-81b9-4a41-ad68-df8fa521224f

xx. "DDoS attack halts heating in Finland amidst winter." Metropolitan.fi. Nov. 7, 2016. Accessed online Dec. 7, 2018. http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter

xxi. Zetter, Kim. "A Cyberattack Has Caused Confirmed Physical Damage For The Second Time Ever." Wired. Jan. 8, 2015. Accessed online Dec. 7, 2018. https://www.wired.com/2015/01/german-steel-mill-hack-destruction/

xxii. Hack attack causes 'massive damage' at steel works." BBC. Dec. 22, 2014. Accessed online Dec. 8, 2018. https://www.bbc.com/news/technology-30575104

xxiii. Graff, Garrett M. "The Mirai Botnet Architects Are Now Fighting Crime With The FBI." Wired. Sept. 18, 2018. Accessed online Dec. 8, 2018. https://www.wired.com/story/mirai-botnet-creators-fbi-sentencing/

xxiv. Osborne, Charlie. The average DDoS attack cost for businesses rises to over $2.5 million." ZDNet. May 2, 2017. Accessed online Dec. 8, 2018. https://www.zdnet.com/article/the-average-ddos-attack-cost-for-businesses-rises-to-over-2-5m/

xxv. Korolov, Maria. "Ransomware took in $1 billion in 2016 -- improved defenses may not be enough to stem the tide." CSO Online. Jan. 5, 2017. Accessed online Dec. 8, 2018.

xxvi. Robertson, Adi. "California just became the first state with an Internet of Things cybersecurity law." The Verge. Sept. 28, 2018. Accessed online Nov. 30. 2018. https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law

xxvii. Holloway, Michael. "Stuxnet Worm Attack on Iranian Nuclear Facilities." Stanford University coursework. July 16, 2015. Accessed online Dec. 8, 2018. http://large.stanford.edu/courses/2015/ph241/holloway1/

xxviii. Nakashima, Ellen. "Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes." The Washington Post. Jan. 12, 2018. Accessed online Dec. 8 2018. https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

xxix. Turner, Giles, et al. "New Cyberattack Goes Global Hits WPP, Rosneft, Maersk." Bloomberg. June 27 2017. Accessed online Dec. 8, 2018. https://www.bloomberg.com/news/articles/2017-06-27/ukraine-russia-report-ransomware-computer-virus-attacks

xxx. Pagliery, Jose. "Iran hacked an American casino U.S. says." CNN. Feb. 27, 2015. Accessed online Dec. 8, 2018. https://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html

American International Group, Inc. (AIG) is a leading global insurance organization. Building on 100 years of experience, today AIG member companies provide a wide range of property casualty insurance, life insurance, retirement products, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance www.twitter.com/AIGinsurance | LinkedIn: www.linkedin.com/company/aig.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.