ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Planning for Disasters

Insurance

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***The property policy.*** The typical property policy covers damage from fire, windstorms, hail, civil unrest, and explosions. However, flooding is typically excluded under these policies.
- ***Business interrupted.*** There are two key components to business interruption planning: (1) devise a business plan to minimize the interruption of your company's business in the aftermath of a natural or man-made disaster, and (2) insure against those things you cannot avoid.
- ***The digital age.*** As a first line of defense against cyberattacks and ransomware, consider how your company will react to several of the most likely threats and seek to insure against those risks.
- ***Currently unattainable.*** Insurance may not cover lost customer data as a result of a data breach. In-house counsel should carefully review company policy to understand the parameters of coverage for loss of data — particularly another person's data that may be in your care, custody, or control.

Your company strives to grow its businesses and operate efficiently. However, focusing on growth and continued operations is not enough. You must also evaluate the potential impact of a natural or man-made disaster that disrupts your supply chain, hijacks your computer system, or temporarily closes your business. These disasters may take the form of hurricanes, floods, fires, and cyberattacks. Whatever the form, disaster will strike your company. Are you ready for it?

This article will offer insight into some of the potential disasters that your company may face, how to plan for them, and how you may be able to insure against a crisis caused by external forces. In addition to disaster planning, your company, if it is a public company, has obligations to disclose cybersecurity risks and incidents. Failure to plan or disclose can create liabilities for directors and officers. Those duties and exposures are discussed below.

A myriad of risks

This decade alone has illustrated the diversity of events that can cripple a company, either temporarily or permanently. In addition to "old school risks" such as hurricanes, floods, earthquakes, and fires, companies now face risks from "cryptoworms" used for ransomware attacks, such as the 2017 worldwide "WannaCry" cyberattack. In that instance, criminals hijacked computer systems of companies large and small, encrypted the company's data, and demanded ransom payments for the release of the company's own data. Other potential cyberdisasters include data breaches, such as those suffered by Sony and HBO, and the theft of credit card and personally identifiable information from almost every merchant from Target to Wendy's and almost every financial institution you can think of.

During the 2011 earthquake off the coast of Japan, the resulting tsunamis and nuclear plant meltdown led to long-term devastation across the region. Dubbed the "triple calamities" by *Japan Times* reporter Roger Pulver, those events, along with government-ordered evacuations (the fourth calamity for insurance coverage purposes) had far-reaching economic effects. Insurance companies

far from Japan were on the hook for some of the lost profits experienced by manufacturers whose supply chains were disrupted by the devastating earthquake.

In May 2017, the National Oceanic and Atmospheric Administration (NOAA) forecasted a 45 percent chance for an above-normal hurricane season in 2017, predicting that there was a 70 percent chance of having 11 to 17 named storms, of which five to nine could develop into hurricanes, including two to four major hurricanes (categories three to five). Three months later, NOAA raised its forecast prediction to 14 to 19 named tropical systems and increased its prediction to as many as five major hurricanes.

In the process of drafting this article, Hurricane Harvey devastated many of the residents and businesses of south Texas and the gulf coast. The impact was felt hundreds and thousands of miles away because of the chain reaction of losses caused by the virtual shutdown of the economy in that part of the United States. At the time of the publication of this article, many businesses may still be suffering losses of one type or another that can be traced back to Harvey. Following production of this article, two more hurricanes caused great destruction to the United States — Hurricane Irma in Florida and Hurricane Maria in Puerto Rico.

It will take years for insurance carriers and policyholders to sort out the covered losses caused by the hurricanes from those losses that were not insured. In the meantime, the key to properly assessing your company's catastrophe coverage is to carefully review all coverage grants, compare them against all exclusions, and then carefully apply the coverages and exclusions to your losses since Aug. 25, 2017. It is important to preserve all accounting records, inspection findings, and other evidence such as photographs, videos, media accounts, eye witness accounts, contractor's reports, and engineer's opinions, until your claims are ultimately resolved.

The typical property policy covers damage from fire, windstorms, hail, civil unrest, and explosions. Most businesses affected should look to their first-party insurance policies. Those commercial property insurance policies contain three basic types of coverage that may apply:

- Property damage coverage for physical loss or damage to business property.
- Business income coverage for the policyholder's loss of profit and certain unavoidable continuing expenses.
- Extra expense coverage for both the policyholder's costs in minimizing or avoiding a business income loss and those costs the policyholder would not have incurred but for the covered loss.

