CYBER INSURANCE RADICALLY COMPLEX

March 28, 2024

CYBER HAWAII

ABOUT CYBERHAWAII

CyberHawaii is an information sharing and analysis non-profit organization committed to developing and enhancing Hawaii's cybersecurity capabilities

- CyberHawaii is committed to a whole community approach that will help to:
  - Mitigate cyber risks for all community members
  - Develop educational and workforce pathways for students
  - Augment cyber services being delivered by government agencies, commercial entities, research organizations and Community Based Organizations
  - Inform local decision makers about cyber security risks and solutions
- Founded 2016
- Part of CyberUSA network
- Supported by corporate memberships and grants

CYBER HAWAII

CyberHawaii is a non-profit, information sharing and workforce development organization that focuses on improving cyber resiliency in Hawaii's small and mid-size businesses as well as within the community as a whole.

CURRENT MEMBERS & KEY PARTNERS

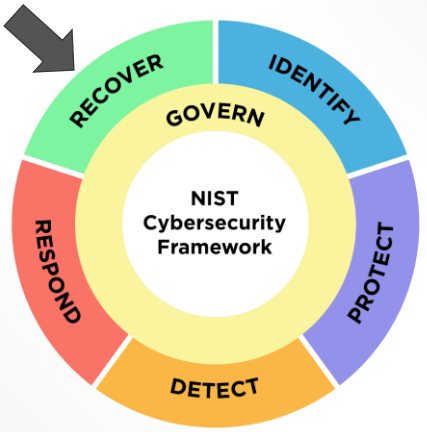
We are supported by the State of Hawaii, the University of Hawaii, private sector businesses and through partnerships with numerous agencies in Hawaii.

CYBER INSURANCE

It's my pleasure to welcome you to today's webinar that focuses on Cyber Insurance. This webinar is brought to you through a grant from the Hawaii Department of Business, Economic Development and Tourism and is supported by the Chamber of Commerce Hawaii and the Hawaii Defense Alliance.

CYBERSECURITY FRAMEWORK

- Cyber Insurance is a key part of a Cybersecurity framework
- Fits into the Recover section of the NIST model
  - Resources to recover
  - Can include data and identity recovery services
  - Preparation to deal with a data breach
- Business needs to demonstrate level of readiness



CYBER HAWAII

While most security presentations do not talk about cyber insurance, the fact is that it has an important place in a cybersecurity framework. The NIST cybersecurity framework is one of the most widely followed and calls out distinct control areas from Identify, Protect, Detect, Respond and Recover. Governance controls were most recently added that address risk management strategy and policies. Cyber insurance fits into the Recover controls section and focuses on things like providing resources to aid in recovery, data and identity recovery services and preparations needed to recover. A business must have a basic level of cybersecurity controls in order to qualify to obtain a cyber insurance policy.

