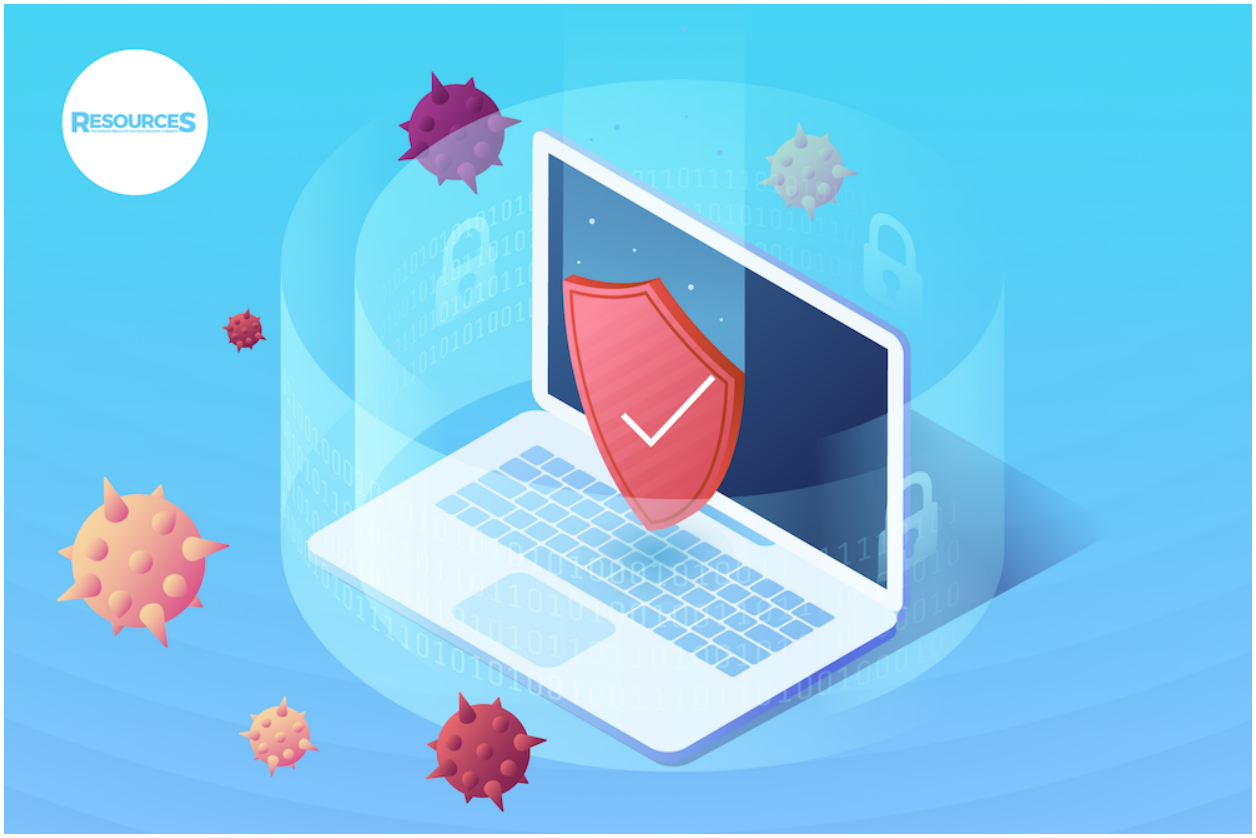

Managing Cyber Exposure

2020 and Beyond

THE NATIONAL ALLIANCE
for Insurance Education & Research

Table of Contents

OVERVIEW

Cybercrime and Changing Coverage Demands

The industry is seeing an increased interest in coverage related to cyber liability, and particularly first-party coverage. Where the focus once was on third-party liability, we're now seeing an appetite for cybercrime coverage that is separate from traditional crime insurance programs. Clients are now asking for broader extortion coverage, business income, and extra expenses. Data restoration costs are also at the forefront of many customers' minds, which requires the marketplace to remain nimble in response to cyber liability.

Data Breach Sources and Associated Costs

The IBM and Ponemon Institute Cost of Breach Report provides some excellent data on costs that risk managers should take into consideration.

For example, human error accounts for 23% of all data breaches and costs an average of $3.3 million. System glitches account for 25% of breaches. Vendor errors cost between $2 billion and $3 billion. But the big threats to watch for are malicious attacks. These attacks account for a whopping 52% of all cyber losses, averaging a global cost of $4,270,000. Of these malicious attacks, 19% are caused by compromised credentials. Another 19% are caused by cloud misconfiguration, and about 13% are caused by hackers. Hackers alone create an average of $4.4 million worth of loss.

Size Matters

The Ponemon study also included some interesting information regarding a business' size and potential losses.

For a business of 500 employees, the average breach costs were about $2.3 to 2.5 million. The average for an entity that has between 500 to 1,000 employees is $2.63 million. For those with 1,000 to 5,000 employees, the cost is $4.09 million on an average basis. If you have 5,000 to 10,000 employees, costs come in around $5.15 million.

This employee data tells us that larger employee groups tend to have more sophisticated tech needs and the staff to meet them. However, when businesses have only about 500 employees they usually have no tech staff, which causes heavy reliance on vendors and vendor-type aspects.

How can we prevent catastrophic losses?

Forensics, special computer systems, firewalls, and audits help agencies build better crisis management, communication, and education about cyber risks for their clients.

Here are some things to consider when performing a risk assessment for your clients:

- What is the enterprise doing to protect itself?
- What notification activities happen when a breach occurs?
- What are the costs for outbound calls and general notices, as well as state and federal regulatory requirements?
- Will you need to engage outside experts to help with brand and reputation?
- What is the total loss of business? What about the loss of customers?

Things Will Stack Up

If a hack on your computer system involved credit information, studies estimate that you could lose upwards of 30% of your customer base. Often, these customers will not return after the breach.

What are the three most important things agency clients can do?

