Bloomberg Law®

Bloomberg Law Practice Suite – Cyber Insurance

Cyber Insurance

Authors:

Walter J. Andrews
Sergio F. Oehninger
Patrick M. McDermott
Hunton & Williams LLP

About the Publication:

This practice guide, *Cyber Insurance*, authored by Hunton & Williams LLP, and published by and available on *Bloomberg Law*®, provides guidance on the distinct considerations involved in negotiating and obtaining cyber insurance coverage, identifying and quantifying risk, best practices for preventative cyber security measures and business continuity plans, and coordinating and communicating with the insurer as part of incident response.

About Hunton & Williams and the Firm's Insurance Coverage Practice:

For decades, the insurance coverage lawyers at Hunton & Williams LLP have helped our clients maximize insurance recoveries through insurance program reviews, claims presentation and negotiation, litigation, alternate dispute resolution, trials and appeals.

Our policyholder-focused practice helps clients take full advantage of their available insurance coverage to help pay their legal bills and ultimate liabilities. From our major offices in Washington, DC; New York; Miami; Los Angeles; Dallas; Atlanta; London; and other key commercial centers, we advise policyholders about traditional and emerging insurance products in virtually every sector of the economy, including financial services, utilities, energy, natural resources, health care, chemicals, pharmaceuticals, consumer products, retail, manufacturing, telecommunications, technology, and more.

Our lawyers counsel clients on a full range of insurance products and coverages, including:

- Cyber and Data Breach Coverage
- General Liability Insurance for Bodily Injury, Personal Injury and Property Damage
- Product Liability, Environmental Liabilities and Mass Torts
- First-Party Property Coverage
- Business Interruption and Extra Expense Coverage
- Directors and Officers Liability Coverage
- Professional Liability, Errors and Omissions Liability, Bankers Professional Liability and Technology E&O Liability
- Credit Risk and Financial Guaranty Insurance
- Fidelity Bonds and other Crime Coverage
- Employment Practices Liability Insurance
- Trademarks, Copyrights and Other Forms of Intellectual Property

We keep pace with insurance products and regulations as they expand and adapt to fast-developing technologies and rising concerns related to cybersecurity, privacy, intellectual property theft, corporate social responsibility, sophisticated financial products and credit risks and terrorism, among others, while still addressing traditional areas such as property and casualty, product liability, environmental issues and business torts.

Ask us how we might help you or your clients maximize available insurance recovery.

CONTACTS

Walter J. Andrews
Partner
Miami
(202) 955-1802
wandrews@hunton.com

Sergio F. Oehninger
Counsel
Washington, DC
(202) 955-1854
soehninger@hunton.com

Patrick M. McDermott
Associate
Washington, DC
(202) 955-1858
pmcdermott@hunton.com

About Walter J. Andrews:

Walter's practice focuses on complex insurance litigation, counseling and reinsurance arbitrations and expert witness testimony.

As the head of the firm's insurance coverage practice, Walter offers clients more than 25 years of experience managing insurance-related issues, including program audits, policy manuscripting, counseling, litigation and arbitration. He works with companies in a diverse range of industries, including financial services, consumer products, food and beverages, chemicals, real estate and municipalities.

Walter is admitted to practice before courts and arbitral bodies across the United States and abroad, including the United States Supreme Court; US Courts of Appeal for the Second, Third, Fourth, Sixth, Seventh, Eighth and Eleventh Circuits; and US District Courts for the Eastern and Western Districts of Virginia, Eastern District of Washington, Western District of Washington, District of North Dakota, Southern and Middle Districts of Florida, Southern District of New York, and Eastern District of North Carolina. He litigates insurance coverage and bad faith disputes around the nation, involving business interruption, product liability, construction defect, reinsurance matters, cyber insurance and e-commerce issues, and other emerging claims. These matters involve a variety of insurance contracts, including professional liability, first party property, general liability insurance policies, cyber insurance, and various reinsurance agreements.

About Sergio F. Oehninger:

Sergio represents companies in complex insurance coverage disputes nationally and internationally. Sergio counsels multinational corporations on insurance coverage and risk management issues arising in various industries – including financial services, retail, manufacturing, energy, technology and real estate.

His insurance coverage advice focuses on risks such as: cyber and data breach; commercial general liability; directors and officers; professional liability/errors and omissions; employment practices;

property and casualty; business interruption; excess, umbrella and integrated risks; and other insured and reinsured risks under occurrence-based or claims-made policies. As part of his Latin America practice, Sergio frequently advises Spanish-speaking corporate clients on cross-border exposures in connection with transactions, projects, operations, products and services.

Sergio's experience includes matters cumulatively exceeding one billion dollars in losses or exposures before federal and state courts throughout the United States and ADR tribunals. He is admitted to practice before the Supreme Court of the United States, the US Court of Appeals for the Fifth Circuit, and US District Courts in Virginia, Colorado and Washington, DC.

Sergio frequently makes presentations and writes alerts, articles and contributions to the Hunton & Williams Insurance Recovery Blog.

A strong advocate of public service, Sergio has served on the boards of several non-profit organizations and his pro bono work includes advice to a 501(c)(3) charity dedicated to combating gang violence and raising funds benefiting children living in poverty.

About Patrick M. McDermott:

Patrick's practice focuses on complex civil litigation matters, with an emphasis on insurance and reinsurance coverage disputes.

During law school, Patrick served as a judicial intern in 2008 for the Honorable Michael F. Urbanski of the U.S. District Court for the Western District of Virginia and in 2010 for the Honorable Ricardo M. Urbina of the U.S. District Court for the District of Columbia.

About Bloomberg Law:

Bloomberg Law helps legal professionals provide world-class counsel with access to actionable legal intelligence in a business context. *Bloomberg Law* delivers a unique combination of practical guidance, comprehensive primary and secondary source material, trusted content from Bloomberg BNA, news, timesaving practice tools, market data, and business intelligence. For more information, visit **www.bna.com/bloomberglaw.**

Bloomberg Law: Privacy & Data Security brings you streamlined access to the expertise of Bloomberg BNA's privacy and data security editorial team, contributing practitioners, and in-country experts together with unmatched practice tools to help you quickly respond with confidence to client inquiries.

In Practice tools include exemplar policies and provisions, checklists, and forms to facilitate your drafting needs for privacy and data security tasks such as:

- New York Cybersecurity Regulation for Financial Institutions Managing a Data Breach
- Managing Privacy and Data Security Risk in Mergers
- Designing a Privacy Policy
- Cross-Border Data Transfer

Bloomberg Law Practice Suite – Cyber Insurance

Sergio F. Oehninger, Patrick M. McDermott and Walter J. Andrews

Walter J. Andrews is a Partner with Hunton & Williams LLP and Head of the Insurance Coverage Practice Group. Sergio F. Oehninger is Counsel in the firm's Insurance Coverage and Latin America Practice Groups. Patrick M. McDermott is an Associate in the firm's Insurance Coverage Practice Group.

Table of Contents

I. Description of Business and Technology Cyber Exposures to Be Covered

A. Introduction

Cyber risk is a growing concern for both local and global companies as mobile technologies, cloud software, big-data analytics, and the Internet of Things (IoT) become increasingly prevalent and interconnected. Due to an expanding global preference for internet-connected devices, which according to a 2016 report are forecasted to reach 28 billion connected devices by 2021, cyber-based business exposures are expected to skyrocket.

Given these emerging and increasing threats, cyber has been a front-and-center "boardroom issue" for some time now. In recent surveys, nearly 75 percent of corporate counsel name data breaches a top data-related legal risk, and nearly 70 percent assert that their legal department is more focused on cyber security than it was last year. Recent cyber events have shown that prevention is very difficult for most, if not all, companies. It is therefore about resilience and being able to recover quickly, efficiently, and cost-effectively so that your company can continue its operations.

This landscape has created a burgeoning field of insurance coverage options. But, in part due to the field's novelty and the difficulties of identifying and quantifying risk, cyber insurance policies have proven distinct from other insurance contracts, and therefore require careful consideration and should be implemented in conjunction with prophylactic cyber security measures, best information technology (IT) practices, and business continuity plans (BCP).

B. Cyber-Related Risks

When contemplating insurance coverage for cyber-related risks or losses or when reviewing existing insurance programs for adequacy of coverage or gaps, companies must first consider the specifics of their cyber-related liabilities and exposures. Companies may not be able to obtain insurance coverage for all potential liabilities and exposures. However, envisioning the possible or most likely key threats or losses can help identify the areas in which insurance coverage is most needed and can better protect the return on your company's insurance investment.

1. Cyber Risks, Threats, or Causes of Loss

Cyber risks, threats, or causes of loss include:

a. Threat Actors

Threat actors are individuals or groups that target a person or an organization. They can be internal or external to a target and known or unknown. Examples include:

- External threats such as third-party hackers and cyber criminals
- Insider threats such as rogue or negligent employees
- Hacktivists (like "Anonymous")
- Business competitors
- State actors

b. Threat Targets

Threat targets include anything of value to the threat actors, such as bank accounts, personal identifying information (PII), confidential business information (CBI), intellectual property, trade secrets, computers, mobile phones, computing devices, hardware, wearables, employee systems, cloud services, automobiles, autonomous vehicles, mass transportation, telecommunications, energy grids, sources or systems, critical infrastructure, or other targeted information or systems.

c. Threat Vectors

Threat vectors are tools or paths that threat actors use to attack the target. These include:

- Malware, ransomware, and cyber extortion
- Emails containing links or attachments, including phishing, spear fishing, and whaling attacks
- Unsecured wireless hotspots
- Mobile devices
- Social networking sites such as LinkedIn, Instagram, and Facebook
- Social engineering schemes
- Removable media like USBs
- Big-data warehouses
- Unsecured employee home networks
- Internet of Things (IoT)

