Whitepaper:

Cyber Liability Insurance Overview

Sponsored by the

State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)

June 2016

Contents

1. Introduction

The rise in the number of cyber security breaches is a phenomenon that undoubtedly will continue to increase. Information security breaches affect the private and public sectors, large and small organizations regardless of where they are located, and the need to be better prepared can no longer be ignored. However, implementing and maintaining a good cyber security program will not guarantee an organization won't be a victim; so many entities are taking a broader approach on appropriate protections as they consider their overall risk strategy. States and local governments have a long history of experience preparing for physical emergencies; however, cyber incidents represent relatively new territory. This lack of familiarity on how to prepare and respond is a very real concern. It is important to note however, that physical attacks can have cyber repercussions, and vice-versa—they are not, necessarily, mutually exclusive.

This whitepaper is a resource document that presents a broad overview on the topic. It focuses on data breaches involving the loss of Personally Identifiable Information (PII), Personal Health Information (PHI), Credit Card information, etc. However, there are, of course, many other forms of cyberattacks organizations must be prepared for—such as Distributed Denial of Service (DDoS), and Ransomware—that has become quite prevalent lately.

DHS and the Multi-State Information Sharing and Analysis Center warn that cyberattacks against law enforcement, fire departments, and other emergency services are increasing. Targets such as these, for whom lost access to systems could cost lives, are very much of interest for ransomware threat actors.The escalation and impact of cyber breaches is recognized by the Federal government and steps have been taken to raise awareness about this serious issue. In 2013, President Obama highlighted cybercrime as a serious threat to the economy, and issued an executive order that resulted in the creation of the Cybersecurity Framework by the National Institute of Standards and Technology (NIST).

The Department of Homeland Security has implemented a number of initiatives, including establishing a working group of leading insurance companies to address the various issues involved in cybercrimes, including developing cost-effective products and services to assist organizations to be more prepared, and reducing the financial burden when an entity experiences a major breach.

This is a timely issue that continues to receive media attention and is a topic of discussion for many legislators at the Federal and state levels. There have been numerous breaches at all levels of government, most notably at OPM (Office of Personnel Management), and the costs can be significant. This document provides background on cyber insurance: cyber risks to consider covering, reasons for investing, types of coverage available, factors influencing risk & cost, and suggested next steps.

Every organization's needs are slightly different, but this relatively new type of insurance is worth exploring as part of an overall risk management program. The goal is to raise awareness so

state and local governments have the opportunity to determine what makes sense for their organization and to be better prepared *before* they experience a cyber breach.

2. Overview

For years, information security professionals have said, "either you have been breached or you just don't know that you have." A "data breach" is defined as the unauthorized disclosure of personally identifiable information, which is in turn defined as the combination of public (name, address) and non-public (SSN, bank routing number) data, which in aggregate may be used to perform financial fraud (also known as "identity theft").

Data breaches are now a fact of life, so it is critical for organizations to understand how to manage the risks related to a data breach and reduce the significant cost that can result from them.

A relatively new development available as part of a risk management portfolio is the emergence of cyber liability insurance (CLI) coverage. This coverage has existed in the market for over 10 years; however, most organizations either have never heard of it or know very little about it.

The market for cyber insurance in 2015 was $2.5 billion. For 2020, it is estimated anywhere between $5 billion and $10 billion. By comparison, workers' compensation insurance is a $55 billion market. More than 60 insurers offer cyber coverage, with just seven of them landing 65% of the business. There are a number of reasons for the growth in cyber liability insurance. One of the catalysts has been not only an increase in cybercrime, but also new regulations.

The huge increase in the number of breaches has resulted in 47 states passing legislation requiring organizations to notify customers if they have a data breach. The challenge is, most states and many local governments have information on citizens not currently residing in their state, therefore they need to be aware of and comply with breach notification laws in other jurisdictions. There is no standardization right now and no overarching Federal requirement. This can be a burden, particularly as the timeline for notification can vary. As the expense of dealing with a breach gets higher – and the cost of dealing with mandatory notification is added – considering the option of CLI becomes more essential, in much the same way that existing business insurance policies for fire, flood and theft are vital components in a risk management toolkit.

Cybercrime also is a growing concern for the Federal government and many state legislators.