WEBINAR PRESENTERS

Tammy Yamada

Vice President Commercial Lines

Pyramid Insurance

Mark A. Smith

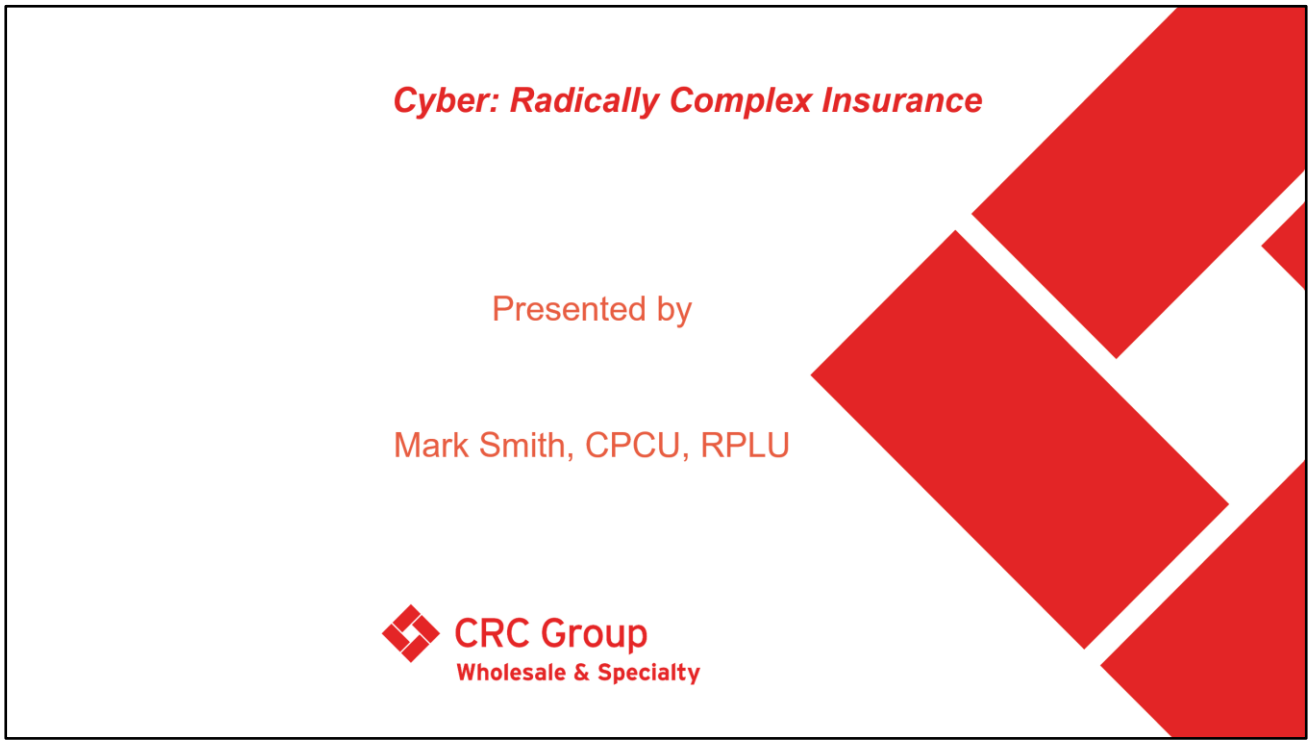
Senior Vice President

CRC Insurance

Questions should be entered into the Chat window and will be read at pauses in the presentation. This presentation is also being recorded and the recording will be available on the CyberHawaii website in a few days. During this presentation you're requested to remain on mute unless asking questions during designated Q&A sections.

Your presenters today are Tammy Yamada from Pyramid Insurance, a local full-service insurance agency. And Mark Smith of CRC Insurance, a wholesale and specialty insurance broker. At this point I'd like to turn the session

over to Tammy to move us forward.



Cyber Insurance is radically complex insurance. Why? It's simple because no other insurance product has so many moving parts! Depending on how you count, there are potentially up to twenty-two different coverages found in a single policy that respond to cybercrime losses. Uniquely, a cyber event triggering coverage under one insuring agreement, may spiral and simultaneously trigger other insuring agreements. As an illustration, think of a bowling alley. One throw of the ball strikes one pin and it topples over hitting another and then another until half or all are down, unless you are an awful bowler like me. It's often just like this with cyber claims. One cyber event and half or more of the coverages can be activated.

To better understand Cyber Insurance, today's presentation will be examining the insuring agreements, each of which are best understood by looking at specific claim examples. We will consider several reasons businesses should purchase cyber insurance, focusing on loss facts, claim costs, loss prevention and mitigation measures provided by insurers, then how to obtain the coverage and finally, what to expect when filing a claim.

Third Party Liability

- Network Security/Privacy Liability

8

All cyber carriers' have structured their policies into essentially two groups or sections. The first is for Third Party Liability claims, which allege harm arising from a wrongful act of an insured in securing, storing, or processing third party data in their possession or by a third-party vendor servicing data on their behalf. The second group is for First Party losses, indemnifying the insured for their own expenses or income loss arising from a cyber event as well as the option of cybercrime coverage for actual theft of an insured funds or funds they hold in escrow.

There are five third party insuring agreements in a cyber

policy. The first two are network security and privacy liability which are similar but different.