2. Cyber Incidents

Cyber incidents can involve first-party or third-party expenses or both, including the following:

a. First-Party Losses and Expenses

- Forensic analysis to determine extent of damage
- Crisis response costs
- Public relations efforts, including possibly engaging consultants
- Fees for legal advice and counseling
- Business loss, including lost income, impact on reputation, or lost digital assets like intellectual property, customer lists, or other data
  - These losses can originate from a direct breach or a breach of a business partner, vendor, supplier, or company upon which your company is dependent.
- Losses resulting from social engineering schemes, such as fraudulent payments to imposters or other cyber criminals
- Ransom payments, including to cyber criminals
- Physical loss, such as damage to hardware
- Repair, including restoring or replacing data
- Improving cyber security

b. Third-Party Liabilities and Expenses

i. Incidents Involving Compromised Personally Identifiable Information

- For incidents that compromise personally identifiable information (PII) of third parties, such as customers, clients, or patients, the costs of:
  - Contacting and notifying affected third parties
  - Providing credit and identity monitoring
  - Providing call centers for customer service and updates
  - Providing identity restoration services
  - Providing identity theft insurance
  - Replacing credit cards or other products
  - Forensic IT or accounting services
  - Public relations
  - Breach coach counsel
  - Other crisis response actions

ii. Incidents Involving Lawsuits and Similar Claims

- Expenses and legal fees incurred to defend individual lawsuits and class actions
- Amounts the insured becomes legally obligated to pay due to settlement or judgment
- These claims or lawsuits may be brought against:
  - The company by customers whose personal information was compromised
  - The company for failure to adequately hire, train, or supervise employees
  - The company by banks or other financial institutions that may have covered fraudulent charges to customer accounts or that may have replaced compromised credit cards
    - In mid-2017, Home Depot agreed to pay $25 million to settle claims brought by financial institutions arising out of a data breach. See also In re Target Corporation Customer Data Security Breach Litigation, Financial Institution Cases, 64 F.Supp.3d 1304 (D. Minn. 2014) (holding that issuing banks may sue retailers in tort based upon retailers' alleged failure to maintain security resulting in cyberattack); see also Lone Star National Bank v. Heartland Payment Systems Inc., 729 F.3d 421 (5th Cir. 2013) (holding that claims by issuing banks arising out payment card data privacy incidents are not barred by the economic loss doctrine).
  - Directors and officers alleging that they failed to adequately oversee cyber security or procure adequate cyber insurance

iii. Incidents Involving Government Inquiries, Investigations, Subpoenas, Demands and Similar Claims

- Expenses, including fines and penalties, and legal fees associated with government inquiries and investigations, potentially initiated by:
  - Federal Trade Commission
  - Federal Communications Commission
  - Consumer Financial Protection Bureau
  - Securities and Exchange Commission
  - U.S. Department of Justice
  - Other Federal or State Agencies

iv. Other Third-Party Liabilities and Expenses

- Contractual payments or other losses and liabilities for which a policyholder may be liable absent any contractual requirement, including payments related to enforcement of PCI Data Security Standards (PCI DSS) in merchant services agreements
- Remedying the transmission of viruses or other malicious electronic material to third parties

3. Emerging Risks

As technology continues to develop and as the use of that developing technology becomes more prevalent, new risks will continue to emerge and resulting losses will be more frequent. Examples of these risks are:

- **Blockchain.** As Forbes recently put it, blockchain technology is "a distributed and immutable (write once and read only) record of digital events that is shared peer to peer between different parties (networked database systems)." Satoshi Nakamoto—the creator of bitcoin—described it as a "peer-to-peer network using proof-of-work to record a public history of transactions." Commentators predict that the use of blockchain technology will greatly expand in the coming years and reports have found that using blockchain technology may result in billions of dollars of annual savings. Like all technology, blockchain is not without security risks and, therefore, companies should consider whether they would like insurance coverage for such risks.
- **Autonomous vehicles.** Autonomous vehicles such as self-driving automobiles and drones pose unique risks. As this technology is used more and more in supply chains—through self-driving trucks and remote-controlled cargo ships—the potential disruptions resulting from cyber incidents will only expand.
- **Artificial intelligence.** Expanding use of artificial intelligence will likely create unique risks. For example, if a company replaces a job function with artificial intelligence and an error results from the use of artificial intelligence, would the resulting losses be covered under an errors and omissions policy like they would if a human made the same error? Or would that loss fall under a cyber insurance policy? Companies should consider these and similar questions.
- **Internet of Things (IoT).** The Internet of Things refers to the concept of connecting physical items to the internet, including everyday items like refrigerators, cars and the like. When more and more devices become connected to the internet, cyber risks expand. For instance, a cyber incident resulting in bodily injury becomes much more realistic and likely when something like a car is connected to the internet.

C. Types of Cyber Insurance Coverages Available in the Marketplace

Different insurance companies and brokers may refer to applicable coverages with different terms or by different names. Thus, regardless of the label, policyholders should carefully consider all possible threats and causes of loss as well as potential expenses and losses facing the company and work to match those specific exposures and risks with the

corresponding cyber insurance covering them. Generally speaking, policies that provide varying coverages for cyber risks and threats can include those listed below. But as with all insurance, the scope of coverage is dependent on the particular terms and conditions of each policy – "the devil is in the details."

- **Network Security and Privacy** insurance generally covers (a) failures or breaches of the company's network security, such as hackings or virus transmission, and (b) electronic disclosure of confidential information, including personally identifiable information and personal health information, even if not caused by a failure or breach of the company's network security.
- **Digital Asset Protection** will typically reimburse the insured for costs incurred to remedy the loss of intangible physical assets, like software or data, which are in some way compromised due to a network security failure.
- **Breach Event Expenses** insurance is designed to cover the costs the insured incurs while responding to a cyber event. These policies are generally triggered by a privacy incident involving the discovery or notification of a breach, and covered expenses can include computer forensics, legal expenses, public relations management, consumer notification and credit-monitoring services.
- **Business/Network** Interruption and Extra Expense coverages may protect against lost income resulting from a cyber event and can be included in network security and privacy coverages or offered separately. These protections can also extend to cyber events that impact a company that the insured is dependent on and to any system failure beyond network security failure.
- **Media Liability** coverages generally extend to advertising injury claims such as infringement of intellectual property, copyright and trademark infringement, and personal injury torts like libel and slander. This coverage evolved from general liability policies and is often bundled into a media endorsement or section in a cyber policy or a stand-alone media liability policy. It can apply to expenses and damages arising from electronic publishing or other publication of material.
- **Errors and Omissions (E&O)** insurance may cover claims arising from errors in the performance of your services, including technology services like software and consulting. This could include expenses and damages related to the alleged failure of technology products to perform or serve their intended purpose.
- **Directors and Officers (D&O)** policies may cover exposures to a company's executives from claims that negligent corporate governance or oversight contributed

to a company's inadequate cyber defenses and successful cyberattack or breach that caused losses or reduced stock value or both.

- **Reputational** coverage refers to specifically written insurance that covers damage to reputation and expenses to prevent or mitigate damage to reputation.
- **Ransom or Cyber Extortion** coverage can protect against attacks in which data or network capabilities are held hostage pending payment of a ransom, often in bitcoin or other cryptocurrency.
- **Legacy/Traditional Coverages:** In some circumstances, policyholders can seek coverage for cyber-related losses under traditional insurance policies. Such policies include general liability policies, errors and omissions policies, crime policies, and property policies. However, newer general liability policies tend to include exclusions that preclude coverage for cyber-related losses, thus requiring a detailed review to confirm the scope of coverage and the possible need for stand-alone cyber insurance.

II. Worksheet for Obtaining and Negotiating Cyber Insurance Policies

A. First Steps

Identify your company's potential exposures and determine where insurance coverage is most needed.

1. Involve Stakeholders

Consider involving C-suite executives, particularly the Chief Information Security Officer (CISO), Chief Information Officer (CIO), Chief Operating Officer (COO), Chief Legal Officer/ General Counsel, Chief Financial Officer (CFO), and/or Risk Managers in the process.

- When discussing these matters with executives, minimize jargon and technical concepts and explain the consequences of not obtaining insurance, including the monetary consequences that could result from a cyber event.
- Executives and their teams should be or become familiar with what the threats are, what assets are at risk, and how the company's security program minimizes those threats and protects assets. With that background, the executive can better understand how insurance will help mitigate losses should a threat materialize.
- CISOs and CIOs in particular can help identify threats, risks, and potential losses and can help weigh different coverage options through discussions with your legal and risk management teams.

2. Consider Involving Insurance Brokers and Outside Counsel

Think about employing an insurance broker and an insurance coverage attorney who can help identify necessary and available coverage, discuss insurance and legal issues, and assist in the steps below.

B. Complete Insurance Application

It will be critical to involve all stakeholders, especially information technology and network security personnel, in the completion of your company's insurance application. Involve legal and operations team members to ensure your company provides correct and complete responses on your insurance application.

Practice Tips:

- **Accuracy:** While many applications can be time-consuming, particularly for cyber-related insurance, it is better to take the time to provide accurate answers rather than face an insurer trying to use an allegedly inaccurate answer to avoid coverage after a claim arises. Even unintentional inaccurate answers or unintentional omissions can cause issues.
- **Avoid Definitive Answers to Questions About Your Evolving Risk Control Measures:** Describe risk control measures generally and broadly, and work diligently to adhere to those measures after submitting the application. In addition, be cautious when giving definitive statements or warranties regarding your own or others' conduct. Anticipate future arguments by insurers seeking to void the insurance contract due to inaccuracies in your application by "painting with a broad brush" to the extent possible.
- **Representations:** If answering questions about a third party's practices, couch responses in terms of what representations were made to your company. For example, if asked about the due diligence used to confirm that the provider's practices comply with applicable laws, consider beginning the response with "the cloud service provider represents that . . . ."
- **Awareness:** Be careful when responding to questions regarding cyber events because such events could go undiscovered for some time. For example, the company may have experienced a hacking event before the application, but that hacking event may not be known at the time the application is completed. So, when answering questions about prior cyber events, include a caveat based on present awareness.
- **Ambiguity:** Be wary of potentially ambiguous questions. For example, if asked, "Are all users of the applicant's network issued unique passwords," seek clarification as to what the insurance company means by "users"; i.e., does it mean employees, or employees and customers, or something else.
- **Corporate Knowledge:** Pay close attention to how the application defines "you" or "your" or any similar term. For example, applications may ask about "your" knowledge of events that may lead to claims and then define "your" as including all of the company's employees. Such broad definitions are troublesome, since a single employee may know about an event that relates to claims but has not yet passed that knowledge on to the individuals responsible for completing the insurance application. Thus, limit terms like "your" to the company's control group, such as enumerated executives and its risk manager. Similarly, if the application leaves this issue ambiguous, companies can clarify that their answers are based on the present knowledge of the control group.