President Barack Obama shone a spotlight on the problem. In 2013, he highlighted cybercrime as a serious threat to the economy, and issued an executive order that resulted in the NIST Cybersecurity Framework, which gives organizations a guideline on how to respond and handle cybercrimes, and to which incentives are attached – notably, a reduced barrier to risk transference through the insurance mechanism.

Also, the House Infrastructure Protection, and Security Technologies subcommittee held hearings in early 2016 to examine potential opportunities to promote the adoption of cyber best practices and more effective management of information security risks through cyber insurance.

Comments at the hearings by various insurance experts were very much aligned. They noted there is a need to explore ways for the marketplace to expand to create a wide array of diverse, affordable products that also will benefit small- and medium-sized entities.

They explained cyber insurance companies typically create cyber insurance policies on a case by case basis that can often result in higher premiums. However, they can use market incentives to help better mitigate their risks and ultimately make cyber insurance more accessible.

They agreed cybersecurity insurance is potentially an effective, market-driven way of increasing cybersecurity both in the public/private sectors. The underwriting process will scrutinize an organization's technical defenses, incident response plan, procedures for patching software, policies for limiting access to data and systems, and monitoring of the vendor network.

Exact coverage varies depending on which insurance company is selling the policy, but common coverage includes forensics, restoration of the network, public relations, attorney fees, notification of victims, call centers to field inquiries, litigation, extortion payments,

They cover data breach and privacy claims, incident response costs, liability for damages, defense costs, civil fines and penalties, industry fines and penalties (such as payment card industry), business interruption costs, and media liability. The latter is for Web site content that is libelous.

They also cover pre-incident services such as certain network security costs, employee training, and incident planning, all of which come before a breach occurs but that can help mitigate the ultimate cost.

Cyber-related bodily harm and property damage, as well as stolen intellectual property, are generally not covered because it is difficult to put a price tag on them. Funds-transfer fraud (e.g., an attacker spoofs an email with an apparent order from the CEO for the CFO to cut a big check to a third party, and the attacker ends up getting the money) is also not covered.

Insurance companies can move markets and help improve cybersecurity through insurability criteria that adopts controls. Bottom line: the more organizations reduce their cybersecurity risks, the lower their premiums.

I. What is Cyber Liability Insurance?[i]

The term “cyber liability insurance” is often used to describe a range of coverages, in much the same way that the word “cyber” is used to describe a broad range of information security related tools, processes and services.

Although coverages vary, cyber risks typically include:

- Identity theft as a result of security breaches where sensitive information is stolen by a hacker or inadvertently disclosed, including such data elements as Social Security numbers, credit card numbers, employee identification numbers, drivers' license numbers, birth dates and PIN numbers.
- Damage to the firm's reputation.
- Theft of valuable digital assets, including customer lists, business trade secrets and other similar electronic business assets.
- Introduction of malware, worms and other malicious computer code.
- Human error leading to inadvertent disclosure of sensitive information, such as an email from an employee to unintended recipients containing sensitive business information or personal identifying information.
- Lawsuits alleging trademark or copyright infringement.

However, cyber risk remains difficult for insurance underwriters to quantify due in large part to a lack of actuarial data. Insurers compensate by relying on qualitative assessments of an applicant's risk management procedures and risk culture. As a result, policies for cyber risk are more customized than other risk insurers take on, and, therefore, can be more costly. An organization's operation will dictate the type and cost of cyber liability coverage. Also, the size and scope of the organization will play a role in coverage needs and pricing, as will the number of customers, the presence on the Web, the type of data collected and stored, and other factors.

Cyber liability policies might include one or more of the following types of coverage:

- Liability for security or privacy breaches. This would include loss of confidential information by allowing, or failing to prevent, unauthorized access to computer systems.
- The costs associated with a privacy breach, such as consumer notification, customer support and costs of providing credit monitoring services to affected consumers.
- The costs associated with restoring, updating or replacing business assets stored electronically.
- Business interruption and extra expense related to a security or privacy breach.
- Liability associated with libel, slander, copyright infringement, product disparagement or reputational damage to others when the allegations involve a business website, social media or print media.
- Expenses related to cyber extortion or cyber terrorism.
- Coverage for expenses related to regulatory compliance for billing errors, physician self-referral proceedings and Emergency Medical Treatment and Active Labor Act proceedings.