- Get recertified with your credit card companies
- Get a compliance audit
- Handle the fines and penalties you are obligated to pay under consumer law

Agents Should Focus on "the 2020 Problem"

Malicious data breaches are the fastest-growing threat that the marketplace needs to address. These breaches account for about 50% of all exposures, but it's really the ransomware and destructive malware that cause the biggest problems. This is the problem: We are now seeing destructive malware, such as wiper-style attacks, which create an average of $4.62 million worth of loss. The COVID-19 pandemic has impacted the significant increase in ransomware claims as well because many people now work from home. This alone is reason enough to focus on this cyber security issue.

The increased cost of providing goods and services online has also increased the importance of ensuring online business activities follow cyber security measures. Despite that, you must understand that ransomware will still come in. Today, insurance

companies are not offering any kind of pandemic-related extensions for cyber liability products. Ransomware coverages are starting to come out with significant increases in deductibles, creating even more challenges for insurance and risk management professionals. Be sure that you understand what ransomware is.

How can you help clients control cyber threats?

First, clients must understand that cybercrime is a huge risk management issue, meaning a combination of risk management techniques and special insurance products are needed in order to create solutions. Agents should provide value-added services in terms of risk controls and risk prevention techniques. An agent has a lot of work that needs to be completed long before a client calls and says, "I've got a ransomware attack. What do I do?"

The first step in risk management is risk identification. Once the risk is identified, agents can then consider the scope of the exposure as they complete their analysis. This process helps agents understand the extent of the potential risk and helps the client identify the potential costs associated with a breach.

Once Bitten, Twice Shy

If clients have been the victim of ransomware attacks, they can expect future attacks within the next 14-22 months. These future attacks often result in paying double the initial ransom. Since hackers already know the business is susceptible to cyberattacks and are banking on the chance your clients may have forgotten the previous ransomware attack, they will come back. Make sure your clients aren't still low-hanging fruit.

Learn your lessons. Here's a quick list:

- Complete all protections and put endpoint protections in place
- Double your efforts at loss reduction
- Get the proper cyber insurance in place
- Enhance essential coverages: DLP or data loss prevention, controls, spam filters
- Make sure your backups are properly screened
- Set up better network segmentation
- Have better firewalls and segmenting items
- Increase the security education for the employees

But wait, there's more!

Educate and prepare your clients for:

- Fines and penalties
- Increased cyber insurance costs
- Higher deductibles and other cost increases

Takeaway

Remember that the average time it takes to detect and contain a data breach (based on the Ponemon study) is 280 days. A malicious attack takes 315 days. This means your client is not going to have an immediate notification. Make sure they understand that!

It's also good to understand that 61% of the data breach costs are incurred in the first year of the loss, so continuing coverage is going to be highly important. You should help your client understand and evaluate the coverage provided. Do they understand what third-party liability is? What remediation is? Are they aware of regulatory exposures and payment card industry exposures? Is all their data covered? Make sure that you explain remediation services and how data restoration services will work.

Most importantly, agents should know what the various coverage triggers for ransomware will vary since there is no universal language for them.

MANAGING CYBER EXPOSURES

Risk Management

Due to increased regulatory pressure, unique security breaches, and significant challenges in managing business in the cyber world, we are learning that we must understand a highly technical and rapidly changing cyber threat landscape. In response, agents should consider implementing the risk management process:

- Analysis of Risk
- Control of Risk
- Financing of Risk
- Practice of Risk Management
- Principles of Risk Management

Those of us who have the CRM designation understand the process of risk management and that the first step is to identify the problem.

Is avoidance still the best technique?

Avoidance is not an option anymore, since having assets means there are also vulnerabilities to keep in mind. Where there is value, there are thieves, and cyber-criminals know the value of your information. Today, risk professionals can no longer afford to underestimate the value of information or ignore cyber risks as major threats to an organization. Instead, they should implement a thorough and robust risk management program.

What should agents consider during the process of risk analysis?

1. Identity theft is the largest and fastest-growing crime in the world.
2. Data is difficult to protect and even more difficult to replace.

Data is an important competitive advantage for every enterprise. Knowing what customers want, what they like, and what market interests they have gets enterprises ahead of the curve and attracts dollars.

The appeal of mining data forces us to find solutions to replace it once an enterprise is compromised. But how do you replace the irreplaceable?

3. Cyber Warfare

We are now seeing cyber warfare over the rights of information. There is a reason cybercriminals want to expend resources, including artificial intelligence, to steal information: it has value, and they want that value. We must know that in order to start understanding the severity of this problem.

4. Is your information secure? Remember: **C.I.A.**

The three critical qualities of information security include the confidentiality of the information, maintaining the integrity of the information, and making sure the information is available at a certain time.

Confidentiality: What information needs to be kept confidential and protected?
Integrity: Make sure that information can't be changed.
Availability: Is the information available to the proper people at the proper time?

If you're an agent conducting an analysis of exposure, here's what you should look for:

- Remember: C.I.A.
- Protect the three principal categories of information: public, confidential, and "internal use only"
- Think like a cybercriminal

Cybercriminals today need only to steal a password or a credential to sabotage a business. The risk of these criminals getting caught is very low, and the rewards are high.

They want to acquire financial records, wire transfer records, credit card information, health records, and medical history. They will then use that information for identity theft and to obtain intellectual property as well as copyrights, patents, trademarks, trade dress, and trade secrets.

Before you begin to control risk, understand what's floating below the iceberg.
There are many hidden costs that risk managers need to consider as they bring a program together:

- Credit monitoring
- Breach notification
- Identity restoration

- Forensic analysis
- Data restoration costs
- Business interruption
- Brand and reputation protection
- Hiring an outside public relations firm

Risk Control & Prevention Considerations

The assault is from all angles on the inside.

Good risk control and risk prevention locates, classifies, and protects critical information assets and either encrypts them or protects them with firewalls or limited access. However, securing the perimeter of the business enterprise is not enough. How do we get intruders out of the network? How do we quarantine a breach? How do we figure out the extent of the damage?