- **Effect on Subsequent Claims:** Be cognizant of the fact that in the event of a subsequent cyber loss or claim, insurance companies will often seek to use your answers to limit or preclude coverage. Giving truthful and complete responses may reduce that risk.

Applications for renewing insurance with a particular insurer are generally different from applications for purchasing insurance for the first time from that insurer. Renewal applications can incorporate prior applications. It is therefore crucial to pay attention to whether a renewal application incorporates prior applications and, if so, to review prior applications to assess potential risk based on representations made on those applications and to make clarifications if necessary.

C. Consider Insurer Proposals

Unlike coverage provided by other types of insurance policies, coverages provided by cyber-related policies are not yet standardized and can vary widely from insurer to insurer. Thus, in choosing an insurance policy, price alone should not be the determining factor. The cheapest policy may also provide significantly less coverage than a more expensive policy.

Also, unlike other common insurance policies, there is no standardized cyber form that most insurers use. Rather, each insurer uses its own unique "manuscript" form or policy. And because of the developing nature of cyber risks, each insurer is constantly reevaluating the coverage it provides. So, as a general matter, the policy language is highly negotiable, and companies should not feel constrained to accept the policy that the insurer first offers.

When considering the policy that the insurer offers, note the following aspects of the coverage. The importance of these specifications can vary based on the policyholder's business and pricing concerns.

1. *Who* Is Covered

Consider what individuals and entities are covered as insureds. Be certain that all relevant companies, subsidiaries, and affiliates that you intend to be covered are, in fact, covered. Also, determine whether directors and officers are covered. Those individuals may face lawsuits arising out of cyber events that include allegations related to improper corporate governance or oversight of security or privacy practices. For example, a December 2016 lawsuit against Wendy's and 19 current and former directors and officers made a variety of those types of

allegations, including a claim for "failing to implement and enforce a system of effective internal controls and procedures with respect to data security." And directors and officers insurance policies may exclude coverage for such cyber-related lawsuits, leaving a coverage gap.

2. *What* Is Covered

Next, scrutinize what is covered, including the following.

- What data is covered?
  - Pay close attention to the policy language. Consider *InComm Holdings Inc., et al. v. Great American Insurance Co.,* case number 1:15-cv-2671 (N.D. Ga. 2017), which held that a debit card service was not covered under a computer fraud policy that covered data lost through use of a computer because the fraudulent debit card redemptions were made over the phone.
- What physical loss is covered?
- What business loss is covered?
  - Is there a "waiting period" after a cyber event during which the insurer will not cover losses, such as lost profits?
  - Is there an end date following a cyber event after which the insurer will not cover any losses, such as lost profits? o
- How long does coverage last?
- What costs related to responding to a data breach or other cyber event are covered?
- Is employee error covered?
- Are ransom or extortion payments covered?
  - Ransomware attacks are increasing. A ransomware attack occurs when a hacker takes control of a company's electronic files and then demands that the company pay to release the files.
  - As internet and infrastructure become increasingly connected, including through the Internet of Things, ransom demands can have more dramatic consequences. Consider the case of an Austrian hotel, in which hackers shut down a hotel's keycard management system, effectively locking hotel guests outside their rooms until ransom was paid in bitcoin (https://cdn.ampproject.org/c/www.thelocal.at/20170128/hotel-ransomed-by-hackers-as-guests-locked-in-rooms/amp). The hotel's managing director indicated that its insurance policy would not cover the hotel's losses.
  - Hackers may demand payment in non-standard currency such as bitcoin (as they did in the Austrian hotel example above). It is important to ensure that your policy would cover such payments.

- Are internal investigation costs or the costs of responding to governmental inquiries and investigations covered?
- Are additional costs incurred in complying with government regulations following a cyber event covered?
- Are penalties or fees imposed by the government covered?
- Are penalties or fees imposed by contractual agreement covered?
- Are claims of emotional distress by individuals whose confidential information was accessed, disclosed, or published covered?
- Are losses resulting from physical instrumentalities like fire, wind, or water covered?
- Are losses resulting from theft of physical devices like computers and phones covered?
  - While a normal property insurance policy should cover the loss of a stolen computer, it may exclude coverage for the disclosure of confidential information on the stolen computer, for instance.
- Are losses resulting from cyber terrorism, foreign enemies, state actors, or cyber warfare covered?
- Policies may exclude these types of losses, and such exclusions can be particularly problematic given the increasing awareness of the involvement of state actors in hacks.
- Are losses resulting from third parties' cyber events covered?
  - Given the increasing ubiquity of the Internet of Things, obtaining coverage for this type of loss can be very important. See *Coverage Risks in the Age of the 'Internet of Things'*, Lon Berk & Paul Moura, Law360 (Jan. 3, 2014); *The Risk of Insuring Supply Chains From Cyber Risk*, Lon Berk & Sergio Oehninger (June 29, 2015).
- Are losses resulting from portable electronic devices covered?
- Are losses resulting from leased, vendor-owned or employee-owned electronic devices covered?
- Are claims against the company alleging that the company's failure to hire, train, or supervise its employees properly resulting in a cyber event covered?
- Are bodily injury and property damage covered?
  - This is another area in which the increasing ubiquity of the Internet of Things is an important consideration, since a cyber event could lead to bodily injury or property damage as a result of a malfunction of a physical object that is connected to the internet.

3. Coverage Depends on Policy Language and Particulars of Cyber Event or Claim

As with all insurance policies, coverage can depend on the actual language used in a particular policy. And as noted above, this is particularly true in the cyber insurance context, as standardization of policies is at an early stage. Consider the examples below:

- Coverage can depend on how the policy defines the electronic system from which losses must emanate. Insurers' form policies use various terms, including "Computer System," "System," and "Digital Assets." One insurer's form includes coverage for cloud computing in some instances, but not in others. That same form is arguably unclear on whether there is coverage for cyber events arising out of mobile devices that are not traditionally labeled as computers. Other forms are clearer that there is coverage for cyber events arising out of such mobile devices.
- Coverage can also depend on how the policy defines confidential information. For instance, one insurer's form requires such information to include a person's first name or initial and last name, while another contains no such requirement. As another example, one form includes a third party's non-public information, while others do not. These distinctions can create significant differences in the coverage ultimately available.
- Coverage may be affected when there are covered and non-covered causes of injury. Some policies may allow the insurer to allocate costs or expenses between covered and non-covered causes. Insurers may use such provisions to decrease the amount they pay by claiming that certain costs or expenses resulted from non-covered causes. Other policies may only pay when the cyber event is the "overriding cause" of the loss, which is another provision insurers may invoke to avoid payment.

4. Consider Overall Coverage in Light of Key Cyber Risks and Identify Potential Gaps

Risk managers should conduct a side-by-side analysis using multiple breach scenarios to understand how an insurer's policy works and identify gaps or overlaps in coverage. Coverage counsel should be part of the gap analysis team. An eye on recent case law interpreting policy language should be integrated into the placement stage to help policyholders avoid later coverage disputes. Examples of potential gaps include:

- Losses resulting from voluntary transfer of funds based on social engineering scam
- Contractual payments resulting from cyber events, like payments related to enforcement of PCI Data Security Standards (PCI DSS) in merchant services agreements
- Damages resulting from data lost due to physical loss of hardware
- Coverage for bodily injury and property damage resulting from cyber event, which is of particular concern given the increasing prevalence of the Internet of Things

Also, contemplate whether your policy provides coverage only for actual cyber events, as opposed to alleged or reasonably suspected cyber events. Companies can spend

significant sums investigating whether an event actually occurred, and limiting coverage to actual cyber events may leave companies without coverage for such an investigation.

5. Applicable Limits and Sub-Limits and Related Considerations

a. Limits and Sub-Limits

Companies should also evaluate carefully the policy's coverage limits and sub-limits. For context, according to recent studies, data breaches often result in millions of dollars in costs, and average costs per lost or stolen record can run in the hundreds of dollars.
When evaluating limits, it is important to know whether expenses like attorneys' fees are covered within limits or in addition to limits. Most often, expenses are covered within limits, but a policy that covers expenses in addition to limits can provide significantly more coverage.

Limits can apply to the entire policy or can apply to individual coverages offered within a policy. For example, a policy may have an overall limit of $10 million and also have a $5 million sub-limit on privacy and network liability coverage.

Sub-limits apply to very specific portions of the policy. For instance, a sub-limit could apply to losses arising from a government investigation, coverage for payment card industry claims and losses, cloud-based exposures, or losses resulting from a cyber event at a third-party vendor.

Thus, sub-limits significantly affect the value of coverage for the type of loss or claim that is subject to the sub-limit. *See, e.g., State National Insurance Company v. Global Payments*, 2013 WL 2468621 (N.D. Ga. Apr. 12, 2013) and 2014 WL 940404 (N.D. Ga. Jan. 7, 2014). In *Global Payments*, a credit card processor paid substantial sums to the payment card companies as a result of a data privacy incident. The insurer argued that certain lower sub-limits applied to the credit card processor's coverage, which would materially limit the amount of coverage available for the loss. Before the court ruled on the insurer's argument, the case settled. This serves as an example of why it is important for policyholders to understand sub-limits in their cyber insurance policies and how they may affect their ability to protect themselves against cyber risks.

b. Deductibles, Retentions, and Co-Insurance

In addition to considering limits and sub-limits, the company should assess deductibles or retentions, as well as co-insurance. While deductibles and retentions are different, generally

speaking, they both are the amounts that must be paid or deducted before the insurance will pay. Higher deductibles or retentions can be used to lower premium payments; they would require the policyholder to pay more of the everyday claims, yet would maintain insurance coverage for more catastrophic claims. Co-insurance requires the policyholder to pay a certain percentage of the total loss.

Cyber insurance is largely designed to protect against low-frequency but high-severity cyberattacks affecting very large numbers of electronic records. But costs associated with a majority of data breaches fall below deductibles in cyber policies. Thus, for large corporations, deductibles may not be a concern, but for smaller companies or companies with tighter budgets, deductible costs can present a significant problem. There is not a one-size-fits-all solution to these challenges, which businesses must address on a case-by-case basis.

In addition, while older policies provided full coverage for post-breach events such as forensic analysis and data breach notification to customers, newer policies may make those services subject to high deductibles and retentions. Deductibles for the costs of forensic investigation, breach letters or crisis management are typically lower than deductibles for class actions or regulatory investigations. Companies should consider these issues at the placement stage, depending on the company's needs, structure and budget.