Securing a cyber liability policy is not a simple task. Insurers will be interested in the risk management techniques applied by the organization to protect its network and its assets. The insurer will probably want to see the organization's incident response, business continuity, and disaster response plans and evaluate them with respect to the organization's risk management of its networks, websites, physical assets and intellectual property. The insurer will be interested in how employees and vendors, partners, etc. are able to access data systems. At a minimum, the insurer will want to know about antivirus and anti-malware software, the frequency of updates, the performance of firewalls, threat detection capabilities, and security clauses in contracts with vendors.

The complexity of the applications insurance buyers have to complete varies widely depending on how big their organizations are. A small entity might fill out a form with four or five questions as basic as, "Do you use anti-virus and other basic security measures?", "Do you encrypt sensitive data?", "Do you encrypt all data at rest?", "Have you suffered breaches before?", and "Are there complaints against you about data protection and security?"

Larger organizations might get five-page questionnaires.

Organizations that buy cyber insurance generally fall into two groups. Those with less than $500 million in revenue pay $2,000 to $5,000 per year for payout limits from $1 million to $5 million. Those with more than $500 million in revenue pay $100,000 to $500,000 per year for $5 million to $20 million in payout limits.

II. Cost of a Cyber Breach

Like the policies, the price of the coverage varies, too, although prices are coming down as more insurers enter a market served by the likes of Travelers, AIG, Chubb, ACE Limited and CNA. The increased competition is making cyber insurance more affordable for many smaller organizations that can buy policies tailored to their risk profile. As with all insurance, each organization must carefully evaluate what assets they need to protect so they are not purchasing too much or too little coverage.

However, not having some level of cyber insurance could prove costly for organizations.

The Ponemon Report 2015 Cost of Data Breach Study identified the following trends in cyberattacks, breaches and costs:

- **Cyberattacks have increased in frequency and in the cost to remediate the consequences.** The cost of data breaches due to malicious or criminal attacks increased from an average of $159 in last year's study to $170 per record.
- **Data breach costs associated with detection and escalation increased**. These costs typically include forensic and investigative activities, assessment and audit services,

crisis team management and communications. This total average cost increased from $.76 million last year to $.99 million in this year's report.

- **Hackers and criminal insiders cause the most data breaches.** Forty seven percent of all breaches in this year's study were caused by malicious or criminal attacks. The average cost per record to resolve such an attack is $170. In contrast, system glitches cost $142 per record and human error or negligence is $134 per record.
- **Board involvement and the purchase of insurance can reduce the cost of a data breach.**

For the first time, the study looked at the positive consequences that can result when Boards of Directors (in the public sector – Agency Executive Management) take a more active role when an organization had a data breach. Their involvement reduces the cost by $5.5 per record. ***Insurance protection reduces the cost by $4.4 per record.***

- **Time to identify and contain a data breach affects the cost.** For the first time, the study shows the relationship between how quickly an organization can identify and contain data breach incidents and financial consequences. Malicious attacks can take an average of 256 days to identify while data breaches caused by human error take an average of 158 days to identify.
- **Business continuity management plays an important role in reducing the cost of data breach.**

The research reveals having business continuity management involved in the remediation of the breach can reduce the cost by an average of $7.1 per compromised record.

There are several reports/studies with varying numbers regarding the cost of a breach. Ponemon is one of the leaders, as is Verizon, so as a comparison, following is an excerpt from the Verizon 2015 Data Breach Investigations Report:

RECORDS	PREDICTION (LOWER)	AVERAGE (LOWER)	EXPECTED	AVERAGE (UPPER)	PREDICTION (UPPER)
100	$1,170	$18,120	$25,450	$35,730	$555,660
1,000	$3,110	$52,260	$67,480	$87,140	$1,461,730
10,000	$8,280	$143,360	$178,960	$223,400	$3,866,400
100,000	$21,900	$366,500	$474,600	$614,600	$10,283,200
1,000,000	$57,600	$892,400	$1,258,670	$1,775,350	$27,500,090
10,000,000	$150,700	$2,125,900	$3,338,020	$5,241,300	$73,943,950
100,000,000	$392,000	$5,016,200	$8,852,540	$15,622,700	$199,895,100