As an example of a network security claim, consider a hacker who has exploited a vulnerability in an insureds computer system, such as a weak Remote Desktop Protocol or port, resulting in a data breach evidenced by the hacker gaining access to personal identifiable information of the insured's customers, such as credit card, social security, passport, or driver's license numbers, essentially, any personal information not available to the public and protected by law. Affected individuals could bring suit for the thievery of their personal information if they became victims of identity theft, asserting the insured did not adequately protect their network from attack by eliminating the vulnerability. In addition, the information accessed might involve corporate confidential information held under a non-disclosure agreement. For instance, if the insured is a law firm, it could hold highly confidential Merger and Acquisition information, which if disclosed by a cybercriminal, could blow up a deal devasting the law firms' client.

Privacy liability arises out the unauthorized access or disclosure, of personal identifiable information in either

paper or an electronic format, as defined by state and federal privacy laws. This also includes patient healthcare information protected by HIPAA. A typical privacy claim does not arise out of network security failure but what I call an oops! This could involve a lost laptop with personal information or the theft of unshredded documents meant for destruction. For example, a doctor sent patient healthcare records to the wrong patient who has a similar name, or an accounting firm mailed important tax documents to the wrong clients when a mail clerk mixed up envelopes in the mail room. Or an attorney lost client files when riding home on the train after leaving a brief case behind on the seat. Any of the affected parties could bring a claim for damages from the unauthorized disclosure of their confidential or personal information. None of these claims involved a lack of network security but a mistake made by employees in handling information.

Third Party Liability

- Network Security/Privacy Liability
- Regulatory Defense, Fines & Penalties

Trend Alert

Regulatory agencies and State Attorney Generals are beginning to proactively investigate breaches and levy fines for non-compliance with security and privacy regulations. As a result, fines and penalties will become increasingly more common.

9

Regulatory Defense and Fines and Penalties is an additional third-party coverage. All fifty states, various branches of the federal government and even the European Union have data privacy laws including the requirement to protect personal identifiable data often by encryption as well as to supply prompt notice to affected individuals after the discovery of a data breach. If such notice is not provided on a timely basis as specified by law, regulatory authorities may bring suit. For example, a clinic accidentally lost thousands of paper patient records when they moved locations. The clinic, thinking they would eventually be recovered by their moving company who obviously moved them somewhere, did not want to

upset their patients and did nothing. But state and federal authorities became aware of their disappearance which is a privacy violation and brought a regulatory claim for failure to secure the records as well as for a notice violation, resulting in thousands of dollars in fines. I remember many years ago, a delivery truck was moving patient files from a hospital in Spokane, and the driver forgot to close the back door of the truck, and hundreds and hundreds of patient files went flying in the air as he drove up the South Hill for his next pickup. It certainly made the local evening news! This is obvious a case of the OOPS! No matter how good any entity's cyber security may be, privacy violations can still happen from the most unforeseen circumstances and the regulators are always watching.

Third Party Liability

- Network Security/Privacy Liability
- Regulatory Defense, Fines & Penalties
- PCI DSS Fines, Penalties & Assessments

10

A contractual coverage titled Payment Card Industry Data Security Standard Fines and Penalties, is a form of third-party coverage in these policies. A hotel group learned from their acquiring bank who processed their card transactions, their point-of-sale machine terminals were compromised and all credit card transactions for the week had somehow been skimmed by hackers who sold the stolen card data on the dark web. The Payment Card Industry (PCI) organization determined the hotel's Point-Of-Sale system was the source of the theft and found after an investigation, the hotel was not PCI – Data Security Standard compliant at the time of the event, a contractual violation of the card processing agreement. As

a result, the acquiring bank imposed contractually authorized fines and penalties to recover the fraudulent use of the cards and cost of their replacement to the tune of $270,000. The hotel was able to negotiate repayment over the course of two years out of their merchant account. This also happened to a small sporting goods store in Eugune Oregon a few years back which had to repay $50,000 in assessments. These claims are not as common now due to chip and pin technology but still do occur.