6. Considerations for Directors and Officers Coverage

Shareholder derivative suits against executives alleging failure to take proper measures to protect the company from a data breach are on the rise. To ensure the sufficiency of executive liability coverage, your company should seek to include data breaches and other cyber risks or claims within the scope of coverage afforded by your company's D&O policies, in as broad terms as possible. Issues may include:

- Directors and officers should be covered under traditional D&O policies, but D&O policies may have exclusions prohibiting coverage for cyber events. Some of those exclusions can be worded broadly enough to include privacy-related torts. Be mindful of exclusions and make sure that privacy-related liabilities aren't excluded.
- In addition, carefully evaluate cyber policies to identify available coverage for directors and officers, keeping in mind the rising prevalence of shareholder derivative suits alleging failure to protect against data breaches. Insurance companies may be willing to provide endorsements meant to extend coverage to directors and officers.

7. Other Aspects of Coverage to Consider

a. Triggers

Coverage can be triggered by a claim made during the policy period (claims-made coverage), by a cyber event occurring during the policy period (occurrence-based coverage), or by a cyber event discovered during the policy period (discovery-based coverage). Companies should evaluate whether any of the possible triggers are better or worse for them, which often depends on the triggers in prior policies. As a general matter, occurrence-based coverage should be avoided since it can be difficult to pinpoint the time at or during which a cyber event occurs.

In addition, the different coverages in an insurer's forms may contain different triggers. If that is the case, companies should assess carefully the interplay between the different coverages.

b. Notice

Policies contain different requirements for providing notice to the insurance company. Pay attention to these requirements and ensure they are realistic and achievable, particularly in the fast-moving environment of responding to a cyber event. See Flow Chart.

c. Retroactive Date

Generally speaking, an event must occur after the policy's retroactive date to trigger coverage under the policy. The retroactive date is particularly important in the cyber context since cyber events like data breaches can go undiscovered for lengthy periods of time. A retroactive date that is earlier than the policy period will provide prior-acts coverage; *i.e.*, coverage for losses arising out of events that precede the institution of the policy. If the retroactive date is the same as the date on which the policy begins, coverage for such prior events is likely to be precluded. Thus, the earlier the retroactive date, the more likely the policy will cover previously undiscovered cyber events.

d. Coverage Territory

Coverage territory refers to the area in which an event must occur to trigger coverage under the policy. A U.S. company can have losses in the U.S. resulting from a hacking attack originating from a foreign country or targeting assets in a foreign country. Thus, a worldwide coverage territory is preferable.

e. Selection of Third-Party Vendors

Policies vary on whether the insurer or policyholder selects third-party vendors such as outside counsel, public relations firms, forensic investigators, etc. As a general matter, it is preferable for the policyholder to select third-party vendors.

Some policies have lists of vendors from which the policyholder may choose. If your company has preferred third-party vendors, be sure to ask the insurer to add those to any such list.

Some policies allow the insurer to select third-party vendors, even when the claim is within the company's retention or deductible. As a general matter, companies should avoid such provisions.

f. Control and Consent

Consider whether the insurer or policyholder controls the response to the cyber event and any related litigation. Similarly, the policy may contain provisions requiring the policyholder to obtain the insurer's consent before acting. Such consent requirements can be particularly problematic when responding to a cyber event, which often requires immediate action. If the policy contains consent provisions, be sure to include a provision that the insurer may not unreasonably withhold consent.

If the insured's consent is required before the insurer can enter into a settlement, the policy may contain what is known as a hammer clause. That clause significantly reduces the insurer's future obligations (often as a percentage of its current obligations) if the insurer wants to settle but the insured refuses to provide consent.

If the policy contains any consent requirements, ensure that they are prominently noted in any manual of policies and procedures related to responding to cyber events.

Also, be sure your insurer approves your preferred choice of defense counsel up front and negotiate to have your counsel's rates approved to avoid a dispute in the event of a cyber event or claim.

g. Cooperation

Carefully review the cooperation requirements. Policies should require reasonable cooperation, not unlimited cooperation.

h. Dispute Resolution

Determine whether the policy requires mediation or arbitration of disputes under the policy and whether the policy mandates the application of a particular law.

i. Definition of "Security Event"

The definition of "Security Event" or similar concept in your cyber insurance policy may be critical to the scope of coverage. As an example, many cyber policies define "Security Event" to mean "unauthorized access to a Data Asset." Thus, the mere existence of malware on a company's Computer System may not constitute a Security Event under such a definition; unauthorized access to "a" Data Asset would be required, and if that unauthorized access occurred after policy inception, the policy should be triggered whether or not other Data Assets were accessed previously. That result might be different if, for example, the policy defined "Security Event" as "unauthorized access to *any* Data Asset." This example underscores the importance of the particulars of the policy and facts at issue.

j. Excess Coverage

Excess and umbrella policies apply after a loss exceeds the limits of a primary policy. Excess and umbrella policies can provide extra protection for your company's cyber exposures and risks, especially for catastrophic events.

k. Price

As stated above, premiums can vary, but a lower premium may not reflect a better deal and may merely reflect less coverage.

8. The Insurer

Evaluate the insurance company, including:

- Capabilities. For example, if your company has worldwide locations, does the insurer have capabilities to assist in responding to a cyber event in the relevant locales?
- Reputation for paying and handling claims.
- Experience in writing cyber coverage and handling cyber claims.
- Financial stability and ratings (A.M. Best, Standard & Poor's, Moody's Investors Service, and Fitch Ratings all provide ratings for insurance companies).

D. Next Steps

Obtain a complete copy of the policy. While a binder or certificate of insurance may provide evidence that an insurance policy is in force, companies should nevertheless obtain the actual policy document to know the precise terms of their coverage and responsibilities under the policy.

- Practice Tip: Companies should have a depository for insurance policies and should organize and label them so that they are readily available if needed. It is also a best practice to have insurance program schematics and policy charts created as reference tools and high-level reviews of your insurance program structure.
- Whenever changes occur in your business, consider whether they will require you to make changes to your insurance policy.
- Practice Tip: Do not wait until an insurance policy is up for renewal to ask for changes. If your company faces a new or changed risk, you can discuss adding or changing coverage with your insurance company at any time.

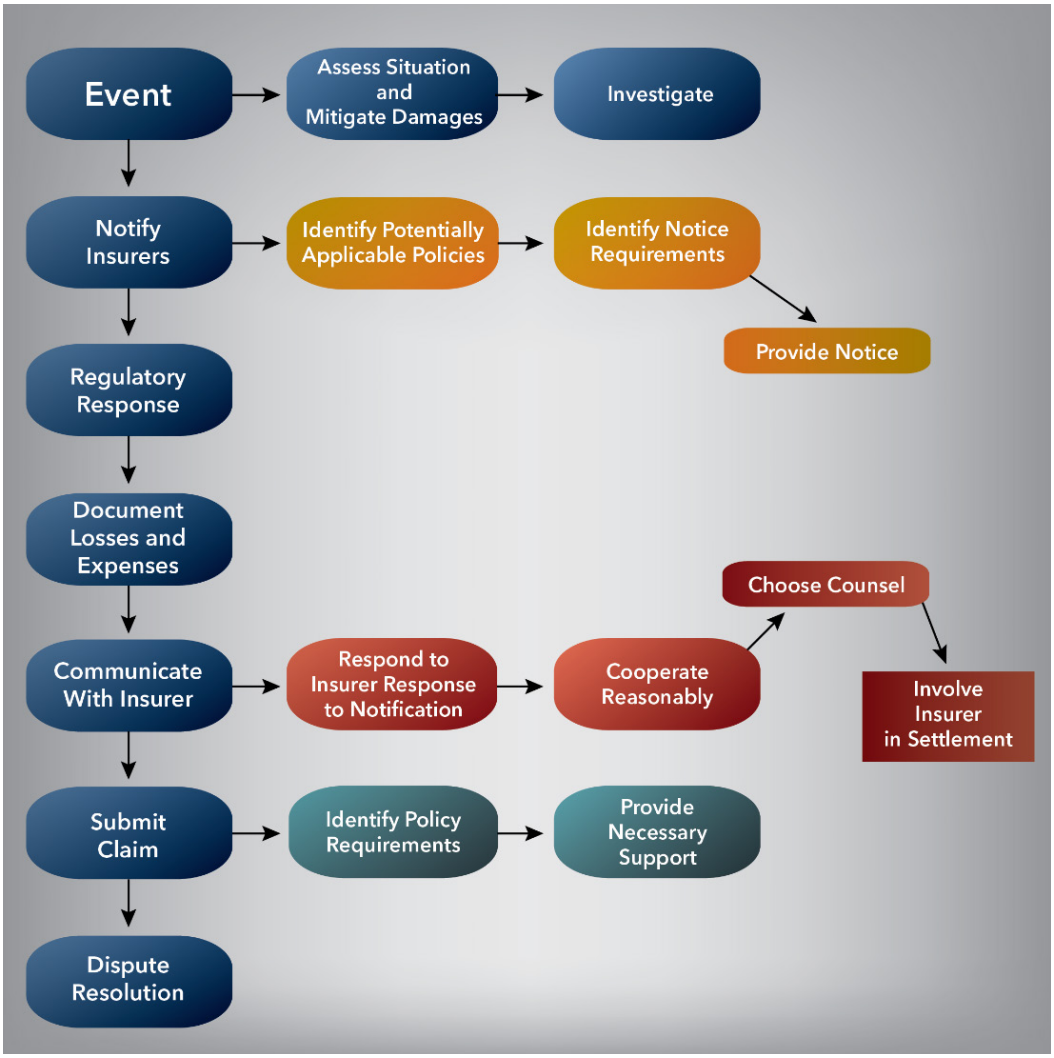
E. Policies Issued to Third Parties

In addition to obtaining their own policies, companies should consider requiring certain third-party vendors to obtain cyber insurance coverage and ensure that those policies cover any liability to the company resulting from a cyber event affecting the third-party vendors, including by adding the company as an additional insured.

In connection with this process, companies should ascertain whether any insured vs. insured ("Ivl") exclusions exist in the third-party vendor's policy. Depending on the nature of the exclusion and the manner in which the company is named as an additional insured, the policy may end up eliminating a potential source of discovery (as when a lawsuit by the company against a third-party vendor is excluded from coverage due to Ivl exclusions). Moreover, if other customers of the third-party vendor are also additional insureds, claims between customers may also be excluded.