Consider BYOD: the Bring-Your-Own-Device movement.

We're now allowing smartphones and other devices to access private servers, which creates portals and potential entrances into a database. Risk managers should manage, control, and back up valuable assets while also enforcing proper recognition of who can and can't get in.

Don't rely solely on vendors or your IT department.

Everybody must be involved in, aware, and understanding of risk management. People should be hired and properly trained to understand security protocols.
The biggest asset is your employees.

Train them to know what a phishing attack is and what malicious attacks look like.

There are challenges to properly training employees. COVID-19 and the rapid transition of people working from home have created many challenges for risk managers. Management has become lax and must strengthen the way they manage exposures successfully when people work from home. We must have a consistent control program. Ask yourself: Is it adequate? Is it satisfactory? Is it upgraded yearly? Do employees adhere to it? Is it effective?

Consider these solutions:

- Care about cybersecurity
- Conduct a vulnerability assessment
- Test vulnerabilities regularly
- Make sure that security is everybody's business
- Make sure everybody is trained in cybersecurity awareness
- Understand what's open, how to allow the door to be open, and what the key to open the door is
- Security controls are the saws and hammers that get the job done

How can insurance help?

There are three basic elements included in most complex cyber insurance programs:

- Legal liability: protects against lawsuits as a result of a data breach
- Business interruption: replaces lost revenue as a result of downtime
- Breach notification costs: includes credit monitoring, notification costs, elements related to brand reputation, and forensic costs

CONTRACT DYNAMICS AND TRANSFERS

Picture this: An online retailer has a contract with a technology company that's going to design the retailer's website. The company is responsible for securing the retailer's website, processing orders, and storing customer data in a cloud-type environment. What are the potential opportunities for negligence in this scenario?

In this situation, the e-commerce transaction provider has an opportunity to create potential negligence-loss scenarios that are going to impact the retailer. A good solution to this would be to enforce a risk transfer through a contract to limit loss scenarios as much as possible. What else should insurance agents be aware of?

Content Liability

Content liability is a negligent situation that can create problems for the retailer. Including areas that are going to create exposures in contracts to the service provider builds content liability in the risk management and risk identification process. This includes assets at risk of potential trademark and copyright infringement, such as logos, design elements, and intellectual property.

Agents should also be aware of any data breaches that could cause privacy claims. Proper security measures should be put in place to protect clients, credit card transactions, private information, and any other key identifiers that are non-public and must be protected.

Other exposures to watch for:

- First-party exposures: notification costs, forensics, fines and penalties, regulatory

- Business interruption loss: viruses, ransomware, denied access, downtime, data restoration, and rectification work

As a purchaser of these technology products, the retailer would try to require that the assumption of full liability for these losses be transferred to the technology company through a commerce transaction. The retailer would need to have adequate indemnification.

Can the other party pay for it?

The short answer is: it depends. Did the retailer mandate insurance coverage for the technology company? Did they require the technology company to have an emissions policy? Did they require them to have media or content liability coverage? Did they require third-party cyber coverage for the care, custody, or control of the data that they would be manipulating?

To obtain appropriate coverages, contractual transfer elements and insurance elements like the general indemnity clause (also known as hold harmless and indemnification clauses) must be included in the contract.

The technology vendor cannot limit its liability for Bodily Injury ("BI"), Property Damage ("PD"), privacy liability, or business interruption. Agents should demand that, tell the retailer that they will be fully indemnified, and assure them that all liabilities created by the negligence will be paid for. In this scenario, an intellectual property indemnity clause is needed to protect the website containing trademark, copyright infringement, exposures, and potential claims.

If the intellectual property indemnity clause is agreed to, how will the infringement on the intellectual property indemnity clause be paid for? It may not be covered under the Technology Errors and Omissions policy. Property defense coverage may need to be brought in as a separate item.

Clauses Clients Should Have

- Intellectual property indemnity clause
- Financial loss indemnity clause to pay for all losses, including my regulatory proceeding attorney's fees and other items
- Content liability coverage for financial loss, data breach, reconstitution of database, and business interruption created by negligence

What if vendors push back?

The retailer must ensure they have the financial capability to handle a breach of privacy indemnity. The vendor may push back and only want insurance recourse coverage. In other words, they are only going as far as the insurance they have.

A vendor may want loss limited to a specific time period where they will only be responsible for six months, which is in violation of the statute of repose for any completed operation exposure.

Agents should be wary of language that states they are not going to be liable for more than a million dollars, for example. There should not be any kind of monetary cap on that indemnification. Retailers should strongly oppose any kind of non-insurance transfer language.

What's the best thing to do?

Focus on making the retailer's cyber policy to be in excess of what the technology vendor is providing. Agents must monitor these kinds of contract issues and have those discussions with their clients.

Keep in mind that coding and programming errors aren't found immediately. It can take a business anywhere from 280 to 340 days to realize it's been hacked. Agents should consider time limits, timelines, and other items that ensure good financial security. You want to make sure that the retailer knows how to indemnify and how to negotiate through problems and examine all contracts to determine what liability is present.

What does an underwriter need when an agent is submitting business?

Underwriting is done when a fully completed application is submitted. The completed application must indicate the coverage elements the client wants.

What are some potential challenges the underwriter may encounter?

Underwriters will also need to know about historical elements. One of the things they look out for is claims-made contracts. We are now starting to get substantial historical loss data to help examine and actuarially affirm current pricing. What we know right now is that the pricing that underwriters are giving is subjective and highly dependent

upon their individual judgment. Good, experienced underwriters develop premiums for exposures based upon receipts.

We know that pricing premium and underwriting are done with insuring agreements. If the insurance application indicated the client wants network and information security liability for $5 billion, then they will rate what network information security liability would be. If you want a communications and media liability as an insuring agreement, then there'll be a premium charge and a limit established for the communications and media liability. If you want regulatory defense expense, there'll be a premium charge and a rate that will be applied to the limits that apply for the regulatory defense.

What about crisis management, breach remediation, data restoration expenses, etc.?