Third Party Liability

- Network Security/Privacy Liability
- Regulatory Defense, Fines & Penalties
- PCI DSS Fines, Penalties & Assessments
- Media

11

The final third-party coverage included in the policy is Media Liability, which is odd, as Media Liability does not involve any cybercrime theft except the theft of intellectual property, which lends credence to why I call cyber radically complex insurance. This covers media wrongful acts by or on behalf of the named insured, typically defined as the media perils of libel, slander, defamation, copyright and trademark infringement, product disparagement and plagiarism, to name a few, arising from the insureds media content, which may include websites, advertisements, blogs, social media posts as well any printed media. An example was a suit against an architectural firm who included a picture of

their downtown office building on their website. Another architectural firm who designed the building alleged the use of the photo of the building they designed was a violation of their architectural copyright as they argued the image on the website implied the insured had designed the building. They sued for damages and won almost a million dollars.

As I said before in my bowling pin analogy, it is very possible a single data breach may involve more than one of these third-party coverages. For example, in the skimming attack on the hotel mentioned earlier, it could trigger a third-party network security claim by credit card holders who found fraudulent activity on their cards resulted in damage to their credit scores including loan denials or a regulatory claim if the hotel failed to notify affected card holders, in addition to the PCI DSS claim which occurred.

First Party Loss

- Breach Response
- Extortion
- Data/System Restoration/Bricking
- Business Income/System Failure
- Reputational Harm

12

Let's look at first party loss coverages. These insuring agreements indemnify the insured for expenses paid to respond to a data breach, the payment of an extortion demand, a loss of income or the loss of money.

Breach Response coverage supplies payment for expenses incurred in a suspected data breach. For example, if a firm believes it has been penetrated by a hacker, the insured will reach out to their insurer who engages a forensic investigation firm to determine how it happened and what if any data had been affected. This can be very costly. In Montana, a technology firm who was breached spent over $500,000 alone on a forensic investigation and never did

determine the source of their attack. Once the forensic firm determines what data has been compromised or stolen, this information in turn is supplied back to an attorney to evaluate the data and decide if a state or federal breach law requires notice to affected individuals. Now keep in mind, the lawyer must look at the residency of each affected individual and evaluate their home state's data breach laws to determine if notice is required. If yes, then the law firm draft's the notification documents particular to the state in which each affected person resides, these notices will then be sent to a fulfillment firm for printing and mailing, a call center set up to handle inquiries by affected individuals after their receipt of the notice, and credit monitoring may be offered to each affected person depending on the data compromised. Finally, a public relations firm will be hired to engage with the press to protect the insureds reputation. All of this is extremely expensive. It is especially expensive if the entity does not have cyber insurance and must engage on the fly individual vendors or lawyers to provide these services on an emergency basis. They can charge sky rates much higher than what they charge insurance companies who have negotiated their rates downward, as the entity has no choice but to respond to the breach quickly.

In case of a ransomware claim, hackers either encrypt or exfiltrate the insureds data, lock down the insured's computer network, or do all three. They will make a ransom demand of bitcoin before providing the encryption keys to unlock the insureds data or network. If the ransom is not paid, they will destroy the data, sell, or make it public, the latter two are known as double extortion. Even worse, they may extort any individuals whose data they have stolen from the insured which is known as triple extortion. Breach response coverage will pay the cost for forensics to determine the affected data and how it was attacked, and Extortion coverage will indemnify the insured for any ransom payment made to the criminals, as well as expenses incurred in negotiating and securing the bitcoin payment. The decision whether to pay the criminals their extortion demand is tough one. It is best mitigated by having encrypted offline backups routinely evaluated, but even these can sometimes be corrupted or incompletely backed up. Unfortunately, even if the ransom is paid, many victims do not always get all their data back if at all. If the criminals exfiltrate the insureds data and threaten to sell or make it public, this is an extraordinarily strong incentive to pay the ransom and protect the stolen data. When the data is exfiltrated, this is normally considered a data breach and the breach response process I have mentioned commences.