Unfortunately, flood is typically excluded under property policies. If available, flood insurance provides the most immediate and obvious coverage for destruction of the type caused by hurricanes. But there are significant limits to that coverage. Without getting too far into the details, flood coverage is underwritten by the US federal government. There are various statutory parameters controlling the terms and conditions of the Standard Flood Insurance Policy (SFIP). The SFIP Insuring Agreement states: "We will pay you for direct physical loss by or from flood to your insured property." The National Flood Insurance Program (NFIP)'s General Property Form offers commercial policyholders coverage for (a) Building Property up to US$500,000 and (b) Personal Property up to US$500,000.

A flood policy is not a cure-all and is not a substitute for a property policy. For example, the SFIP excludes loss of revenue or profits, loss of use, and loss from interruption of business or production. Companies should look to their property policies for such coverage.

Contingent Business Interruption (CBI) coverage may come into play for companies that did not suffer direct physical damage but were otherwise impacted by Harvey if, for example, their supply chain was disrupted. Similarly, businesses can look to contingent extra expense coverage to pay for increased costs caused by Harvey to offset some income losses.

Affected businesses should also look to service interruption coverage, which is designed to provide coverage for business income losses attributable to the interruption of utility or telecommunications service. Income losses from such outages may be covered under your company's property insurance policy. As with contingent extra expenses, a policyholder's expense in minimizing the loss caused by service interruption should be covered. For instance, the policy may cover the purchase of cell phones for employees to use while the company's phone service is out of order.

Catastrophes, by definition, cause widespread damage. They also typically cause damage by a variety of mechanisms, as illustrated by the wind, flood, and storm surge damage caused by hurricanes Katrina (2005), Ike (2008), and Harvey (2017). Harvey's impact is more widespread and the resulting losses are sure to make it one of the top three costliest US disasters (along with Katrina and Superstorm Sandy (2012).

Business interruption planning

There are two key components to business interruption planning. The first is devising a business plan to minimize the interruption of your company's business in the aftermath of a natural or man-made disaster. The second is to insure against those things you cannot avoid.

A business interruption plan should identify the most critical business functions to preserve or restore. Company leaders must consider the critical and time-sensitive functions necessary to stay in business, prioritize those functions, and determine the amount of downtime that is acceptable. The prioritization may depend on which business functions are needed to fulfill legal obligations, maintain cash flow, secure market share, and preserve the company's reputation. A company should perform a business impact analysis to analyze the consequences of different types of disasters. Once key business functions are identified and prioritized, the business interruption plan should document the physical and human resources necessary to restore the most critical business functions.

Your insurance plan must include coverage for the disruption and interruption of your business following a disaster. The interdependency of companies within the vertical supply chain, the growth of outsourcing, and reliance on just-in-time inventories all increase the risk of loss if one company in the modern web of commerce falters. For example, if a supplier is shut down because of a natural disaster and fails to supply goods or services required, revenues of the buyer might be seriously affected. CBI coverage can mitigate that damage.

> A company should perform a business impact analysis to analyze the consequences of different types of disasters. Once key business functions are identified and prioritized, the business interruption plan should document the physical and human resources necessary to restore the most critical business functions.

Business Interruption (BI) insurance protects against the loss of prospective earnings because of the interruption of the policyholder's business caused by an insured peril to the policyholder's own property. With BI coverage, you can recover some or all of your lost earnings if your insured factory is destroyed by fire, for example. CBI coverage is a close cousin of BI coverage, and protects the

policyholder against the loss of prospective earnings caused by an insured peril to someone else's property. With CBI coverage, you can recover some or all of your lost earnings if your key supplier's factory is damaged by a covered peril.

However, insurance is only one component of a comprehensive business interruption plan. Insurance may provide coverage for lost income suffered during the specific period of restoration, but restoring business operations quickly reduces long-term effects that insurance cannot cover, such as minimizing the loss of customers and contracts.

Therefore, a business interruption plan will help mitigate covered and non-covered aspects of the loss. Every company should have a detailed plan to resume partial operations or re-open as quickly as possible, and to preserve the documentation necessary to present a business interruption claim. Many sophisticated insurance brokers and insurers can help formulate these plans.

Insurance coverage for "old school risk"

Business interruption coverage

Given the business necessity of BI and CBI coverage, corporate counsel must (in the imperative sense) know their company's coverages before disaster strikes. You don't want to lose your main supplier and then only learn that your policy has restrictive BI/CBI terms or relatively small sub-limits. Again, know your coverage before you need it.