III. Post-Cyber Incident Steps Flow Chart

Flow Chart – Steps to Optimize Coverage Following a Cyber Event



A. Event

1. Assess Situation and Mitigate Damages

Immediately after an event, companies should mobilize to get the situation under control and initiate any emergency response plan in place, including working with lawyers and vendors to minimize potential damages and ensure compliance with potentially applicable laws and regulations. Cyber policies may provide coverage for these expenses; they may

also require companies to take these steps. In addition, policies may require companies to use particular attorneys and third-party vendors to obtain coverage for the expenses. Understanding such limitations in advance will help maximize insurance coverage.

2. Investigate

Companies should immediately begin to investigate the cause of the event and loss, identify the types of loss and damage, and evaluate potential solutions. These are also important steps in obtaining insurance coverage.

B. Notice to Insurers

Upon learning of a cyber incident, companies should immediately review the notice requirements in their insurance policies and strongly consider notifying their insurance companies about the incident. Generally, companies should provide notice to any insurance company that has issued a policy under which the company may want to attempt to obtain coverage.

1. Identify Potentially Applicable Policies

a) Companies should first look to any cyber-specific insurance policy they have.
b) They should also look to traditional insurance policies, including commercial general liability policies; property policies; business interruption/continuity policies; directors and officers policies; errors and omissions/professional liability policies; and crime policies, among others. While these policies may exclude coverage for cyber-related losses, policyholders have successfully obtained coverage under standard policies for such losses.
c) Also, be aware of policies issued to others, such as business partners, contractors, vendors, or suppliers, under which your company may be entitled to coverage as an additional insured or under other contractual or equitable theories.

2. Identify Notice Requirements

Most policies contain provisions requiring companies to provide notice of an incident within a certain time frame. Notice provisions vary from policy to policy. Some may require notice as soon as possible or practicable. Others may require notice within a certain number of days. Policies should be reviewed carefully to identify the applicable notice requirements. Failure to provide timely notice can impact the availability of coverage. See *Retaining Insurance Coverage in the Face of Late Notice and Misconduct Exclusions,* Sergio Oehninger, Risk Management (August 2015).

3. Provide Notice

Policies are also likely to contain provisions about the method by which companies must provide notice to the insurer, including with respect to specific coverages or sub-limits within the policy that the company believes will apply. Companies should follow those provisions closely to avoid providing any insurance company with a technical defense.

C. Regulatory Response and Notification Costs

Data breaches may trigger responses from regulatory agencies, including the Federal Trade Commission, Federal Communications Commission, Consumer Financial Protection Bureau, Securities and Exchange Commission, Department of Justice, and state regulatory agencies. Those actions can result in high response costs, including mandatory and recommended notification costs, attorneys' fees, and crisis response costs, among other expenses, and can lead to settlements, damages, penalties, or fines. While coverage for such amounts varies policy to policy, cyber-specific policies and other policies like directors and officers policies will often cover expenses incurred in responding to such investigations.

D. Documentation

1. Record Keeping

Businesses should also keep records regarding the losses suffered, including documenting any physical damage (including to data), amounts paid to prevent further damage or remedy existing damage, and amounts lost due to the disruption of business activities. Maintaining these records will prove helpful in seeking recoveries under insurance policies.

2. What to Document

Policyholders should document all losses and expenses. Doing so will protect the company in the event that a loss or expense is later covered by insurance. For example, with respect to a cyber incident, the company should keep track of things like investigation expenses and remediation expenses.

E. Interaction with Insurer

1. Insurer Response to Notification

Insurers will likely respond to the initial notice of an incident in one of four ways:

- ask for more information;
- deny coverage;
- acknowledge coverage; or
- acknowledge coverage or potential coverage in whole or in part but reserve their right to later deny coverage.

Policyholders should carefully consider their responses to such insurer communications.

2. Cooperation

Most policies place a duty to cooperate on the policyholder. The contours of the duty will depend on the policy language and applicable law. However, as a general matter, the policyholder need not cooperate with unreasonable or burdensome requests or requests solely designed to help the insurer later deny coverage.

3. Consent to Settlement

Some policies contain a requirement that the policyholder obtain the insurance company's consent to settle claims against the policyholder or assume any financial obligation. These provisions can turn into traps for policyholders that do not involve their insurance companies in settlement or related negotiations. These clauses are generally subject to a reasonableness standard so that the insurer may not refuse to consent to a reasonable settlement.

4. Counsel

Insurers may try to select counsel for your company to use in connection with dealing with the data breach and any related litigation. However, you may be entitled to counsel of your own choosing. This will depend on the policy provisions and applicable law. This issue can also be addressed before purchasing your policy by specifically identifying your preferred counsel in the policy.

F. Claim Submission

1. Identify Policy Requirements

Some policies have specific requirements that must be met in company submissions for reimbursement of losses. Be sure to identify and address those requirements to avoid the insurer raising any technicalities.

2. Documentation

Providing the documentation necessary to support the claim submission will avoid technical and tactical delays on the part of the insurance company. This is particularly true for cyber incidents, where damages are not always as apparent as in run-of-the-mill liability cases.

G. Dispute Resolution

- If an insurance company denies coverage, formal dispute resolution is sometimes the only way to obtain the coverage that the company is entitled to.
- Some policies require that disputes be submitted for arbitration. Those policies often contain specific rules for initiating the arbitration and proceeding in the arbitration. Those rules are generally enforceable.
- Some policies contain mandatory mediation requirements before proceeding to other formal dispute resolution. Like the arbitration requirements, these clauses contain specifics as to how mediation must proceed.
- To best position your company for successful dispute resolution and to maximize cyber insurance coverage, the steps described in the sections on Interaction and Claim Submission above should be carefully followed and documented.
- If the company chooses instead to file a lawsuit, the forum for that litigation can have a large impact on the resolution of the case, so companies should carefully evaluate where to file any such lawsuit.

IV. Communicating With Your Cyber Insurer

A. Responding to Insurer Coverage Positions

Insurer coverage positions will largely fall within three categories:

(1) denying coverage;
(2) accepting coverage but under a reservation of rights; and
(3) accepting coverage.

Below we highlight some of the key considerations in responding when the insurer denies coverage (scenario 1) or accepts coverage under a reservation of rights (scenario 2).

1. Insurer's Denial of Coverage

- Evaluate the basis for denial and carefully review your insurance policy. If the insurer's basis for denying coverage is unsound, challenge it in writing.
- If the insurer sticks to its denial, evaluate whether to keep the insurer updated with respect to the progress of the company's response to the cyber event, any claims arising out of the event, and any related settlement negotiations. While there is no general requirement to do so once the insurer denies coverage, a duty could arise under applicable law or specific policy language. Moreover, even if it is not required, keeping the insurer up to date even though it denied coverage can be beneficial, particularly to head off the possibility of later arguments based on the insurer's alleged lack of knowledge, and because subsequent developments might cause the insurer to reevaluate the denial.
- Evaluate whether to use the insurers' preferred or required third-party vendors for things like forensic analysis, public relations, and outside counsel.
- If the insured wants to pursue coverage and will need to bring suit, evaluate when and where to file. Timing can depend on a variety of factors, including:
  - the applicable statutes of limitations;
  - the policyholder's capability to fund the response to the cyber event without insurance;
  - the policyholder's willingness to "fight" the insurer while at the same time responding to the cyber event; and
  - whether the applicable law requires a resolution of any underlying lawsuit before determining insurance coverage issues for that lawsuit.

2. Insurer's Acceptance of Coverage Under Reservation of Rights

- A reservation of rights means that the insurer is maintaining its ability to deny or limit coverage at a later time. Faced with a reservation of rights by the insurer, the insured must make the following assessments and decisions:

- Evaluate whether to tell the insurer expressly that the policyholder is not accepting the insurer's reservation of rights. The effect of such a declaration can vary depending on the policy language and the applicable law.
  - **NOTE:** This consideration is particularly important when the insurer attempts to reserve its rights to recoup attorneys' fees incurred in defending any litigation against the policyholder.
- Evaluate whether the insurer's reservation of rights releases the policyholder from certain obligations under the policy or allows the policyholder to act in ways it could not act if the insurer acknowledged coverage without reservation. For example, a reservation of rights may entitle the policyholder to pick third-party vendors not otherwise available to the policyholder.
- Evaluate whether the insurer's reservation of rights creates a conflict between the insurer's interests and the insured's interests that alters or modifies the parties' rights and obligations under the contract or changes the dynamics between the insurer and its insured.
- Evaluate any privilege issues raised by a reservation of rights. (See the Preservation of Privilege section below.)

B. Responding to Insurer Requests for Information

Insurers will undoubtedly ask for information about the policyholder's claim. Although the volume of documents can be enormous, the policyholder should not let requests for significant amounts of information discourage it from pursuing coverage. Keep in mind that the policyholder generally need only respond to reasonable requests; onerous requests can and should be resisted.

Also, keep in mind that the insurer may be seeking information to help it find ways to deny coverage. In responding to insurers' requests, two other items to consider are:

(1) the duty to cooperate; and

(2) the preservation of applicable privileges.
Always review policy language first. Different policies may contain different requirements.

C. Duty to Cooperate

1. Source of Duty

- Generally, insurance policies require the policyholder to cooperate with the insurance company. For example, a policy may provide that "You and any other involved insured must cooperate with us in the investigation, settlement, or defense of the 'claim' or 'suit.'"
- Even in the absence of a specific contractual duty, common law duties may require the policyholder to cooperate with the insurance company. For example, policyholders have a duty to act in good faith in their dealings with insurers. That duty may include a duty to cooperate. See *First Bank of Turley v. Fid. & Deposit Ins. Co. of Maryland,* 928 P.2d 298, 304 (Ok. 1996) (stating that policyholder's duty to cooperate is "both contractual and implied in law").