In the event the hackers damage or destroy the insureds electronic data or computer systems or if the insured elects not to pay the ransom and later finds it impossible to restore their data from backups, Data and Systems Restoration coverage will pay the costs to restore, repair, or may even re-create the affected electronic data or software systems. This may be as simple as paying IT experts to help restore the data from backups or as complicated as paying the insured the costs to recreate the damaged or destroyed data. For example, an A&E firm fell victim to a ransomware attack when all their data was encrypted. Choosing not to pay the ransom, the firm chose instead to download their cloud-based backups. Unfortunately, ah you know where this is going, all their backups failed, which is not particularly uncommon. It was discovered they had not assessed the effectiveness of the backup process before the attack. The firm paid out $20,000 for forensics (breach response costs) and over $270,000 to pay engineers on staff to recreate data they had lost vital to continuing their business and meet contractual requirements. If the cyber-attack had been so extreme that the insured's computer hardware itself was damaged, and the cost to repair exceeded the cost of replacement, Bricking coverage would kick in to replace

damaged hardware.

Business income exposures can be covered as well. Business Interruption coverage will pay for the loss of income and extra expenses if a loss is a result of a network security failure. For example, a restaurant whose point-of-sale system was shut down by a malware attack could only accept cash, so they lost significant income until their system was restored as they could not accept credit cards. Cyber business interruption will pay for this type of income loss for up to between 180 to 360 days, what is known as the period of restoration or until the system is fully restored if earlier, after the insured provides a proof of loss. There is normally an hourly waiting period before the coverage kicks in, anywhere from six to twelve hours, depending on the insurer. The business income coverage is often modified to include systems failure coverage, which is not related to a network security failure, but an unplanned, unintentional, or unexpected shutdown of a computer system resulting in lost income. This could arise from a software installation gone haywire, hardware failure or an accident, it does not include a shut down due to power failure or an interruption of the internet itself.

Policies may also include dependent business interruption

and or dependent systems failure for losses arising out of a security failure or unplanned system interruption of an Internet Technology vendor, like a Managed Services Provider, Point of Sale vendor, Application Services Provider, or other business services provider like an accounting, fulfillment, or payroll firm. Some carriers even expand their coverage to apply to a supply chain partner, which provides products or services to the insured under a written contract. This last point is especially important, there must be a written contract with the vendor or coverage will not apply. In a recent claim, a midwestern title company used an Application Services Provider to host their network and all online applications and underwriting platforms. The ASP suffered a ransomware attack, how it occurred we do not know, shutting down all customers platforms as well as the destruction of customer records as their backups were found to be corrupted in the attack. The title company lost over $1M in revenue as well as extra expenses incurred as they had to scramble and find new software to relaunch their underwriting platform which took five months. Had the ASP experienced an unplanned interruption of their network instead of a ransomware attack, the dependent system failure coverage would have kicked in.

One more form of business income coverage is often included in the policies is known as reputational harm. In the event of an adverse public media report of cyber extortion, data breach or security failure affecting an insureds client, the policy will pay the net profit after taxes that would have been earned had such a report not been made. A typical waiting period of two weeks after the report applies and the policy provides an indemnity period of between 60 and 360 days depending on the policy form. This coverage recognizes the immediate loss of trust of clients after a cyber-attack involving their data goes public. For example, a law firm was a victim of a network security attack in which an attorney opened a phishing email allowing criminals to access and steal client data. The media made the attack public and several of the law firm's clients terminated their relationship, leading to a loss of income during the period of indemnity. A few firms have gone bankrupt following such reports after losing most of their clients.

First Party Loss

- Cyber Crime
  - Computer Crime
  - Funds Transfer
  - Social Engineering
  - Invoice Manipulation
  - Telephone Fraud
  - Cryptojacking/Utility Fraud

13

Cyber policies offer several individual crime coverages typically purchased on a commercial crime policy. This means there may be a coverage overlap for those insureds already buying crime. These are often written at a sublimit of between $100K and $250K. A recap of these coverages includes the following:

Computer Crime. Cyber criminals penetrate the insureds computer system gaining access to the insureds online banking application and send fraudulent electronic instructions to the insureds bank to transfer money to the criminals ’own bank.

Funds Transfer Fraud. Criminals send electronic wire transfer instructions to a financial institution impersonating the insured instructing them to wire money to themselves.