Most commercial property insurance policies provide some coverage for business income loss by adding an endorsement to the insured's property policy. This endorsement is designed to protect the insured for losses of business income that it sustains as a result of direct loss, damage, or destruction to insured property by a covered peril.

This coverage reimburses the actual loss sustained by the insured as a result of direct physical loss or damage to the insured's property by a covered peril. Of course, the insured must actually sustain an interruption of business that causes a business income loss. Even so, the insurer's obligation is limited to the dollar amount of loss actually sustained, but not to exceed the applicable policy limit. "Business income" usually includes the net income (net profit or loss before income taxes) that would have been earned or incurred by the insured and the continuing normal operating expenses incurred, including payroll. However, the coverage is limited to the "period of restoration." The period of restoration begins when the physical loss or damage occurs, and ends when the property should, with reasonable speed, be repaired or replaced.

Since business interruption coverage is limited to a reasonable period of restoration, delay in the restoration process could result in a period of business interruption for which no insurance coverage applies. Further, if a policy provides coverage for expedited repairs, then it may reduce the reasonable restoration period if the business fails to expedite repairs. Under the policy, the business may be required to mitigate its losses by resuming partial operations in a temporary facility or by using an undamaged portion of the business. The type of business and core business functions will drive what is necessary to resume partial operations. A manufacturing facility may be able to maintain production levels by adding shifts. A business that relies on face-to-face interactions may be able to reschedule appointments. Some policies provide coverage for extra expenses incurred, such as extra rent. However, the extra expense coverage available may be limited.

Contingent business interruption coverage

CBI coverage will generally reimburse a policyholder for its expenses and lost profits when it cannot operate because a disaster struck a supplier. However, the supply disruption has to be caused by a covered peril or, conversely, the disruption cannot be caused by an excluded peril. Calamities that are often not covered include disruptions due to earthquakes, floods, or nuclear contamination. For example, if a Japanese company cannot operate because it has been contaminated by the fallout from the damaged Fukushima nuclear plant, its customers probably cannot tap into their own CBI coverage.

As with virtually all other insurance provisions, the policy language for CBI coverage will vary from contract to contract. The ISO "Business Income from Dependent Properties — Broad Form" provides:

> "We will pay for the actual loss of Business Income you sustain due to the necessary suspension of your 'operations' during the 'period of restoration.' The suspension must be caused by the direct physical loss or damage to 'dependent property' at premises described in the Schedule caused by or resulting from a Covered Cause of Loss …."

"Dependent property" is generally defined as property operated by others upon whom the policyholder depends to:

- Deliver materials or services to the policyholder;
- Accept products or services from the policyholder;
- Manufacture products for delivery to the policyholder's customers under contracts of sale; or,
- Attract customers to the policyholder business.

The so-called "dependent" property may be specifically named or the coverage may apply as blanket coverage to all customers and suppliers of the insured.

CBI coverage is usually triggered by the physical damage to customers' or suppliers' property or to the property on which the policyholder depends to attract customers. The type of physical damage must be caused by a peril that is covered under the commercial property insurance policy. Conversely, the peril must not be specifically excluded. For example, CBI coverage may exclude loss that results from the following: Utility service interruption or an off-premises power interruption; change in temperature due to damage to heating or cooling equipment; actions by civil or military authority; lack of ingress or egress; or downstream business interruption when damage at an owned location causes a loss of revenue to another owned location. But note: There may be separate coverage under the commercial property policy for some of those losses.

CBI coverage typically has a "time deductible" in that the "period of restoration" begins a specified number of hours after the time of direct physical loss or damage resulting from any covered cause of loss at the premises of the dependent property.

CBI coverage is generally an included provision contained in most large commercial property policies. However, this included CBI coverage will have a very small sub-limit. For example, if the limit for the commercial property policy is US$25 million, the CBI sub-limit may be as low as US$100,000.

In order to obtain more robust CBI coverage (i.e., higher limits and broader terms), the carrier will

typically want the policyholder to identify the specific supplier, recipient, and leader properties that are crucial to the policyholder's business. The carrier will then specifically underwrite for those third-party properties. So, for example, if the policyholder has an important supplier in Japan, the carrier will actually underwrite for that specific Japanese company and location. It may then exclude certain specific perils it deems too risky. One such peril often excluded by carriers is the risk of earthquake in Japan. That makes obtaining CBI coverage for American high-tech companies that rely on Japanese manufacturers for goods, such as the resins needed for computer chips, very challenging and very expensive if available.