Each insuring agreement has a premium that is charged based upon gross receipts that establishes, within the limit selected, what will be charged for that item. There may be separate limits or aggregate limits depending on the rating methodology used by the underwriter, like hazard rates with differentials.

Underwriters will then try to arrive at a rate. The rating structure may have different rate classifications or hazard classifications based on the size of the enterprise or the number of employees. They will then add other significant elements from the initial application. It becomes very important that the client understands that this is a "warranty application" and they're required to disclose information in order to get appropriate coverage.

Things Underwriters Look for:

- Network security measures
- Support personnel policies, procedures, training programs
- Information security for website PDFs
- Password control
- Content information
- Contractual risk transfers
- Indemnification agreements
- Frequency of loss history

When It Comes to Coverage for Clients...

Understand that forms and policies like the commercial general liability, commercial property, EDP, and equipment breakdown won't protect your client when it comes to cyber insurance. It's very important to understand that standardized coverage forms are not going to be useful.

A proper cyber or privacy insurance type program must not include only mono-line type coverage. It should include robust, multi-level coverages for first- and third-party exposures.

REGULATORY ACTIONS AND POLICY LANGUAGE

Agents will need to understand how to get defense for regulatory actions and how to pay the fines and penalties. Insurance will provide coverage by endorsement, or as an insuring agreement that you have to trigger onto the deck page. Separate items may include language like "contributions by the insured to a consumer redress front for New York regulatory fines and claims expenses." Included definitions specific to the regulatory defense may define "wrongful act" and "privacy incident." Language like "state, federal, or country laws" may be included, which means there may be an element that would require worldwide coverage.

Specific language requires agents to look at limits differently if items like the wrongful act defense or regulatory defense are included. Another consideration to examine is the extent of fines and penalties to be paid. All this to say that agents must read each policy clearly, especially when language like "we'll pay on your behalf damages and claim expenses" is included.

What will the underwriter need to know?

The underwriter wants to know if you are complying with credit card stipulations. These questions are now included on PCI DSS applications, and agents must answer these questions succinctly.

- Have you installed and maintained a firewall to protect credit card data?
- Is there a way to protect the store data?
- Do you encrypt or transmit cardholder data? Is there a security system and application?
- Is a unique ID assigned to each party that gets computer access?
- Are physical assets to cardholder data restricted?
- Are security systems and processes checked regularly?
- Are policies maintained to address information security?

Why should agents care about this?

You become legally obligated to pay an excess of the apical retention. Generally, there's going to be an answer resulting from a PCI DSS assessment, which will include definitions, different coverages, and cost.

Any time there is a point-of-sale device there is also a PCI DSS exposure, which means some kind of fines and penalties coverage is needed. Fines and penalties are not always included in a PCI DSS. Agents need to evaluate and determine adequate coverage.

Risks Associated with Websites

Websites create very broad categories of potential liability, especially with content. Clients may need to have some of that coverage brought into their website media content.

Take personal injury coverage: agents must now coordinate coverage B with CGL and personal injury. But what if they are libel-slander-trade liable? Was emotional distress inflicted? What about in-patient or privacy and interference of the individual's right of publicity under personal injury coverage?

Remember that website coverage under coverage B is only for goods and services. Agents may encounter problems with coverage B and may need more personal injury coverage than is already available.

Precautions for Web-Based Activities

Electronic content, block sites, bulletin boards, and social media links are not covered by coverage B. Agents must consider what media content or website publishing liability they need to bring to the forefront. Some carriers will call it website media liability, content liability, or website publishing. Agents need to be aware of what that liability includes regarding emails, PDFs, photos, and other non-website media activities, such as broadcasts, videos, and public appearances. Only about half of all cyber privacy insurers provide any kind of website or content liability coverage or website professional liability.

Your client may need broader coverage, which means they'll have to pay additional premiums to address this professional liability exposure. Some coverage forms include internet media liability, meaning it's only the electronic format and will require agents to look at electronic publishing wrongful act definitions. What's interesting is that many will not pick up canned spam and telemarketing actions, so agents may need to bring in that coverage if clients have an e-commerce platform or catalogs.

Cyber-Related BI and PD

Cyber coverage-related BI and PD are necessary because cyber and privacy insurance policies virtually always exclude coverage for direct BI and PD. For example, when a client's hospital's computer system was hit with a denial-of-service attack, it caused it to shut down for eight hours. During this time, the hospital was unable to remotely monitor the patients in its cardiac unit. During the downtime, three patients suffered fatal injuries because changes in their conditions could not be ascertained via electronic monitoring, and thus they were not given immediate necessary treatments. Lawsuits against the hospital alleged that the hospital's negligence and failure to prevent the intrusion of the computer system caused the patients' deaths.

In this case, contingent BI and PD were based upon an attack on the system and unauthorized access. Broader, more robust cyber forms will have this cyber-related BI and PD liability. Agents must think about how it coordinates with commercial general liability and how it applies to the medical malpractice coverage for the BI and PD.

Are there exclusions on the CGL that may have an impact? Consider the CG 2106, which allows some bodily injury, or the CG 2107 which has no bodily injury. Agents need to be aware of the limitations of the CGL. Keep in mind that not all coverage forms have

cyber-related BI and PD coverage. Be sure to look into this issue as you start to relate to the robustness of the coverage and the identified exposures for clients.

What solutions are available for agents with clients who conduct e-commerce and have significant exposures from business income loss?

Cyber and privacy insurance policies have two types of time element coverages: business interruption and extra expense. These coverages are different from the property form. Remember: the perils that are necessary to know on the property form are not the same perils under cyber. The perils that are under the property form triggering business income with extra expense using the ISO form are not the same as those we have here.

Cyber has different triggers, including violations of firewalls on authorized access, that force agents to think differently for cyber business income and extra expense. They must recognize that not every carrier will provide business income and extra expense coverage, so there's a debate regarding what they want to do and what they want to provide.