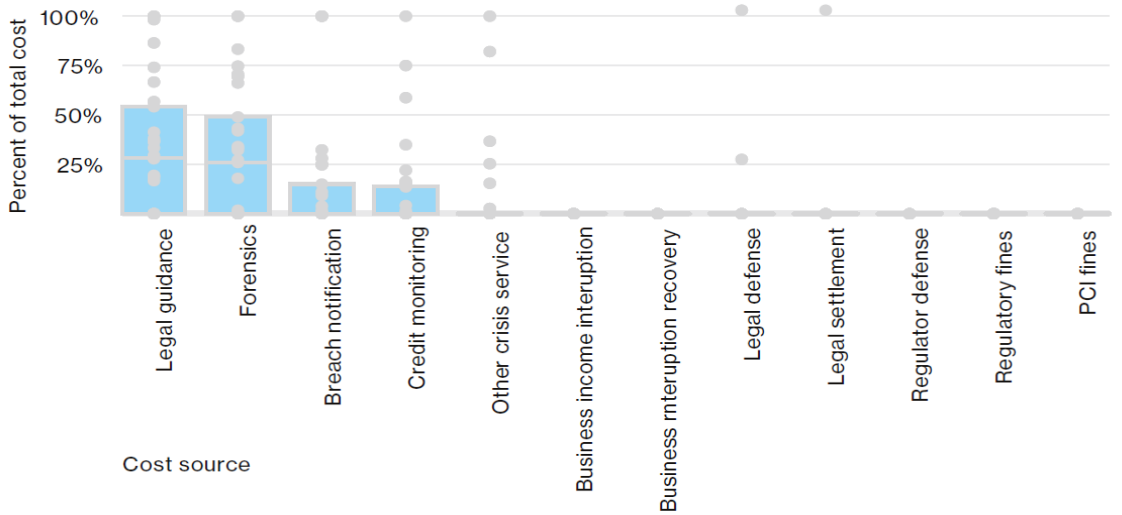
The chart is a bit complicated, but the intent is to show there are many factors influencing the cost of a breach. Definitive numbers should be taken with a grain of salt. For a much more in-depth explanation, see the Verizon 2015 Data Breach Investigations Report.

The bottom line is, there is no consensus on the cost of a data breach because there are so many variables.

It also may be helpful to understand the majority of insurance payouts go toward costs within the phase of breach recovery associated with determining how the breach was caused. Legal guidance during the crisis management phase and forensics investigations are where the majority of funding is spent. These cost categories are followed by breach notification and credit monitoring.

In the following graph from the Verizon 2016 Data Breach Investigation Report, the different cost categories are ordered from first to last. The first phase includes up-front costs which are incurred when you think you have suffered a loss and are receiving third-party guidance and investigative services to determine what happened and establishing how bad it was. Then come the long term costs involving legal representation, settlements and fines. It is important to understand what might not be covered by insurance. As noted in the Verizon report, many cyber insurance policies do not include coverage for remediation costs or judgments to pay punitive damages, each being potentially expensive on its own. In many jurisdictions, punitive damages are not even legally insurable. These costs are not nearly as common, in comparison with the more upfront costs.

Attorneys and investigators do not charge by the number of records breached, but typically on an hourly basis for a fixed number established by a pre-existing retainer, or on demand. Develop relationships before their services are required, and ensure you have processes in place to quickly provide the level of access and information needed. A goal is to ensure hours are not spent looking for a network diagram or SLAs while lawyers and forensic investigators are waiting in the conference room.



III. Industry Challenges[ii]

Providing cyber coverage is a relatively new product line for the insurance industry. The challenge is that there is very little actuarial data on which to determine appropriate coverage costs, coupled with the issue that cyber is a very dynamic area. Threats and vulnerabilities are changing at a rapid rate and the scope of a breach can be enormous. A lack of sufficient metrics with respect to frequency and severity of loss, specifically with Personally Identifiable Information (PII) and Personal Health Information (PHI) assets, and physical destruction as a result of cyber events makes pricing risk a challenge.

Other events that are possible via cyberattack, that do not involve the unauthorized disclosure of protected records, include extortion payout (and ransomware is epidemic) and disruption of critical services through compromise or denial of service. Costs associated with these events may be estimated, however the range is broad and again, not enough actuarial data exists to make credible assumptions about the degree of liability. In the case of the public sector, disruption of critical services such as radio systems for police and fire, water purification, waste treatment, and even traffic management may result in loss of life.