Social Engineering or Fraudulent Instruction Coverage. This is the most common crime loss businesses of all sizes are incurring. The criminals send fraudulent wire transfer instructions by voice, text, or other electronic means to the insured impersonating an insured person, customer, business partner or vendor, which instructs the insured to transfer money or securities. Some policy forms also include funds held in escrow as well as the transfer of tangible property. A contractor thinking it was receiving a request from a construction equipment dealer to change their bank routing instructions on an invoice fell victim to this fraud and wired a Chinese fraudster $2.5M which they could not recover. In all cases, the best way to deter this fraud is to implement mandatory call backs to a pre-determined number with the company or person making the change request.

Invoice Manipulation. The criminals penetrate the

insureds computer system and view outstanding invoices, then they impersonate the insured, and send fraudulent instructions to a customer instructing them of new payment instructions directing payment to themselves. This coverage reimburses the named insured if it cannot collect payment from their customer of an outstanding invoice which was paid to the criminals.

Telephone Hacking. This reimburses the insured because of a hack of their telephone system, for the cost of unauthorized calls by the perpetrator.

Cryptojacking. This reimburses the insured for loss resulting from the unauthorized use of the insureds computer system by a third party for the sole purpose of cryptocurrency mining or other computational uses.

Now that we have reviewed the basic content in a cyber policy, I need to provide some context. First, there is no standardized Cyber Insurance policy among the over 75 insurance carriers offering this coverage. Each insurance carrier has drafted their own policy form, many of which are significantly different from each other. The differences lie primarily in the definitions of the coverages themselves, policy exclusions and or use of endorsements

or a limitation on the number of insuring agreements they provide. Some insurers may want to restrict extortion payments for a ransomware attack to only $250,000 for example. Some add exclusions for loss involving biometric data, others for loss alleging the wrongful collection of data, often involving pixel, or tracking technology. Another example, one insurer's definition of dependent system failure only applies to the unexpected outage of a computer system of an IT Vendor who is hosting a computer network for an insured. Yet another carrier's same coverage is much broader as it will apply to any third party who provides a product or service to the insured under a written contract or what we know as a supply chain partner. For a contractor, who is expecting a shipment of building materials from a supplier who has signed a contract of delivery on a specified date, if the supplier is a victim of a cyber-attack, their delivery could be seriously delayed, leading to the contractor's loss of income if the contractor's client fires them due to the delay. This is just one example of how minor differences in a policy can be significant.

It is important to work with a local retailer insurance broker like Pyramid Insurance who is familiar with these differences and can offer a policy based on the coverage, not just the lowest price.

Why should a firm buy cyber? Obviously, the scope of the cyber policy coverages speak for themselves, these policies are incredibly comprehensive in scope, radically so as I have said before, providing tremendous protection for the buyer. Secondly, CFC a major cyber insurer reported in 2023 that 96% of all cyber-attacks were directed at small and medium sized businesses, noting these firms have less than state of the art cyber security and criminal organizations view them as low hanging fruit. In their 2023 Cyber Security report, Hiscox Insurance surveyed over 5,000 small businesses and found the following. Fifty-three percent had at least one cyber-attack and of those with under ten employees, 36% had

been victims. Other loss facts found the number one cause of loss was a social engineering attack, or payment diversion, arising out of phishing fraud. I think we should take a quick pause and review what phishing fraud entails since this is a leading attack vector. A criminal sends an email appearing to be authentic or from a known source with the intent to persuade the insured to either disclose information, such as a request to update password information (allowing the hacker into the insureds network), click on a link or download an application which contains malware or ransomware. The email often conveys a sense of urgency or something to pique interest, like" 2024 bonus pool information" or "Urgent, HR Complaint filed today, please respond immediately!" Now note, in one study, it was reported 23% of all employees opened a phishing email. This is not hard to understand. Normally the phishing email address will be off by one letter so instead of msmith@crcgroup.com, it may be masmith@crcgroup.com. Every organization should require ongoing anti-phishing training including ongoing simulated phishing attacks, testing employees at all levels of an organization. The second leading cause reported was a ransomware attack often because of a successful phishing attack. One of five surveyed had experienced such an attack and less than half recovered all their data after paying the ransom.