Some carriers provide business income and extra expense through an endorsement, not built-in as an insuring agreement. If so, agents need to find out how each carrier works through that issue. The insurer shall pay the company any business, income loss, dependent business, interruption, loss, or extra expense sustained during the period of restoration. Some of these first parties are bringing in dependent property. Why is that so important? Consider the following:

Key Components in First-Party Time Element: Questions for Agents

- Is a website a dependent property or location?
- Is cloud storage a dependent property location?
- Can that create a business interruption or extra expense?
- What is the definition of business?
- Does business income include tax, normal operating expenses, payroll?

Exclusion to First Party Time Element

What's not included in First Party Time Element are items such as the updating, restorations, or replacement of any digital assets. That means there's no rectification cost for the extra expense. Clients may not have coverage for trade secrets or a value of

digital assets or proprietary items that have been compromised. Contractual penalties may be an excluded item underneath this as well. Agents need to decide what they're getting in business interruption. If it's a multi-insuring agreement-type coverage form, the other insuring agreements are probably going to be excluded within the time element.

There is a lot of dependent business interruption. Where is the data service? Where is data currently being stored? Is it on your client's server or is it on somebody else's server that counts as dependent property? How many of your clients have that dependent property?

More on Extra Expenses

When agents see language like "any costs or expenses to correct any deficiencies, identify or remediate software errors or vulnerabilities or costs to update, replace, modify, upgrade, restore, maintain, or improve any security system or computer system," they know rectification costs are not included. If rectification costs are needed, a separate limit to include is data restoration.

How much is it going to cost to restore data?

Let's say a client is hit with ransomware, paid the ransom, but still can't access their data. In this case, the data needs to be restored. How long does that take? What does that cost include? Don't forget that it's not going to be covered under the extra expense.

There are other exposures agents need to think about as well, including the first party theft of property coverage element. Other elements include data, asset coverage, cyber extortion, computer fraud, funds transfer, and social engineering. Agents may need to ask if there are endorsements or coverages included for those too. For example, with data asset coverage, agents will need to know if it includes the recapture or restoration of that lost data. Does it have its own limit, and how does it handle? Is it a reimbursement? If so, the client will incur costs.

More on Ransomware and Computer Fraud

How can agents handle cyber extortion coverage, ransomware, and ransomware monies? Cyber extortion is becoming much more sophisticated. Extortionists use artificial intelligence to increase this exposure, and the encryption being used is quite

complex. Coverage restrictions for computer fraud exclude employee acts. This leads to many questions:

- What does that mean under the crime form?
- Does the client have fidelity coverage?
- Will that be covered under the crime form, or does the agent need to modify the computer fraud coverage also?
- What do you get in computer fraud versus fund transfer fraud?

Hot Topic: Social Engineering or Fraudulent Instruction Coverage

Some of the crime forms will provide social engineering or fraudulent instruction coverage. The problem is the crime forms usually can't get the limits that clients may need. So when agents examine social engineering coverage under a cyber-crime form, they need to know where to best to ask for premium dollars to give clients better coverage.

What other coverage provisions should agents be aware of?

Is it per insuring agreement? Is there an aggregate? Are there sub-limits? There may be deductibles that apply for each different insuring agreement. There may be an aggregate deductible because multiple insuring agreements were triggered. Knowing what the limits are, how they apply, and how the deductibles work are all important parts in terms of the comparison.

What current or past entities are brought in? Is additional insured coverage automatically brought in or added by endorsement? What about first party coverage and loss payee situations? Is there language about expense damage, expense, or defense? What's not covered? Don't just glance over the settlement provision or the consent to settle clause.

Cyber insurance and its coverages are very broad and don't cover everything. What common exclusions should agents be looking for?

Watch for exclusions about fraud and criminal and dishonest acts and understand how they work. Know what's excluded in terms of employment, retirement income security, war, invasion, or insurrection. There are also the bothersome professional services exclusions which will not cover anything unless it's specifically listed.

What are some of the markets that are available out there?

More than 60 insurance companies offer some type of cyber insurance, including by endorsement. Some primary players dominating the market right now are AIJ Aliante, Allied World Ascent, Aksia XL Berkeley Cyber Risk, Berkshire Hathaway, CFC, Chubb, Cincinnati, CNA, Crow, E Franchisor, Sweet Hanover, the Hartford, Hiscox, Liberty, Markel Specialty, One Beacon, Philadelphia, TDC, Specialty Tokio, Marine, HCC, Travelers, Zurich, and other syndicates in London that are also providing coverage.

Conclusion

Cyber privacy insurance continues to evolve, creating a high level of claims and an increasing level of threats. Litigation over coverage interpretation is increasing and COVID-19 has added demand for potential new items concerning working from home. Insurers with lots of cyber experience are refining their underwriting tools and making increasingly valuable risk services available. In turn, they're asking for more information and they're trying to help agents understand the coverages out there.

The market is starting to mature with insurers more often insisting that clients have higher participation. In other words, higher retention limits and deductibles, especially in retail and healthcare segments. Coverages that were easier to find are now changing. PCI DSS is a good example: they're demanding that stronger security standards match up to the payment card industry and the data security standard. Also, ransomware is going to stick around and that will create new dynamics in the future.

AGENT E&O EXPOSURES AND RISK MANAGEMENT

Insurance Exposures & Agent Impact

Exposures are linked to what's happening in the marketplace at any given moment. Ransomware is still an issue: it's driving numerous loss ratios for 2020 and it's causing cyber insurance prices to go up. Analysts and brokers agree, including Moody's Analytics, which said that the insurance industry loss ratio this year for 2020 will be an excess of 50% or higher. That's a significant shift for all of us in terms of the marketplace because we were seeing pricing between 2015 and 2018 going down, even though loss ratios were beginning to increase. They were not significant as they have been in 2020. We know that the direct premiums written for the cyber line have increased since 2015 and have become must-haves for most organizations.