What can go wrong in the digital age? Cyber threats, data breaches, and privacy invasion

In the past, generally before 2006, the main cyber threats were from "activists" looking to take websites offline. Now, hackers seek business disruption and extortion. In addition, there is now a thriving black market for credit card numbers, personally identifiable information, and other such data with sophisticated criminal networks and even state actors peddling this information. Moreover, cyberterrorism by state actors and terrorists is here to stay. Of course, that type of cyberterrorism implicates policy exclusions.

Currently, it seems that both the frequency and severity escalate month-to-month. In 2011, there were less than 60 cyber cases exposing more than one million records and only a handful of ransom attacks. In 2016, there were more than 120 significant ransom attacks and about 60 cyber cases exposing more than one million records.

Every company that uses technology in its operations or handles, collects, and stores confidential information has cyber risk. Your company presently faces:

- Legal liability to others for privacy breaches of confidential information;
- Regulatory actions, fines, and scrutiny;
- Cyberextortion;
- Data kidnapping;
- Cyberterrorism and espionage
- Loss or damage to data/information;
- Loss of revenue due to a computer attack;
- Extra expense to recover/respond to a computer attack; and,
- Loss or damage to reputation following a hack.

If that list concerns you — and it should — you also need to worry because a cyber event can disrupt your supply chain and cause damage. Think about what would happen to your company if there was a cyberattack on internet providers, cloud storage facilities, or power grids. That is the most significant risk for supply-chain disruption, followed by a natural disaster such as a hurricane, earthquake, or flood.

> In 2011, there were less than 60 cyber cases exposing more than one million records and only a handful of ransom attacks. In 2016, there were more than 120 significant ransom attacks and about 60 cyber cases exposing more than one million records.

Several possible scenarios exist:

- A virus infecting the systems of a key supplier destroys essential records, forcing the supplier to shut down systems for several days. Once systems are restored, customers must resubmit their orders, causing further delays.
- An attack on a large commodities exchange interrupts the flow of essential materials resulting in price volatility in markets.
- A malicious attack on a shipper disrupts freight management and logistic systems, resulting in delays in shipments.

In fact, these possible scenarios are becoming frequent realities as discussed in an AP News headline from August 9, 2017:

> Take down: Hackers looking to shut down factories for pay.
>
> DURHAM, NC (AP) — The malware entered the North Carolina transmission plant's computer network via email last August, just as the criminals wanted, spreading like a virus and threatening to lock up the production line until the company paid a ransom. AW North Carolina stood to lose US$270,000 in revenue, plus wages for idled employees, for every hour the factory wasn't shipping its crucial auto parts to nine Toyota car and truck plants across North America, said John Peterson, the plant's information technology manager.

Not only would that event cause losses to AW North Carolina, but it could cause losses for other Toyota suppliers, Toyota dealers, and even Toyota itself.

Planning and protection in the digital age

Now that you are worried, do something. As a first line of defense, consider the following: (1) plan out how your company will react to several of the most likely threats; and (2) seek to insure against those risks.

The risk committee

Your board of directors has a lot to do: The big jobs of strategy and management oversight — not to mention compliance — will not take care of themselves. For many companies, it seems that the risk management role of the board is an ever-expanding one. How can a board handle risk management oversight more effectively?

The answer may be the formation of a board-level risk committee. Certainly, the buzz amongst corporate governance experts is growing when it comes to the idea of adding a risk management or risk oversight committee to the normal big three (the compensation committee, the corporate governance and nominating committee, and the audit committee).

Of course, the responsibility for enterprise risk management oversight belongs to the entire board. To the extent a board committee would be charged with taking the lead on this task, the charge has traditionally fallen on the audit committee — which means the audit committee has been saddled with yet another difficult responsibility.

Deloitte, in its recently released paper "As Risks Rise, Boards Respond: A Global View of Risk Committees," reported on its examination of the existence of board-level risk committees at the 400

largest public companies (across eight countries). Unsurprisingly, financial services companies were the most likely to have either pure or hybrid board-level risk committees, consistent with the extra level of regulatory scrutiny imposed on financial services companies in many countries.