Another reason to purchase cyber insurance are the claims costs. What do these look like? There is no national centralized aggregator of cyber claim statistics, however, the reports offered by the cyber carriers on their own losses is highly informative and sobering. Coalition, a leading cyber insurer for small business reported in their 2023 cyber claim report for all causes of loss, the average loss payment was $197,000. Unlike in the Hiscox report, Coalition reported ransomware their leading loss with an average extortion demand of $1.8M with the actual payment negotiated down to $303,000. Their second leading cause of loss, fund transfer fraud, the payment was $199,000, with the highest percentage of firms attacked under $25M in gross revenue. Hiscox reported in their cyber survey one of eight of all firms paid out more than $250,000 per claim. Given the size of these loss payments most small businesses would not be able to pay these amounts and continue in business. In one claim study, it was found that over 50% of small businesses did not survive a cyber-attack so maintaining a cyber insurance policy is an important consideration.

A further reason for purchasing cyber is loss prevention and loss mitigation. Many cyber carriers offering coverage

provide extremely detailed loss prevention recommendations after conducting free vulnerability scans as part of their underwriting process. These scans look inward to identify and review a company's internet facing assets and look for weaknesses such as unscanned software, stolen information on the dark web, open RDP ports and other significant vulnerabilities. It is like hiring someone to stop by your house and look for unlocked doors or open windows. Some firms offer insureds on day one of a policy's inception 24/7 active threat intelligence security scanning services to alert of any newly found vulnerabilities or specific threat actors. When something is found, they alert their insureds immediately with suggestions for actions to take. These alerts should be taken seriously, and not as some critique of an insureds IT security personnel. Some insurers also provide free or heavily discounted managed risk solutions such as multi factor authentication, end point protection and other security tools. A few even offer virtual CISO's to assist with any ongoing security questions. As previously noted, the number one reason cyber criminals attack small businesses is because of poor cyber security and the number one vector of attack are phishing emails typically resulting in ransomware or funds transfer fraud.

With respects to loss mitigation, the insurance carriers can provide significant benefits which we will discuss when we review how to file a claim.

A further reason to purchase this coverage is it may be a contractual requirement to secure a contract. It is routine for companies to require cyber insurance and agree to include their clients as additional insureds as well as to indemnify them for any loss arising out of a cyber event involving client data. A final reason to buy cyber is many cyber events arise out of a cyber-attack against a third-party vendor who is hosting or storing an insureds data. A loss or disclosure of a company's data by a third- party vendor does not relieve the original owner or collector of that data from data privacy laws. The data owner, not the data holder is responsible for notification of the affected individuals of a cyber event

How to Get Coverage?

- Application
- Limits
- Security Requirements
- Pricing

15

So how does an organization secure coverage? The first step is to work with a local retail insurance agency like Pyramid Insurance who can access carriers who can offer a non-binding indication by simply providing your address, nature of operations, yearend gross revenue, employee count and loss history. However, it is normally best to complete an application detailing existing cyber security measures in place for your agent to market as this may result in better pricing. Please note, not all organizations will qualify for coverage, depending on the nature of business and the data they hold, unless MFA, endpoint detection and encrypted offline backups are in place prior to binding coverage.

By default, most small businesses purchase a $1M limit. Given the size of the typical ransomware payment and the cost of forensic investigations can easily exceed $100K, higher limits should be considered, especially if the organization has a high number of confidential records at risk. Limits of up to $10M or more are available. Cyber is rated off revenue for either the past or projected 12 months, with consideration given to the nature of the risk, number of confidential records and existing cyber security measures in place. Pricing can start as low as $1,500 for small businesses.

How to File Claim?