The premium volume is up from 488 million to over 1.3 billion in 2019. Estimates show 2020 closed out about $1.6 billion worth of premium volume: that's quite significant. When you look at a marketplace that's growing in that area, we know that the demand for cyber coverage continues to increase given the changing nature of the risk and the persuasiveness of the technology. We see more and more new technology coming in and a significant impact on the supply chain risk.

More and more carriers are starting to scrutinize the relationships they have with their insureds. They're asking questions such as:

- Do I also have their upstream partner as well?
- Do I have one of their co-partners or entities?
- Could one event bring in multiple companies and impact us?

In other words, carriers are starting to look at the aggregation of risk, which is going to have some impact on pricing as well.

Coverage and price decisions are becoming bigger and bigger challenges. Therefore, it's critical to understand the problems, the risk management issues, and the coverages required. Then, understanding how to avoid getting into a broker E&O exposure comes into play. We're seeing more and more that buyers without robust insurance continue to lack the coverage they anticipated. Buyers find themselves in situations where the representations about the systems they had in place turn out to be misrepresentations.

Critical Data

In fact, the insurance companies are avoiding coverage and not paying coverage. We know that 51% of consulting and legal services are paid by cyber insurance carriers for data breach claims. We also know that 36% of victim restitution claims are being paid by cyber insurance carriers in data breach claims: that's a little low, but it tells us that we may not have as many identity theft elements as we expected to have when we started pricing this product.

> ➔ **51% of consulting and legal services are paid by cyber insurance carriers for data breach claims**

We know that 30% of the regulatory fines have been paid by cyber insurance. One might hear that figure and assume that everybody's buying it, but not everybody is buying regulatory fines and penalty coverage, or the PCI DSS coverage necessary for compliance. This is a sleeper that's may cause some problems.

What's more, we know that 29% of recovery technology costs are being paid by cyber. One problematic issue is that forensics often finds a problem but doesn't fix it. We're not seeing the rectification costs, so that should be a higher number when we start adding in the cost of finding and fixing the problem.

The Big Unknown

The biggest unknown item is the element of ransomware and extortion costs, only 10% of which have been paid by the insurance carriers. There are some specific rules about ransomware and the insurance company's involvement; recently, we've seen evidence

that those paying ransoms may find themselves subject to problems with the treasury department as well, which makes for a complicated situation.

This highlights areas where problems may arise from an errors and omission standpoint. As we put together the coverage, we know that typical data breach claims are not covered 100% as such. There are going to be gaps in insurance. That means we don't have the proper endorsement or we need to add an endorsement. For example, filing to initiate the proper trigger on the insuring agreement or the deck page could cause issues. On top of that, a lot of the coverage forms have sub-limits, which are inadequate to cover the loss exposures. And if they're inadequate to do that, clients may ask why you didn't recommend higher limits as an E&O claim.

We also know that many people are starting to ask about their limits (e.g., *Why didn't you tell me to go to 3 million or 5 million in limits? Why did you sell me a 500,000 or a million-dollar coverage?)* Inadequate limits are starting to raise their ugly heads. Of course, the key element when understanding this product being claims made is defense inside the limits, which has a significant impact on the overall coverages that we have. We must be aware of these gaps.

Coverage Pitfalls for Agents and Brokers

Some coverage pitfalls are obvious. We've all been trained on claims made. We understand retrospective dates and we know extended reporting periods, but tied to that are the prior and pending litigation exclusions and other items that are causative events. We know we have up to 280 days to discover an actual intrusion. But what does that do to the retrospective date? What does it do to the prior and pending, especially when you're coming up with a renewal or changing carriers?

- We have some new pitfalls and challenges:
- What is an occurrence?
- What is the trigger for that occurrence?
- What coverage form is needed?

For example, consider the scenario in which an employee provides access to their password or is tricked into providing access to their password: is that covered? The devil in the details. Are we taking the time to understand the key triggers and all of the insuring agreements we're looking at? And do we understand how pervasive or how limiting that wrongful act definition is?

Minimum Required Security

A commonality of wrongful acts shows up in most cyber policies now, and we have to understand if we need clarifying endorsements. The biggest one that has made itself known in the last 18 months is the minimum required security practices exclusion. When you make a representation on the application that you're undertaking minimum required security practices, that's a warranty that can be a way to rescind or avoid coverage.

The best security practice is to make sure you meet that minimum security. And the key for us is to try to get rid of that kind of exclusion. Then there is the element of what acts foreign countries are undertaking by way of attack.

New Definitions

The cyber terrorism issue has been expanding. New definitions are coming out that create new challenges, including the question of selling cybercrime coverage. For example, if we're not selling cybercrime and are relying on the crime form, you don't have cyber terrorism coverage. This is another pitfall to consider.

Consider one recent event regarding Access Capital Holdings:

ACH was not required to reimburse a silicone manufacturer for the wire transfer theft of more than $1 million under its computer transfer fraud provision because company officials had approved the transfer.

In October 2017, the chief financial officer of Burnside, Mississippi-based Mississippi Silicon Holdings, LLC received an email from a regular vendor advising that future payments should be routed to a new bank account. This is social engineering and cybercrime; social engineering and cybercrime are going to become significant elements in the future right along with ransomware.

Let's look even deeper into this ACH scenario: There was a letter relaying the same instructions written on the vendor's letterhead and signed by the vendor executive, which was attached to the email. The email's body also contained the previous emails between the Chief Financial Officer and the vendor's personnel concerning invoices and shipping details.

The MSH official then authorized wire transfers to the vendor's new bank account totaling $1.025 million. The court ruling said the payments were made in accordance with the company's three-step verification process for large transfers. The CFO initiated the transfer. Another company employee confirmed it on the bank's website and the company's COO orally authorized the transfer on a phone call with a bank representative. Two months later when the vendor called to discuss outstanding payments the company thought they'd already made, they filed a claim for $1,025,831 under the provisions of the commercial crime policy. ACH sent their client a check for $100,000: that was the limit for its social engineering fraud provision. They refused to pay for the claim under its computer transfer fraud provision, which had a million-dollar limit. MSH sued ACH, and a U.S. district court in Amery, Mississippi ruled in the insurer's favor.