2. Cooperation Requirements

- Policyholders are generally required to respond to reasonable requests for information about the loss at issue. See, for example, *Pilgrim v. State Farm Fire & Cas. Ins. Co.,* 950 P.2d 479, 483 (Wash. Ct. App. 1997) (duty to cooperate requires policyholder to provide answers to requests that are "reasonably relevant and germane to the insurer's investigation").
- Some policies require policyholders to cooperate generally; some have specific cooperation requirements. The policy may require that the policyholder request that other insurance companies provide a defense to the policyholder, for example.
- The insurer must exercise reasonable diligence in seeking the policyholder's cooperation. See, for example, *Med. Protective Co. v. Bubenik,* 594 F.3d 1047, 1051 (8th Cir. 2010).
- Some states, like New York, will not find a breach of the duty to cooperate unless the insurer can demonstrate that the attitude of the policyholder in response to cooperation requests was "one of willful and avowed obstruction." See *Cooper v. New York Cent. Mut. Fire Ins. Co.,* 72 A.D.3d 1556, 1557 (N.Y. App. Div. 2010).

3. Examples

a. Actions That May Be Required

- Depending on the policy language and applicable law, the duty to cooperate may require:
  - that the policyholder participate in its defense. See *Davila v. Arlasky*, 857 F.

Supp. 1258, 1264 (N.D. Ill. 1994) (finding policyholder failed to cooperate where policyholder disappeared and did not participate in trial preparation).

- that the policyholder answer relevant questions about personal and business finances and turn over relevant financial records. See *Tran v. State Farm Fire & Cas. Co.*, 961 P.2d 358, 364 (Wash. 1998) (policy gave insurer right to question policyholder about any matter and to examine and audit policyholder's books and records).
- that the policyholder provide information requested and not conceal relevant facts.
- that a policyholder waive the Fifth Amendment privilege against self-incrimination or risk forfeiting coverage rights. See *Bogatin v. Fed. Ins. Co.*, 2000 WL 804433 (E.D. Pa. June 21, 2000).

b. Actions Not Required by the Duty to Cooperate

- The duty to cooperate does not require:
- that the policyholder decline or defer reasonable settlement offers to allow the insurer to determine its coverage obligations. See *Allied Prop. & Cas. Ins. Co. v. Ellinger*, 2006 BL 173909 (Mich. Ct. App. Aug. 31, 2006).
- that after the insurer denies coverage, the policyholder refrain from entering into a reasonable settlement with the underlying claimant that includes an agreement that the claimant will only seek collection of the settlement amount from insurer. See *McNicholes v. Subotnik*, 12 F.3d 105, 109 (8th Cir. 1993) (finding that policyholder did not breach cooperation clause where insurer had denied coverage and policyholder then entered into settlement agreement that included agreement that victim would not seek settlement amount from policyholder).
- "that an insured engage in, or support, a fraud, misrepresentation, or untruth in order to maintain its coverage." *W. Am. Transp., LLC v. Morrow*, CIV.A.99-2217, 2006 WL 2375615 (W.D. La. Aug. 15, 2006) aff'd, 2008 WL 182208 (5th Cir. Jan. 22, 2008).

4. Consequences of Breaching the Duty to Cooperate

- If you breach the duty to cooperate, you can, in the worst case, lose all protection under the insurance policy.
- In some states and under some policies, a breach by itself is sufficient to lose all protection. See *KHD Deutz of Am. Corp. v. Utica Mut. Ins. Co.*, 469 S.E.2d 336, 338 (Ga. Ct. App. 1996) (where cooperation clause was a condition precedent to coverage, insurer was not required to show prejudice).
- In other states and under other policies, an insurer must show that the breach of the cooperation clause prejudiced the insurer before the insured loses all

coverage. See *Truck Ins. Exch. v. Unigard Ins. Co.*, 79 Cal. App. 4th 966, 976 (Cal. Ct. App. 2000) ("Where an insured violates a cooperation clause, the insurer's performance is excused if its ability to provide a defense has been substantially prejudiced."); *Bankers Ins. Co. v. Macias*, 475 So. 2d 1216, 1218 (Fla. 1985) ("In a breach of cooperation clause case, however, the insurer must show a material failure to cooperate which substantially prejudiced the insurer.").

D. Preservation of Privilege

1. Potential Problem

- Policyholders will often have privileged information about the underlying claim for which they are seeking coverage under an insurance policy. Insurers may request that privileged information, and policyholders may want to share that privileged information with their insurers.
- Where otherwise privileged information or documents are disclosed to a third party outside of the attorney-client relationship, however, courts will generally find that privilege does not apply or that privilege has been waived.
- So under the general rule, if a policyholder discloses otherwise privileged information to its insurer, other parties may contend that the information is no longer privileged.

2. Potential Solution

- The common-interest doctrine can provide policyholders with protection in these situations. See *Enns Pontiac, Buick, & GMC Inc. v. Flores,* CV-F-07-01043 LJO, 2011 WL 6181924 (E.D. Cal. Dec. 13, 2011) (finding common interest between policyholder and insurer and stating that "therefore disclosures of privileged information between the two would not waive an existing privilege"). The doctrine can help preserve privileges where privileged information is disclosed to a third party.
- The common-interest doctrine protects the attorney-client privilege to permit parties with common interests to coordinate their positions. It can apply where communications are in furtherance of the parties' common interest.
- Protection under the common interest doctrine may not extend to privileged documents disclosed to insurers when there is a conflict between the insured and the insurer (such as when the insurer has reserved its rights or has yet to decide whether to provide coverage). See *Northwood Nursing & Convalescent Home, Inc. v. Cont'l Ins. Co.,* 161 F.R.D. 293, 297 (E.D. Pa. 1995) (no common interest where

insurer had not yet made a coverage determination); *Int'l Ins. Co. v. Newmont Min. Corp.,* 800 F. Supp. 1195, 1196 (S.D.N.Y. 1992) (common-interest doctrine did not apply where insurer had declined coverage and failed to provide a defense). But see *Enns Pontiac, Buick, & GMC Inc. v. Flores,* CV-F-07-01043 LJO, 2011 WL 6181924 (E.D. Cal. Dec. 13, 2011) (finding common interest applicable even where insurer was defending underlying lawsuit under reservation of rights). Policyholders should therefore exercise caution when deciding whether to share privileged information with their insurers.

- In addition, policyholders should be aware that insurers may attempt to use the common-interest doctrine to compel a policyholder to produce privileged documents exchanged between the policyholder and an attorney retained by the policyholder. See, for example, *Waste Mgmt., Inc. v. Int'l Surplus Lines Ins. Co.,* 579 N.E.2d 322, 329 (Ill. 1991) (requiring policyholder to disclose files of law firm hired by policyholder to policyholder's insurer). When facing such attempts, policyholders should carefully examine the applicable law and weigh the risk of privilege waiver against the risk of the insurer denying coverage on this basis.

V. Snapshot of Potential Legal Issues in Obtaining Coverage for Cyber Exposures and Liabilities

Because of the unique and evolving nature of cyber-related liability, the law with respect to insurance coverage for cyber-related incidents is not as well developed as it is with respect to more traditional forms of insurance coverage. Below we highlight some of the key points from the developing case law, first with respect to cyber-specific insurance policies and then with respect to traditional insurance policies that cover a variety of risks.

A. Cyber Insurance Policies

Published and unpublished court decisions involving coverage under policies tailored to cover cyber-related events are rare, possibly due to the fact that such policies are still a relatively recent offering.

1. Privacy Injury

In a recent federal court case in Arizona, the insurer had paid nearly $2 million to a restaurant for losses resulting from a cyber breach and the issue was whether additional payments by a restaurant to a third party it had hired to process credit card payments made by its customers were reimbursable under the "privacy injury" coverage provision of the restaurant's insurance policy. *P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.*, No. CV-15-01322-PHX-SMM, 2016 WL 3055111 (D. Ariz. May 31, 2016), *appeal dismissed*, No. 16-16141 (9th Cir. Jan. 27, 2017). The court found the policy did not cover those amounts because the third party had not suffered a "privacy injury" as the phrase was used in the policy; rather, the restaurant's customers had suffered injuries that the third-party processor had compensated and the third party had, in turn, requested that the restaurant reimburse those amounts.

In a California case, a non-profit network of hospitals suffered a breach of 32,500 confidential medical records when its third-party vendor's network failed. *Columbia Cas. Co. v. Cottage Health Sys.*, No. 2:15-cv-03432, 2015 WL 4497730 (C.D. Cal. July 17, 2015). The network was fully accessible via the internet, but the vendor failed to install encryption software or take other reasonable measures to protect the data. The hospital was sued, and its insurance company settled the claim for $4.1 million. The insurance company then sued the hospital for full recovery of the settlement, citing an exclusion in the policy barring coverage for "failure to follow minimum required practices." The court dismissed the complaint because the parties had not completed the required alternative dispute resolution process in the policy. Ultimately, the case was refiled in

state and federal court. *Cottage Health v. Columbia Cas. Co.*, No. 16CV02310 (Cal. Sup. Ct. filed May 31, 2016); *Columbia Cas. Co. v. Cottage Health*, No. 2:16-cv-3759 (filed May 31, 2016). The federal court stayed the federal case in favor of the state case. The state case is proceeding and the federal court's decision staying the federal case is on appeal.

Practice Tip:

Know what you are buying. It is important to keep in mind the particulars of the coverage afforded under your policy when providing notice and presenting your claim to the insurer. When negotiating coverage, carve back contract exclusions, and engage knowledgeable brokers and coverage counsel to help identify unfavorable policy terms.

2. Intentional and Willful Acts

A federal district court in Utah rejected an insured's claim of coverage for intentional withholding of electronic information on the ground that the policy's coverage was restricted to acts involving negligence. *Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., Inc.*, 103 F. Supp. 3d 1297 (D. Utah 2015). But the court refused to dismiss the question of whether the insurer had acted in bad faith by imposing inappropriate conditions precedent to claim initiation and failing to diligently investigate, fairly evaluate, and promptly communicate with the insured.

Practice Tip:

Consider what risks your company faces from acts that could be characterized as intentional and whether insurance can be obtained to provide coverage in those circumstances.

3. Credit Card Company Assessments and Penalties

The Hotel Monteleone, after suffering a cyberattack resulting in credit card chargeback liabilities being assessed against the hotel, brought suit against its insurer under a cyber insurance policy that insured Security and Privacy Liability up to $3 million and Payment Card Industry Fines and Penalties up to $200,000. While the hotel argued that the fines fell under the broader Security and Privacy provision, the insured asserted that it fell within the more limited Payment Card Industry Fines endorsement. The litigation has been stayed pending conclusion of mediation. *New Hotel Monteleone, LLC v. Certain Underwriters at Lloyd's of London*, No. 2:16-CV-00061 (E.D. Louisiana).