Fundamentally, insurers look for a strong security culture within the company as a first step in risk triage. Additional factors such as industry, revenue size, geography, and actual assets at risk contribute to how risk is priced.

The evolving nature of cyber threats (e.g. ransomware) and the IT environment (virtualization, the Internet of Things, and the Cloud), compounds the problem of developing accurate actuarial data.

The supply of insurance available to meet market demand depends on the financial ability to accept risk. For an individual insurer, capacity is the maximum amount of risk it can underwrite based on its financial condition. As the cyber insurance market capacity grows, more meaningful limits will develop as loss data accumulates and risk modeling matures.

In addition, aggregation of risk is a very important issue for insurance companies. Aggregation refers to the consequences of concentrated and cascading cyber risks where key aggregation attributes such as internet failure, compromised services providers, or a number of organizations in the same (or different) sectors using the same IT system where something happens to that system and affects all of the organizations in that industry.

This is particularly notable as cloud computing becomes more ubiquitous, one successful attack or failure of a cloud host could cause losses to hundreds of thousands of parties who hold their data within the cloud.

While it’s a best practice to include information security clauses in appropriate vendor contracts, many organizations are now requiring vendors to have cyber liability insurance. Even if a breach was caused by a vendor/third party, the organization still owns the information and is responsible for it. Citizens/customers will fault the organization as the primary custodian—not the vendor.

Insurance companies also are dealing with varying interpretations of the law. Recently, a Federal appeals court in Virginia upheld a lower Federal court in ruling that a commercial general liability policy (CGL) may cover a data breach. In a case involving the publication of private medical records on the Internet, the courts found that coverage included in a CGL for personal and advertising injury applied. The ruling by the U.S. Court of Appeals for the 4th Circuit was a defeat for Travelers Insurance which had argued its 2012 and 2013 CGL policies did not require it to defend its insured, Portal Healthcare Solutions, which was being sued over a data breach.

IV. Reasons to Invest In Cyber Insurance[iii]

There are numerous reasons to invest in cyber insurance, and following are a few to consider:

- The threat landscape is dynamic and there are a growing number of adversaries. Organizations are outmatched in their ability to combat cyberattacks from nation states, global criminals and malicious insiders.
- Cybersecurity has become an issue for states and local governments and they are increasingly looking to cybersecurity insurance as a financial instrument for transferring risk as part of their enterprise-wide risk management strategy. Cybersecurity involves the entire organization, including stakeholder domains outside the IT dept. Driving a culture of collaboration between stakeholders is challenging, but the underwriting process can be a catalyst for better security throughout the organization.
- Regulatory risk is increasing as states, the Federal government, and other regulatory bodies continue to pass tougher laws. The NIST framework is increasingly being viewed by many in the legal community as creating a standard of care to be used by plaintiff attorneys to allege lack of sufficient oversight and even negligence.
- Legislators are beginning to give greater legitimacy to the role of cybersecurity insurance. There is growing support for market-based incentives such as insurance that rewards strong cybersecurity programs with discounted premiums and broader coverage. The lack of robust actuarial data to model risk and a challenging underwriting process that validates the dynamic threat environment is a growing priority for the insurance industry.
- Adversaries are increasingly focused on third parties such as managed service providers, off-premise maintenance, and even cloud services that have access to sensitive information and other critical assets of the target enterprise. Liability for PII or PHI typically still rests with the data enterprise owner, even though a breach may have occurred at, or been the fault of, a third party.
- Attacks from the inside continue to be difficult to prevent. Cybersecurity insurance

typically provides coverage when the employee is the perpetrator, just like when the attack is from the outside. This probably will not extend to acts involving members of the executive team however. When asked who posed the biggest internal threat to corporate data, 55% of the respondents to the 2015 Vormetric Insider Threat Report identified Privileged Users, followed by contractors, service providers, and business partners.

- Security does not equal compliance because compliance standards are essentially minimum requirements. Treating information security as a compliance issue distracts from implementing a comprehensive program and ultimately results in a false sense of security. Many companies have been in compliance with their required standards and still fell victim to a data breach or a security incident.
- One of the biggest challenges continues to be quantifying cybersecurity risk in terms of dollars and cents. The premium charged by an insurance company can help solve this problem, especially when implementation of security controls and policies reduces overall risk.
- States and local governments responsible for operational technology, industrial control and SCADA (Supervisory Control And Data Acquisition) systems are particularly vulnerable due to the often very distributed nature of the OT/ICS environment. Built primarily for 24/7/365 availability and to operate in remote and isolated environments, these systems and devices have historically been air gapped but are increasingly being connected to the corporate information technology network and the Internet.