Questions to Consider

The dispute in this previous example boils down to a disagreement over the interpretation of the policy's computer transfer fraud provision. The policy means what it says: coverage under the computer transfer fraud provision is available only when a computer-based fraud scheme causes a transfer of funds without a company's knowledge or consent. The case highlights that a potential E&O claim could be filed against the agent for failure to procure adequate coverage.

Ask yourself these questions:

- ➔ Do you, as an agent or broker, understand the coverage you're selling?
- ➔ Do you thoroughly understand social engineering, cybercrime, the crime form, and impersonator coverage?
- ➔ Do you understand the impact of sub-limits that comes out of this case?
- ➔ How would presenting the coverage and disclose the impact or requirements for validation in a social engineering claim scenario like this?

Standard of Care

Standard of care is a simple behavioral concept. What is the generally accepted behavior of an insurance agent or broker?

Are you a licensed insurance agent or broker? If so, you're now in the business of soliciting, procuring, and placing insurance, which means you have to follow a standard of providing reasonable care, diligence, and judgment in ordering and procuring requests for coverage from clients.

This applies to cyber insurance as well. You must understand the client's requests and what they're really asking for. Are they asking for social engineering? Are they asking for unauthorized act coverage? Privacy invasion coverage? Business income? PCI compliance coverage? If you're unable to provide that coverage or procure that coverage, you got to give them prompt notice that you're unable to so that appropriate measures can be taken to protect the client, such as going to another broker, company, or agent to procure the coverage.

That's the general rule. We can solicit it, we can do it, but we have to do what we agree to do. This reaches into other areas of our performance or our behavior. We can get sued for failure to obtain coverage, commonly referred to as faulty coverage. We can get sued for failure to place coverage after agreeing to procure (e.g., you got a quotation and you didn't get the coverages that everybody had quoted on it). A failure to provide proper advice can be prevented by a heightened standard of care.

Failures of the Standard of Care

Violations of the standard of care can present as specific failures. Failure to advise the insured promptly of rejection of coverage or inability to place coverage is a sign of an inadequate standard of care. This includes the cancellation or non-renewal of coverage. Failure to renew coverage as requested by the client and provide the updated information or supplemental applications that are required by the insurance carrier is a failure to service the policy. The failure to place on best terms and conditions available is sort of a gray area, but it's an item that's asserted against us. Misrepresentation and placing with an insolvent carrier always creates additional items for us in terms of the cyber claims that we can deal with if litigation is filed against an agent or broker in procuring cyber professional liability or E&O coverage.

In other words, make sure you get the proper endorsements, make sure the proper premium payments are taking place, and make sure the proper payment plans and any premium financing is done.

Coverage Issues vs. Procedural Issues

It used to be the rule of thumb that 50% of claims were procedural and 50% were knowledge-based. we're now seeing claims becoming more and more knowledge-based. Consider this fact: 66% of all claims are coming from improper coverage, which means there's a knowledge issue in play. Within faulty coverage or improper coverage, there are three major sub-problems: failure to obtain the proper coverage, failure to obtain coverage, and failure to renew coverage. And all three of those have an impact on us on faulty coverage. The risk is in the beginning, the middle, and at the end. So the key elements for us have to do with our ability to analyze the risk properly and offer proper cyber coverage.

Today, all proposals should recommend that insureds buy cyber insurance, It's no longer a "nice-to-have" item. It should be there all the time because it's a necessity. The process of not physically requesting the proper coverage just because you get an

indication from a carrier is not getting proper coverage. You have to fill out an application, get hard numbers, get hard limits, and let the client understand what's taking place. Failing to understand the trigger of a wrongful act, not understanding which insuring agreements are applying, and/or not understanding the sub- limits can be critical problems.

➔ **66% of all claims are coming from improper coverage, which means there's a knowledge issue in play**

Generally, there must be a finding of express or implied contract to advise creating a special relationship. We're finding that in most of the cyber liability claims against agents and brokers, they have gotten into a heightened standard of care. They are into the affirmative obligation to provide because a client doesn't understand it. Remember that you must understand the need and sell the need to the client. They have to understand the exposure that puts us into that heightened standard, into that special relationship and professional standard of care. In the area of cyber and technology E&O items, we have become more like risk advisors in that procurement.

New Roles for Brokers & Agents

This means we have clients who are substantially relying upon us. We have to understand the gravity of that duty. We, as brokers and agents, have to look at our agents, our omissions limits, our coverages, and limitations that are going to be applied because faulty coverage is going to be a substantial reliance issue. We know that we have a certain skill, a certain knowledge level, and we're constantly training. We're required to update ourselves, to maintain our licenses. And as such, part of the educational process today, and going forward is updating our cyber and technology skillsets. We know that we have a duty to know the types of coverages available and know the types of carriers that are involved. In other words, we must be able to canvas the marketplace and understand what over 65 active insurance companies are providing. Consider these questions:

- Are they providing standalone products?
- Are they endorsements onto coverage forms?
- What are the limitations? What are the sub-limits?

These are all important elements we have to bring into this coverage. We may recommend coverages and limits to our client, whether expressly because of a

consulting contract or because we implicitly agree to. This places us on a slippery slope of enacting a higher standard of care and professionalism and raises questions about how to avoid that precarity.

Options, Options, Options

One way to protect everyone involved is to always provide options: provide the options, and let the client choose. We know the potential of any claim under cyber liability. We know how long it takes. We know what the average cost per claim has been. We've given clients that information. We know we need to continuously work on that as we go forward today, we know a mega breach of data of over 50 million records can reach a price tag of up to $400 million.

In fact, a recent decision made in St. Paul, Minnesota determined that a claimant would only get an insurance payout of $90 million. The rest of it would have to be paid out of their pocket target. And this mega breach was close to 110 million records: a breach of 1 million to 10 million records costs an average of $50 million. *How much is enough?* is a decision for the insured, the client, and the agent broker to work out. This is why options become such significant elements as we try to build a program for our clients. Impact to limits, the definition of occurrence, continuing exposure to a similar condition, and the aggregation of all these elements together becomes a significant factor.