Only 11 percent of the global non-financial services companies examined by Deloitte, however, had board-level, stand-alone risk committees. When adding to the mix hybrid board-level risk committees, this number jumps to only 26 percent. A “hybrid committee,” as used in the report, includes a committee that combines risk with another function (e.g., an audit and risk committee). Notwithstanding the high degree of regulation and scrutiny US public companies are under, only two percent of US non-financial services companies examined by Deloitte had board-level risk or risk hybrid committees.

This low percentage feels especially surprising given that the Securities and Exchange Commission (SEC) issued new disclosure requirements in 2009 for all public companies concerning the board’s role in enterprise risk oversight.

Then again, perhaps this low percentage is not surprising in a world where past board-level risk committees have failed to avert catastrophic outcomes. After all, some of the prominent US financial institutions that suffered dire consequences in the financial crisis of 2008 had board-level risk committees.

Cybersecurity disclosures

It’s 2017 and at this point everyone understands that cybersecurity is a board-level issue that needs to be to be addressed proactively. However, even as far back as 2011, fresh off the heels of a massive data breach involving Wyndham, the SEC reminded public companies of their obligation to disclose cyber issues to investors in a timely manner.

That’s when the SEC released its guidance on disclosing cybersecurity risks and incidents. While not a rule or regulation, the SEC offered its view on how public companies should handle such disclosures in various scenarios.

The SEC had not previously brought a case against a company or its directors and officers for cyber disclosure failures. Some believe that the SEC has been waiting for an enforcement opportunity to show how the guidance should be interpreted and implemented.

Enter Yahoo. In January 2017, reports came out that the SEC was investigating Yahoo for not promptly disclosing the significant data breach it suffered in 2014. According to media reports, disclosures about these breaches were only made in 2016 — after the planned sale of the company to Verizon Communications was announced.

Yahoo also finds itself in the midst of class-action lawsuits from both consumers and shareholders alike for negligence and other claims as a result of the data breach disclosures. Further, in its November 2016 quarterly report on form 10-Q, Yahoo disclosed that “the Company is cooperating with federal, state, and foreign governmental officials and agencies seeking information and/or documents about the Security Incident and related matters, including the US Federal Trade Commission, the US Securities and Exchange Commission, a number of State Attorneys General, and the US Attorney’s office for the Southern District of New York.”

From an insurance perspective, the lawsuits brought against Yahoo directors and officers look like

something that would fall within a D&O insurance policy as a classically covered claim. There's no reason to think that D&O insurance would fail to respond just because the underlying issue relates to a cyberbreach.

> While it's not possible to speculate on the outcome of the SEC investigation into Yahoo in an informed way, the fact remains that this investigation is a timely reminder for all public company directors and officers that this is an area of disclosure that the agency takes seriously.

On the other hand, government investigations of corporate entities are not automatically covered by a technology company's D&O insurance policy. In the current insurance market, however, there are some insurance products that would respond.

The private plaintiff litigation from shareholders isn't a surprise outcome. On the seriousness scale, however, private plaintiff litigation takes a back seat to investigations by government entities like the SEC.

While it's not possible to speculate on the outcome of the SEC investigation into Yahoo in an informed way, the fact remains that this investigation is a timely reminder for all public company directors and officers that this is an area of disclosure that the agency takes seriously.

As a result of its investigation, the SEC may issue additional interpretive guidance for cyber disclosures, like it has done in the past with things like non-GAAP financials.

Some companies aren't waiting to enhance their cyber disclosures. For example, according to the *Wall Street Journal*, 17 companies disclosed breaches to the SEC in 2016. On the other hand, it seems likely that more than 17 companies had breaches in 2016.

From the *Wall Street Journal*:

> Many hesitate to do so, because offering too much or too little information to investors can hurt companies. On the one hand, investors may feel management or boards tried to hide a problem or failed to disclose a breach in a timely way. On the other, too much disclosure could cause investors to bid down a company's stock price, even if a later investigation reveals little impact on the business, according to experts.

Although some companies may feel hesitant to be aggressive when it comes to cybersecurity disclosures, the Yahoo investigation tells us that the stakes are high if you find yourself with a significant data breach on your hands and the SEC decides the disclosure to investors was not timely enough.

Cyber coverage overview

According to Insurance Information Institute, insurers are issuing an increasing number of cyber insurance policies and becoming more skilled and experienced at underwriting and pricing this rapidly evolving risk. More than 60 carriers now offer stand-alone cyber insurance policies, and it is estimated the US market is worth more than US$3.25 billion in gross written premiums in 2016, with some estimates suggesting it has the potential to grow to US$7.5 billion.