Assessment Tools & Services

Many organizations may not have the tools to effectively evaluate their risks, however, a number of product and service companies have joined the market for automating the risk assessment process for cybersecurity insurance. Underwriters are using (and developing) risk assessment products and services to require a higher level of risk maturity for potential customers. This is a very important development as cybersecurity insurance customers can take advantage of these risk assessment products and services to validate their maturity for underwriters and to drive down the cost of premiums

The ‘Fine Print’ and Exclusion Clauses:

An exclusion clause, i.e., ‘the fine print’, is a clause in an insurance contract that eliminates coverage for specified events. It’s important organizations understand what the restrictions are in the policy, including exclusion clauses, before executing the contract.

Example: the Company shall not be liable for Loss on account of any Claim based upon, arising from, or in consequence of any fact, circumstance, situation, transaction, event, act or omission

of which any insured had knowledge prior to the inception date of the first Liability Insurance Policy issues and continuously renewed by the Company to the Parent Organization.

V. Key Coverage Items[iv]

Following are some key coverage items to consider and discuss with a broker or insurance company before signing a contract:

1. Full Prior Acts coverage – Insurers typically try to limit coverage to acts from the first day the policy begins, known as the retroactive date. However, in the context of the challenges in detecting an attack, buyers can seek to remove this exclusion and avoid the risk of a claim denial.
2. Restrict knowledge and notice of a circumstance to the executive team – It may be beneficial to avoid allowing the insurer to attribute liability to the whole enterprise, because enterprise-wide detection has proven to be a challenge for most organizations.
3. Warranty – It may be possible to remove language that tries to warrant that security is maintained to the same level as represented in the underwriting submission. The dynamic nature of the risk leaves this open to insurer interpretation in the event of a loss.
4. Operational Technology – The majority of insurance policies provide coverage only to the corporate IT network. If relevant, it may be beneficial to broaden that language to also address operational technology such as SCADA and industrial control systems.
5. Outside Counsel – It may be preferable to agree on outside counsel at the outset. In the event of a security breach, a dedicated legal expert can take the response lead, including attorney-client privilege. Negotiating with an insurer during a security incident may not be advisable.
6. IT Forensics – Similar to choice of counsel, the preferred forensics firm can be agreed upon up front, rather than leaving the decision to the underwriter. Incident response and forensics can be very expensive and a significant part of the overall incident cost.
7. Law enforcement – Law enforcement is typically involved in major security breaches. Frequently, the first time a company knows it has been victimized is when the FBI calls. As such, it may be advisable to prevent the insurer from excluding claims for "failure to disclose as soon as practicable," for instances where law enforcement has advised nondisclosure during the investigation.
8. War & terrorism – Many insurance policies exclude coverage for acts of war such as invasion, insurrection, revolution, military coup and terrorism. With the emergence and growth of the nation state adversaries, it may be possible to eliminate this clause from a cyber liability insurance contract.
9. Intentional Act – This coverage addresses an employee or insider as perpetrator acting in isolation of the executive team.
10. Continuity of Coverage – When renewing an insurance policy with the same insurer, firms may be able to avoid signing a warranty regarding a circumstance or claim.

In addition, it may be beneficial to work with the insurer to identify an outside public relations firm. Expert advice on communications is a critical component during a breach, as there are numerous audiences to interact with: citizens, media, etc. Avoiding a communication faux pas is highly recommended during an already very stressful situation.

It is important to note that several large insurance companies provide lists of pre-qualified experts (legal, forensics, PR, etc.). It is easier to have expenses covered for these services if you select consultants from their roster.

If this feature is available through your insurance provider, it is advantageous to research and identify the best matches for your organization and then establish business relationships. Response activities will go more smoothly if you've had discussions with firms you want to work with prior to a breach.

If possible, it is beneficial to have some of these experts review your incident response plan and provide feedback as they have experience assisting entities during a breach. You also can consider inviting them to participate in, or at least observe at, your next incident response exercise.