Questions to consider:

- How does the sub-limit impact the coverage?
- What are the adequate limits?
- What are you buying for yourself in terms of adequate limits?

We know that the cost of a data breach could continue for years following the event. We know that 61% of the average data breach cost occurred in the first year and 92% in the first two years. We know we have 280 days to discover the data breach. If that's the case, we need to manage renewals, understand the concurrency of coverage from year one to year two, understand our retro dates, understand the triggers in the policy, and understand the need for extended reporting. All these elements become significant in dealing with the concept of faulty coverage.

Risk Management: E&O Exposure & Expertise

The impact of cyber risk has huge impacts not only on yourself as an insurer or broker, but also on the advice that you give insureds.

The licensed insurance agent or broker needs to have knowledge. With that knowledge, you must be careful in how you provide risk control advice and make sure you understand what you're suggesting. Don't list something off or send it out in an email without understanding what you're saying. We should remain generic in our discussions and let professionals provide the advice specifically: Bring in the forensic expert. Bring in the auditor. We are risk advisors with a heightened professional standard of care. Therefore, we must maintain our credibility by staying current in education, updating ourselves, taking cyber courses related to the insurance company providing it, or through The National Alliance.

Remember that generic advice and risk management are important. Items that are generic include investing in a security orchestration automation response, commonly referred to as a SOAR program to prove detection or response. But the SOAR program details depend on the vendor or tech person who will be coming in and doing the analysis. Today, we're at a zero-trust security model to help prevent unauthorized access. Determining what that process is becomes part of the application.

Do you understand what a zero-trust security model should be?

If you see these terms or hear these terms and they don't make sense to you, educate yourself about them further.

Clients should have a stress test done on their system by an outside vendor to determine how their incident response plan will roll out. Many clients aren't doing stress tests, but other elements that we could recommend to them include asking their vendors to help determine their endpoints and remote employee access. Always tell your client to invest in governance, risk management, and compliance programs. They're going to make them better. Remember, we have 50 States that have their own statutes about privacy. For example, privacy rules in California have become quite complex. Try to use managed security, to help find the gaps in the organization and the training.

These days, we're seeing contracts between business enterprises and upstream clients that will not allow you to work with them unless you have cyber insurance and/or securities programs in place. We need to remember that the CGL and commercial

property policies do not respond and provide adequate coverage, and we have to be able to make that clear to the client. And that's why we have to talk standalone coverages. Remember that privacy forms have some common terms, but all of them have different features. And you're going to have to spend time reading it to understand those differences and educate yourself using outside resources like the Betterley Report.

Educating Yourself

It's critical to understand these elements:

- first-party post-breach response expenses and coverages
- third-party liability coverages for information security
- privacy
- regulatory issues
- defense penalties
- payment cards
- industry fines and assessments
- website media
- other types of communications, social media, PDFs, and emails

Are you getting that coverage? And then of course we have to consider the contingent bodily injury and property damage liability, exposures, time element coverages, business interruption, and extra expenses. Theft of property coverages have to be brought in as well. As we think through this, how do we restore each of these items? The cyber extortion, the computer fraud, the funds transfer fraud... Think, too, of the social engineering and fraudulent instruction coverage we discussed above. These all become important elements. As you start to understand your knowledge base, recall that you have to know your marketplace.

What coverages are there? Do you understand the difference between an AIG policy and a Beasley policy? Do you know what's different in a Chubb contract versus a Cincinnati contract? Do you know what Hartford's willing to take or Hiscox is willing to take? Know your markets, know what's out there, and understand that there are over 65 active insurance markets out there writing some form of cyber insurance.

Trends in E&O Ethics

For ethical agents and brokers who are doing their jobs, there's a direct correlation to the impact on E&O limits. The more you move towards the role of a risk advisor, risk management consultant, or fee-type service broker, the higher standard of care will mean you must have higher limits. Many insurance brokers and small- to medium-size firms are significantly increasing their E&O limits. The large brokers have their own kind of programs, but the small- and medium-sized firms are increasingly playing in the $4 million to $5 million range on their E&O limits. Some are even buying an excess of that and going to the $10 million to $25 million range because of their exposure and because they are functioning more and more as professionals and advisors than mere order takers.

We've seen that the type of business you're soliciting establishes some of that decision basis. Commodity-driven products that are out there, such as personal auto, come into play as well. Homeowner's has almost become commodity-driven except for the high wealth. So the type of insurance is establishing some of that standard.

→ **Many insurance brokers and small- to medium-size firms are significantly increasing their E&O limits.**

What type of marketing system are you? Are you a captive agency system and independent agency system? Are you providing risk management value? Added services change that element. We know that membership in a trade association and following an enforceable code of ethics can create a higher amount of liability for you. Many readers are CICs and already have professional designations, and that responsibility increases your level of ethical performance and also your legal standards.

Parting Thoughts

Use the skills that you've developed as a reasonably competent producer agent or broker in a similar situation.

Generally, liability is created by the failure to procure the requested insurance or procuring insurance that was materially deficient in some way. And that's that faulty coverage that was discussed. This is our ethical, basic duty to our clients when we're working with them in the cyber insurance and technology E&O insurance areas.

If the producer agrees to advise, give the buy, give the advice, but do it with the caveat of understanding in some jurisdictions.

The duty to advise may arise when their producer has a continuing relationship; be aware of your relationships in the advice you give to the client liability to third parties, which are also starting to come into our realm. Be aware of certificate holders, lessors lessees, additional insured loss payees, vendor contractors that are allowed for coverage. Don't forget our spouses, dependents, and domestic partners either.

Remember that the primary intent of state insurance laws is that our insurance agents are prohibited from creating unfair or deceptive practices in soliciting selling or servicing insurance.

Honest, full disclosure and integrity are vital for establishing trust and success in procuring cyber and technology insurance relationships.