P.F. Chang's incurred more than $2 million in fees passed through to the restaurant by Bank of America; the bank incurred those charges from Mastercard after hackers obtained and disclosed 60,000 P.F. Chang's customers' credit card numbers. P.F. Chang's had agreed to reimburse the bank for fees imposed by credit card companies resulting from P.F. Chang's acts. A federal court found that P.F. Chang's insurer, Federal Insurance Company, was not obliged to cover those costs because, among other reasons, fees assumed by contract were excluded from coverage. *P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.*, No. CV-15-01322-PHX-SMM, 2016 WL 3055111 (D. Ariz. May 31, 2016), *appeal dismissed*, No. 16-16141 (9th Cir. Jan. 27, 2017).

A family-owned retail chain, Spec's Family Partners, Ltd., suffered two data breaches of its credit card payment system, which resulted in the loss of customer information, including credit card numbers. Spec's third-party credit card transaction service, First Data Merchant Services, then sent two letters to Spec's, demanding payment of millions of dollars under the indemnification obligations in the merchant agreement between First Data and Spec's. A federal court found that Spec's insurer was not obligated to provide coverage with respect to those demand letters because the letters fell within an exclusion precluding claims based upon a written contract. Spec's Family Partners, Ltd. v. Hanover Ins. Co., No. 4:16-cv-438 (S.D. Tex. Mar. 15, 2017), appeal pending, No. 17-20263 (5th Cir.).

On March 27, 2017, St. Paul Fire & Marine Insurance Co. filed a suit seeking declaratory judgment that its CGL policy did not cover fines and penalties assessed against its insured, Rosen Hotels, after hackers installed malware into the hotel's credit card payment network. The insurer asserted, among other arguments, that the fees were barred under the policy's contract liability exception, which precludes coverage for "injury or damage for which the protected person has assumed liability under any contract or agreement." According to the insurer, the insured had assumed liability for the fines under its Merchant Service Agreements with its credit card service providers. *St. Paul Fire & Marine Insurance Co. v. Rosen Millennium Inc.,* 6:17-cv-540 (M.D. Fla. 2017). The insured may have a strong argument for coverage under the exclusion's exception, which covers damages the protected person would be liable for without the contract or agreement. See *A Cyber Coverage Warning for Hospitality Insureds,* Walter Andrews, Sergio Oehninger, & Andrea DeField (April 4, 2017).

Practice Tip:

Because many cyber insurance policies have not been judicially tested, insurers will likely attempt to parse language in their favor. Carefully review the policy, ask questions during the underwriting process, and pay close attention to your policy's endorsements and any sub-limits, as they can dramatically alter the scope of coverage. If credit or debit card

breach protection does not come in your standard policy, consider asking for a "Fines and Penalties/Consumer Redress Funds/Payment Card Expenses Insuring Agreement" endorsement. Regardless, to evaluate the propriety of any denial of coverage, review your policy and any applicable case law closely.

B. Traditional Policies

In some circumstances, policyholders can seek coverage for cyber-related losses under traditional insurance policies like general liability policies, errors and omissions policies, crime policies, and property policies. Newer general liability policies tend to include exclusions that may preclude coverage for cyber-related losses.

Practice Tip:

Even when coverage is questionable, businesses should submit cyber insurance claims, especially since significant harm can occur shortly following a data breach.

When seeking coverage under those policies, insureds may run into some of the issues identified below.

1. Publication

Under traditional insurance policies, one coverage issue that can arise with respect to data breaches related to individuals' personal identifying information is whether that information constitutes a "publication" as that word is used in many general liability policies. The decisions thus far have been highly fact-dependent:

- A federal appellate court upheld a federal district court's decision finding a publication of private medical records where those records were accessible on the internet through a simple Google search, even though there was no evidence that any third party in fact accessed the records. *Travelers Indem. Co. of Am. v. Portal Healthcare Sols., LLC*, 644 F. App'x 245 (4th Cir. 2016); see also Syed A. Ahmad, Sergio F. Oehninger & Patrick M. McDermott, *If Information Is Available Online and No One Accesses It, Was It a 'Publication' for the Purpose of Insurance Coverage for Cyber security Loss?*, Privacy and Security Law Report, Bloomberg BNA, May 9, 2016.
- A New York state court found no publication because the policyholder had not published the information. Rather, a third-party hacker published the stolen information. According to that court, the policy did not cover publications by a third

party (as opposed to the policyholder). *Zurich Am. Ins. Co. v. Sony Corp. of Am.*, No. 651982/2011, 2014 WL 3253541 (N.Y. Sup. Ct. Feb. 24, 2014), appeal withdrawn, 127 A.D.3d 662 (N.Y. App. Div. 2015).

- A Connecticut court found that there was no "publication" where there was no suggestion that private identifying information of current and former employees on lost computer tapes "was ever accessed by anyone." *Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 83 A.3d 664, 673 (Conn. App. Ct. 2014), aff'd, 115 A.3d 458 (Conn. 2015).

Practice Tip:

Do not assume that general liability policies do not cover all or some aspect of losses or damages arising from a cyber event in which PII, confidential business information, or other private information is disclosed.

2. Loss of or Damage to Code

When loss of or damage to computer code occurs, an issue that often arises is whether it constitutes property damage or physical loss or damage as typically required to trigger coverage under both general liability and first-party coverages (like property insurance). Courts have gone both ways on this issue:

- A federal appellate court found that erasing of data was "direct physical loss" covered under property policy. *NMS Servs., Inc. v. Hartford*, 62 F. App'x 511 (4th Cir. 2003).
- A Texas state appellate court found that the loss of code was "physical loss." *Lambrecht & Assocs., Inc. v. State Farm Lloyds*, 119 S.W.3d 16 (Tex. Ct. App. 2003).
- A federal district court found that a company's lost ability to use full capacity of its servers constituted tangible property loss. *Vonage Holdings Corp. v. Hartford Fire Ins. Co.*, No. 11-6187, 2012 U.S. Dist. LEXIS 44401, at *9 (D.N.J. Mar. 28, 2012). A Minnesota state appellate court found that computer tapes and data were tangible property under a general liability policy. *Retail Systems, Inc. v. CNA Ins. Cos.*, 469 N.W.2d 735 (Minn. Ct. App. 1991).
- An Oklahoma federal district court found that loss of computer data was intangible property under the relevant policy. *Contra State Auto Property & Casualty Ins. Co. v. Midwest Computers & More*, 147 E Supp. 2d 1113, 1116 (W.D. Okla. 2001).
- A federal court in Arizona found that a computer outage resulting from loss of programming information constituted "physical loss or damage." *Am. Guarantee & Liability Ins. Co. v. Ingram Micro, Inc.*, 2000 WL 726789 (D. Ariz. Apr. 18, 2000).
- However, a federal appellate court has found that a software upgrade that caused computer crashes did not constitute a physical loss to tangible property. *Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89 (4th Cir. 2003).

- A federal district court held that there was no coverage for third-party claims following a point-of-sale attack where the underlying plaintiffs (credit unions) did not allege "property damage" to affected debit cards, but rather harm to "intangible" data on the cards, which was not covered by the policy. *Camp's Grocery, Inc. v. State Farm Fire & Cas. Co.*, No. 4:16-cv-0204-JEO, 2016 WL 6217161 (N.D. Ala. Oct. 25, 2016).

Practice Tip:

When hardware or data is physically damaged or lost, consider general liability insurance and property insurance as potential sources of recovery. Also, ensure that your cyber security programs include adequate first- and third-party coverages.

3. Loss of Use of Computer Systems

Courts have also evaluated whether loss of use of computer systems or data is property damage or physical loss or damage. Again, courts have come to both conclusions:

- A federal appellate court found that computer freezes, pop-up ads and a hijacked browser constituted "property damage" where that phrase was defined to include loss of use of property. *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797 (8th Cir. 2010).
- Another federal appellate court found that underlying claims that a software upgrade caused computer crashes were not covered under the "loss of use" portion of the policy because the court had found that no property had been physically damaged, which was a requirement for the loss of use coverage to apply. *Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89 (4th Cir. 2003).

4. Crime Coverage

Cyber-related events can involve criminal acts and, therefore, may trigger coverage under crime insurance policies.

- A federal appellate court has found millions of dollars of coverage for a data breach under a crime policy. *Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.*, 691 F.3d 821 (6th Cir. 2012).
- Another federal appellate court affirmed a district court's decision finding coverage for a hacking incident under a financial institution bond, which is similar to a crime insurance policy. *State Bank of Bellingham v. BancInsure, Inc.*, 823 F.3d 456 (8th Cir. 2016). The court rejected the insurer's arguments that there was no coverage

because of an employee's negligence in mistakenly leaving one of three security measures disabled and computers running overnight.

- Another federal appellate court found no computer fraud coverage where, according to the court, there was no unauthorized transfer of funds, because the person making the transfer was authorized to do so, even if that person was fraudulently induced to make the transfer. *Pestmaster Servs. Inc. v. Travelers Cas. & Sur. Co. of Am.*, 656 F. App'x 332 (9th Cir. 2016).
- New York's highest court found that coverage for "fraudulent entry of . . . Electronic Data or Computer Program" referred to "unauthorized access into plaintiff's computer system, and not to content submitted by authorized users," and therefore found no coverage for $18 million in payments for fraudulent Medicare claims submitted for services that were never performed. *Universal Am. Corp. v. Nat'l Union Fire Ins. Co.* of Pittsburgh, Pa., 37 N.E.3d 78 (N.Y. 2015).
- Recently, numerous cases have involved insureds seeking coverage for losses resulting from social engineering schemes. The typical scheme involves an email from a high-level executive's email account directing a subordinate employee to wire funds to a bank account actually owned by a third-party scammer, the true author of the email.
- A federal district court found no coverage under a crime policy for a manufacturer's $800,000 loss, reasoning that the fraudulent email that prompted wire transfers to fraudsters did not "directly" cause the transfer given intervening the events of production milestones, authorization of the transfers, and initiating the transfers without verifying bank information. *Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., No. 5:16-cv-12108, 2017 BL 267253 (E.D. Mich. Aug. 1, 2017)*.
- A federal district court found coverage under a crime policy for a cloud-based service provider's loss of $4.8 million resulting from an employee being deceived into transferring as a result of an email made to look like it was from the company's president when it was actually from an unidentified third party. *Medidata Sols. Inc. v. Fed. Ins. Co.*, No. 15-cv-907 (ALC) (S.D.N.Y. July 21, 2017). The court concluded that the policy's computer fraud provision and funds transfer fraud provision covered the loss.
- A federal district court found coverage under the computer and funds transfer fraud provision of a commercial crime policy for an IT company's loss resulting from an employee's receipt of an email from an individual posing as an executive of the IT company. *Principle Sols. Grp. LLC v. Ironshore Indem. Inc.*, No. 1:15-CV-4130-RWS, 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016).
- However, a federal appellate court found that a crime policy did not cover a loss under a computer-fraud provision where the loss was precipitated by a multi-faceted scheme (including telephone calls, letters, and emails) and the court concluded that the false email was a mere "incidental" part of the scheme and did not "directly" cause the loss. *Apache Corp. v. Great Am. Ins. Co.*, 662 F. App'x 252 (5th Cir. 2016).