- Carrier Hotline
- What to Expect
- Proof of Loss

16

So how is a claim filed? All cyber carriers have a claim hotline staffed 24 hours a day. If there is the mere suspicion of a breach or other attack, it is imperative to contact the hotline asap as well as let your agent know of the incident. The hotline personnel will assign a breach coach within 24 hours or less who will quarterback a mitigation response. As noted earlier, a forensic investigation firm will be engaged to determine the source of the attack, the scope of the attack and the data that may be at risk. This will in turn be sent to the attorney who will determine if the attack reaches the level of a breach under state or federal law and if notification is required. If it is, the attorney will draft a notification letter and hire a fulfillment firm to send out notifications and if credit monitoring is warranted, engage a credit monitoring company to monitor affected individuals. A call center will also be set up to take calls from affected individuals. Lastly, the insurer will engage a public relations firm to manage the insureds public response to protect their reputation. If the incident involves an extortion demand, the carrier will work with the insured to determine the best course of action and to assist them in the process of negotiating and paying the ransom in bitcoin. If it is a funds transfer loss, they will work with the insured's financial institution to see if the payment can be stopped or mitigated to reduce the loss. Lastly if a lawsuit arises, the carrier will hire an attorney to provide defense.

With respect to business income or reputational harm losses as well as any type of cybercrime losses, the insured will need to provide a proof of loss. This usually requires hiring a forensic accounting firm to assist the insured in quantifying the loss. Most insurers will pay for their assistance. This is one area where there may be profound disagreement with the carrier in terms of what qualifies as a loss, and it can take a considerable amount of time work out an agreement.

Recap

- Comprehensive
- Ooops
- Bad Actors
- Asset Protection
- Experts
  - Pre-Attack
  - Post Attack

17

To recap, as we have reviewed the policy, it is certainly a radically complex insurance policy, covering first and third-party losses, including breach response costs, lost business income, PCI related contractual damages, media liability, regulatory fines or penalties, damage to hardware and crime.

The policy responds to both Oops, mistakes by employees including the loss of data in paper form as well as the malicious attacks of cyber criminals. It also responds when a third party in possession of an insured's data is responsible for a breach or loss of business income.

The coverage provides asset protection for the insured to financially respond to these attacks and pay any resulting losses which can be extremely expensive and or crippling for smaller organizations.

Finally, it provides immediate access to experts. In the late 1700's the origin of many insurance companies started with local fire brigades. For example, in the city of London, homeowners or businessowners would pay a small premium to a local fire brigade to insure they would later respond to fight a fire at their property. If they had not hired a brigade in advance, the property owner was on their own to put out the fire. Some of these brigades morphed into insurance companies like Fireman's Fund and Cigna. So, it is now with cyber insurance. The insurance companies have contracted not with fire brigades but with mitigation firms to provide experts like ransomware negotiators, forensic investigators, law firms specializing in privacy laws, fulfillment, and credit monitoring firms, and more to respond immediately on behalf of an insured in the wake of a cyber-attack, providing peace of mind for smaller organizations their claim is managed by industry experts devoted to responding to a cyber-attack. How many companies know

exactly what to do if they experience a data breach or ransomware attack? Who are they going to call, what prices will they have to pay for an emergency response? The insurance companies have removed this uncertainty. These losses can be complex, radically complex and it takes a radically complex policy to respond.

QUESTIONS?

Pyramid Insurance Centre, Ltd

Pyramid Insurance offers Cyber Liability Insurance tailored to your specific needs. We are committed to delivering exceptional service. Our experienced agents will work with you to fulfill your business objectives.

For more information or to receive a quote, contact:
Tammy Yamada
Vice President, Commercial Lines
Phone: (808) 527-7294
Email: tammy.yamada@pyramidins.com

Pyramid Insurance has been serving the people and businesses in Hawaii for over 30 years. Locally owned and managed, Pyramid is one of the top insurance agencies in the state.

www.pyramidins.com

Follow us on Social Media

FOLLOW US ON LINKEDIN
Pyramid Insurance Centre, Ltd.

Follow us on Instagram
@pyramidinshi

FOLLOW US ON facebook
@pyramidinshi

SUMMARY *Mahalo*

- Cyber insurance is an integral part of a Cybersecurity Framework
- Many options exist to meet different business needs
- Cyber insurance should be part of your business risk management strategy
- Contact your local insurance broker to discuss policy options

Next Event
Cybersecurity Mentorship
Tuesday April 02, 2024
2pm
CISA/Servco/CyberHawaii
www.cyberhawaii.org

CRC Group
Wholesale & Specialty

PYRAMID INSURANCE

CYBER HAWAII