VI. Questions to Consider

No two organizations are the same when it comes to cyber risks, therefore it is key to understand the cyber risks your entity faces and to ensure your cyber policy is tailored to mirror those risks.

It is equally important to note all policies have a set of exclusions, terms and definitions. Understanding these is essential. On the next page are some additional questions to consider discussing with your insurance broker or agent[v]:

Cyber Liability Insurance		
Questions to Consider	**Y**	**N**
Are there security controls you can put into place that will reduce the premium?		
Will you have to undertake a security risk review of some sort? If so, is it a self-assessment or conducted by an external entity.		
Are you expected to take actions to reduce or limit the risks? And if so, what are they?		
Will you get a reduction for each year you do not claim?		
Is any assistance provided to improve information governance and information security?		
Will there be an increase to your future premiums if you make a claim? If so, what and how big?		
Will there be any support provided to assist in making the right security decisions for your organization?		
As the security / protection industry is evolving quickly, will the insurance carrier ensure your policy is current? If so, how?		
Do all portable media/computing devices need to be encrypted?		
Is unencrypted media in the care or control of your third-party processors covered?		
Are malicious acts by employees covered?		
Will you have to provide evidence of compliance to relevant regulations and standards to prove you were not acting inappropriately?		
Although ignorance of the law is no excuse, if you are not able to keep up with all the compliance regulations enacted in all the states you interact with or where your employees/clients reside, would a claim be refused if you contravene laws in one state but not another – because insurance policies often stipulate you must not be breaking the law?		
Is the policy clear on what happens if there is uncertainty around whether the incident took place a day before the coverage was in place or on the day?		
Are the limits for expenses grouped together in a way that the maximum limit covered is likely to be achieved very quickly, unless you increase the coverage?		
Are all and any court attendances to defend claims from others covered?		
Could you claim if you were not able to detect an intrusion until several months or years have elapsed, so you are outside the period of the coverage (such as the Heartbleed vulnerability that wasn't discovered/publicized for years)?		

3. Conclusion

The increasing risk and level of sophistication of cyber breaches are issues affecting all organizations in the private & public sectors. Depending on the scope of the breach and the type(s) of information compromised, the costs can escalate quickly. Examining the inclusion of cyber liability insurance as part of an overall risk management strategy is an important first step and it makes good business sense to determine viability—prior to a cyber breach. At a minimum, it provides an opportunity to evaluate the current information security protections in place and identify where improvements can be made.

Following are some concepts that are good food for thought[vi]:

Why is insurance a catalyst for security?

- Customer expectations are rising
- Regulators are enforcing compliance
- Legislators want to legislate
- Underwriters are incentivizing better security behavior

Cybersecurity insurance continues to evolve and these are likely developments we can anticipate:

- Continuous monitoring and risk scoring will be the new norm. This is the process of maintaining real time awareness of security threats and vulnerabilities that support organizational risk management decisions.
- Premiums and rates will vary monthly, weekly, daily, and hourly based on dynamic threat vulnerability environment
- Underwriters will establish new relationships with security product vendors to incentivize spending
- Insurance brokers will be better positioned to provide guidance on what coverage is best for your organization

Next Steps:

Next week, ask about and review your corporate cybersecurity insurance policy (if you have one). In the next three months:

- Review your most recent enterprise risk assessment
- Discuss your corporate cyber risk appetite with your executive leadership and risk officer
- Meet with your insurance broker to discuss your cybersecurity insurance policy or investigate purchasing a policy

In the next six months, begin budgeting and scheduling an enterprise risk assessment and considering potential tools or services to automate and provide visibility into your risk environment.

[i] "Cybersecurity." *Naic.org.* National Association of Insurance Commissioners & the Center for Insurance Policy and Research. 25 Jan 2016.
[ii] Weatherford, Mark. "Cyber Security Insurance: The Catalyst We've Been Waiting For." RSA Conference 2016. 2 Mar 2016.
[iii] Weatherford, "Cyber Security Insurance: The Catalyst We've Been Waiting For."
[iv] Weatherford, "Cyber Security Insurance: The Catalyst We've Been Waiting For."
[v] Sembhi, Sarb. "An Introduction to Cyber Liability Insurance Coverage." *ComputerWeekly.com*. Jul 2013.
[vi] Weatherford, "Cyber Security Insurance: The Catalyst We've Been Waiting For."