- A federal district court found no coverage for a $700,000 loss resulting from hackers who, while posing as employees, directed other employees to change account information for a customer. *Aqua Star (USA) Corp. v. Travelers Cas. & Surety Co. of Am.*, No. C14-1368RSL, 2016 WL 3655265 (W.D. Wash. July 8, 2016), appeal docketed, No. 16-35614 (9th Cir. Aug. 1, 2016). In that case, the court found that an exclusion providing that the policy "will not apply to loss resulting directly or indirectly from the input of Electronic data by a natural person having the authority to enter the Insured's Computer System" applied and barred coverage.
- Another federal district court found no coverage for loss resulting from a hacker posing as a client of the insured and sending emails to the insured directing the insured to transfer money to foreign banks. *Taylor & Lieberman v. Fed. Ins. Co.*, No. CV 14-3608 RSWL (SHx), 2015 WL 3824130 (C.D. Cal. June 18, 2015), aff'd, No. 15-56102 (9th Cir. July 17, 2015). The court decided that the insured had not suffered any "direct loss" as required by the policy because the fraudulent emails "did not immediately and without intervening cause result in a loss."

Practice Tip:

After suffering a loss resulting from a third party's malicious actions, including phishing attacks and social engineering schemes, consider coverage available under crime insurance policies and cyber insurance policies.

- *For additional cases, see Bloomberg Law: Privacy & Data Security.*

VI. Prevention – Best Business Practices for Cyber Security

A strong cyber insurance coverage program should be paired in the first instance with a proactive approach to your company's cyber security. Consider taking forward-thinking steps like the ones below to maximize cyber and data security.

- Reevaluate your firm's Information Governance techniques. Work with your Chief Information Security Officer (CISO) or equivalent to "see the big picture" and gain a better understanding of how data moves between departments. Use this data to pinpoint weak points in the firm's digital infrastructure.
- Seek counsel to ensure that the organization's risk and compliance frameworks remain in accordance with differing legislations across international jurisdictions. Specifically, ask about updates on federal data breach laws and also be cognizant of relevant state statutory schemes, like New York's heightened cyber security regulations.
- Remain conscious of both federal and state reporting requirements for data breach. Consult with a lawyer to analyze the firm's responsibilities post-breach.
- Be aware that hacking is often due to the breakdown of basic employee diligence. Administer regular comprehensive employee training in cyber security and privacy. Focus particularly on email security, password protection, and social engineering schemes. Require acknowledgment and provide readily available expert support for employee questions. Consider random tests of employee diligence through mock phishing attacks or social engineering schemes. Finally, emphasize that employee diligence is the foundation of the firm's information security program.
- Design a Written Information Security Program (WISP) to outline the firm's security policies, safeguards, risk assessments, and monitoring techniques.
- Maximize your return on investment (ROI) by focusing first on your organization's most critical risks. Due to the increasingly complex nature of cyber security threat vectors, most, if not all, organizations will be breached by a cyberattack. Limit the financial and reputational impact of future breaches by prioritizing time and investment toward the weakest links in the chain.
- Invest generously in a robust internet security system, a secure email blocking and encryption service, and the latest security software updates.
- Create a data incident response plan. Conduct consistent testing to identify issues with the plan's administration. Make sure it addresses the latest threats to not only confidentiality, but also the availability and integrity of data; i.e., not just theft of your data, but control of your systems.
- Thoroughly evaluate data protection risks and liabilities in the early stages of any merger and acquisition transaction to ensure that the combined entity does not become susceptible to cyberattack.

VII. Glossary of Key Terms for Cyber-Related Insurance Issues

Business Interruption Loss (in cyber context) – loss and expenses incurred as a result of a cyber event; often includes lost profit; loss typically covered by business interruption insurance.

Claim – (1) a request to the insurer that the insurer pay under the policy; (2) an event that can trigger coverage under an insurance policy; can be defined as a written demand for money damages or other relief.

Claims-Made Policy – a type of insurance policy that generally covers only claims that are made during the policy period.

Contingent Business Interruption (CBI) Loss (in cyber context) – lost profits and extra expenses resulting from an interruption of business at the premises of a customer or supplier resulting from a cyber event. In the cyber insurance context, CBI insurance typically pays for loss of income sustained by the insured resulting from damage caused by a covered peril to the premises of another organization on which the insured depends, such as a key supplier, customer, vendor, or other supply-chain business partner.

Coverage Territory – a specific geographic region in which accidents or events must take place to trigger insurance coverage.

Cyber – an admittedly amorphous term, which generally is used to mean of or relating to computers or computer networks (Merriam-Webster).

Cyber Risk – "any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks." See 2016 Cyber Insurance Buying Guide, American Bankers Associate & Financial Services Sector Coordinating Council.

Cyber-Threat – the possibility of a malicious attempt to damage or disrupt a computer network or system; an event, condition, or consequence that produces adverse effects or undesired results to a computer network or system.

Data – the quantities, characters, or symbols on which operations are performed by a computer, which may be stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media (Oxford).

Deductible – an amount of each claim for which the policyholder is responsible. c.f. retention.

Denial of Service – preventing authentic users from accessing information or services; for example, a denial of service attack can prevent a user from accessing email or online banking websites.

Directors and Officers Coverage – generally speaking, coverage designed to protect against losses and expenses related to certain claims against directors and officers and their company.

Errors and Omissions Coverage – generally speaking, covers losses and expenses incurred in connection with claims arising out of alleged professional failures.

Excess Policy – insurance policies that apply after the limits of other identified policies are paid.

Exclusion – a provision in an insurance policy that excludes or prohibits coverage for certain events or in certain circumstances.

First-Party Coverage – coverage designed to compensate for damages to the policyholder's own property.

Information Security – the practice of preventing unauthorized access to and use of information, particularly electronic data.

Insurer – the insurance company that issues the insurance policy.

Internet of Things – refers to the concept of connecting physical items to the internet, including everyday items like refrigerators, cars, etc.

Limit – the amount of money a policy will pay for covered losses.

Malware – any malicious software that disables or interrupts use of a computer system.

Media Liability Coverage – generally speaking, covers losses arising out of the use of electronic media.

Network Security Coverage – generally speaking, covers losses and expenses arising out of failures or breaches of the company's network security, such as hackings or virus transmission.

Occurrence-Based Policy – a policy that covers certain events that take place during the policy period regardless of when a claim is made.

PCI Data Security Standards (PCI DSS) – a set of comprehensive requirements for enhancing payment account data security. They apply to all companies receiving payment by credit card and form industry best practices for any entity that stores, processes, or transmits cardholder data. Business violating the PCI DSS risks substantial fines for data compromise and security breaches, as well as fees associated with non-compliance.

Personally Identifiable Information (PII) – any data or information that could be used to identify a specific person or that could be used to differentiate between individuals; according to the National Institute of Standards and Technology, PII includes names, addresses, email addresses, pictures, fingerprints, handwriting, date of birth, place of birth, race, religion, weight, employment information, medical information, education information, Social Security numbers, passport numbers, driver's license numbers, taxpayer ID numbers, financial account numbers, and credit card numbers.

Phishing Attack – refers to an illegitimate email message often sent to broad, non-targeted groups to collect personal information for malicious purposes or to gain improper access to private networks; the email is usually disguised to appear a legitimate email to encourage recipients to clink on a link or open an attachment containing something like a virus or malware.

Policy – the contract identifying the insurance coverage provided.

Policyholder – the company or individual that purchases an insurance policy and that is generally named in the policy; also known as the insured.

Premium – the amount paid to purchase insurance.

Primary Policy – the insurance policy that is the first to apply to a loss.

Privacy Coverage – covers electronic disclosure of confidential information, including personally identifiable information and personal health information.

Ransomware – malicious software intended to prevent use of a computer system until a ransom is paid.

Reservation of Rights – an insurer's statement that it may deny coverage at a later time.

Retention – an amount that must be paid before the insurer pays. c.f. deductible.

Retroactive Date – in a claims-made policy, this is the date after which an event leading to a claim must occur; if an event occurs before this date, the policy will not provide coverage, even if the claim is made during the policy period.

Risk – a relative value produced by the analysis of probability and resulting impact of a threat occurring or being realized or accomplished.

Social Engineering – a cyber-threat vector that uses deception to manipulate individuals into breaking normal security procedures or divulging personal or confidential information.

Social Networking Sites – web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.

Spear Phishing – the practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information; an email or electronic communications scam targeted toward a specific individual, organization or business, which may be used by cyber criminals to steal data for malicious purposes or to install malware on a targeted user's computer.

Sub-Limit – a limit that applies to a specific coverage, like coverage for losses related to cloud computing.

Third-Party Coverage – coverage designed to compensate for damages to property other than the policyholder's.

Threat Actor – individuals or groups that target people or organizations with a motivation; they can be internal or external to a target and known or unknown.

Threat Targets – anything of value to the threat actors, such as bank accounts, PII, confidential business information, trade secrets, computers, mobile phones, or computing devices.

Threat Vector – a tool or a path that a threat actor uses to attack the target.

Trigger – the process by which it is determined whether an insurance policy applies to a particular event or loss.

Unauthorized Access – gaining access to a network or data using someone else's username and password or otherwise without authorization.

Whaling – a type of social engineering scheme in which a hacker poses as a senior executive.