Cyber insurance is generally available today. Various carriers offer insurance covering risks ranging from privacy liability, extortion (ransom) threats, crisis management, damage to data, programs, software, funds transfer fraud, derivative shareholder litigation, and business interruption. These policies or endorsements include coverage for:

- ***Network security liability:*** Liability to a third party as a result of a failure of your network security to protect against destruction, deletion, or corruption of a third party's electronic data, denial of service attacks against internet sites or computers; or transmission of viruses to third-party computers and systems.
- ***Privacy liability:*** Liability to a third party as a result of the disclosure of confidential information collected or handled by you or under your care, custody, or control. Includes coverage for your vicarious liability where a vendor loses information you had entrusted to them in the normal course of your business.
- ***Regulatory investigation defense:*** Coverage for legal expenses associated with representation in connection with a regulatory investigation, including indemnification of fines and penalties where insurable.
- ***Crisis management and event response expenses:*** Expenses incurred in responding to a data breach event, including retaining forensic investigator, crisis management firm, and law firm. Includes expenses to comply with privacy regulations, such as communication to impacted individuals and appropriate remedial offerings like credit monitoring or identity theft insurance.
- ***Cyber extortion:*** Ransom and/or investigative expenses associated with a threat directed at you that would cause an otherwise covered event or loss.
- ***Network business interruption:*** Reimbursement of your loss of income and/or extra expense resulting from an interruption or suspension of computer systems due to a failure of technology. Includes coverage for dependent business interruption.
- ***Data asset protection:*** Recovery of costs and expenses you incur to restore, recreate, or recollect your data and other intangible assets (i.e., software applications) that are corrupted or destroyed by a computer attack.

Some carriers offer elements of risk mitigation and loss prevention services, like the crisis management and event response expenses as a service bundled with the insurance coverage but not eroding the policy's limits.

All this comes at an expense. The "above the surface" or cyber incident costs include post-breach consumer protection, regulatory compliance, public relations, attorney's fees, and litigation. Some of the beneath the surface or hidden costs are increased insurance premiums, the impact of operational disruption or destruction, loss of value of customer relationships, the loss of revenue, and the devaluation of trade name.

What insurance is unavailable?

Some risks and losses that are generally uninsurable now include loss to business reputation and brand value. Cyber insurance generally does not cover the financial loss arising from brand or reputational impact of a cyberattack, lost customer data, etc. A hack of your customer's data may not be covered as well. Think of the Mossack Fonseca law firm and the "Panama Papers." Insurance may not cover the intellectual property of others in your care, custody, or control. You should carefully review your policy so that you know the parameters of coverage for loss of data, particularly another person's data that may be in your possession.

Insurance also does not generally cover loss of contracts and damage to your business relationships. You cannot insure against loss revenue from contract termination because a client feels you do not have adequate cybersecurity. Similarly, insurance for loss of intellectual property value, such as the value of trade secrets that may be compromised by a cyberattack, is not currently available. Another example of something with a huge downside cost to your organization would be a failed merger or acquisition that did not occur due to a security breach as there is currently no insurance for “deal failure.”

Conclusion: Plan, manage, and insure

Disasters will happen. The frequency of natural disasters is increasing, as is the magnitude of losses. According to the *US Geological Survey*, “Natural disasters are a ‘growth’ industry. Since the 1960s, economic losses from natural disasters on a global scale have tripled, while insured losses have quintupled.”

There is also no doubt the frequency of man-made disasters, particularly disasters caused by cyber threats, are increasing rapidly in both frequency and magnitude. *Newsweek* reports that ransomware attacks rose by more than 250 percent during the first few months of 2017, and the United States is the country worst affected by the issue.

Planning for disasters involves a lot of work. Every company needs a proactive plan to protect its networks and to deal with natural and man-made disasters quickly and efficiently. Every company also needs a thorough evaluation of its current insurance program and a realistic analysis of the additional coverages it needs in the face of both its “old school” and cyber risks.

Priya Cherian Huskins

Partner and Senior Vice President

Woodruff Sawyer & Co.

Woodruff Sawyer & Co. is one of the largest independent insurance brokerage and consulting firms in the country. She chairs the company’s Corporate and Executive Protection Claims Committee.

F. Lane Finch, Jr.

Partner

Swift Currie in Birmingham, Alabama

He has litigated first-party and third-party insurance claims in Alabama and California for almost 28 years.