CONNER STRONG & BUCKELEW

ADDRESSING THE WIDE-RANGING CYBER RISKS FACING BUSINESSES AROUND THE GLOBE

Cybercrime has advanced into one of the largest threats facing businesses around the world. Data breaches and cyber-attacks affect organizations of all industries, sizes and geographies and can leave behind devastating impacts that last for months or even years.

The methods leveraged by cybercriminals to compromise business systems are evolving at a breakneck pace, and business leaders, regulators and cybersecurity experts are struggling to keep up. Data breaches are far from the only cyber threat facing businesses. Ransomware attacks, in which cyber criminals hold a network or database hostage in exchange for payment, have skyrocketed in recent years. Cyber criminals are even capable of hacking into a network and taking control of machinery and devices currently in use, putting employee and customer safety at risk.

All of this means that the need for a robust cybersecurity protection in the form of insurance and risk management has become imperative for all businesses. It is no longer just the large corporations under threat. Every business, no matter how small, must protect themselves from this evolving risk.

CONNER STRONG & BUCKELEW

CONNER STRONG & BUCKELEW

CYBER-ATTACKS BY THE NUMBERS

Data breaches continue to become more costly year after year

2018 Stats:

Average total cost of a data breach:
$3.86 million

Average total one-year cost increase:
6.4%

Average cost per lost or stolen record:
$148

One-year increase in per capita cost:
4.8%

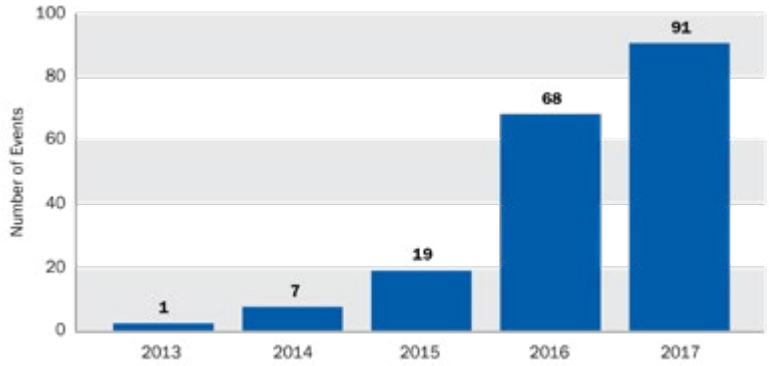
Likelihood of a recurring material breach over the next two years:
27.9%

Source: IBM & the Ponemon Institute's 2018 Cost of a Data Breach Study[1]

Ransomware emerges as a top threat

Ransomware attacks have exploded over the past five years. These attacks have the potential to hold entire systems hostage, completely shut down operations, lead to lengthy business interruptions and cause physical damage to facilities, machines and employees.

INCREASED FREQUENCY OF RANSOMWARE



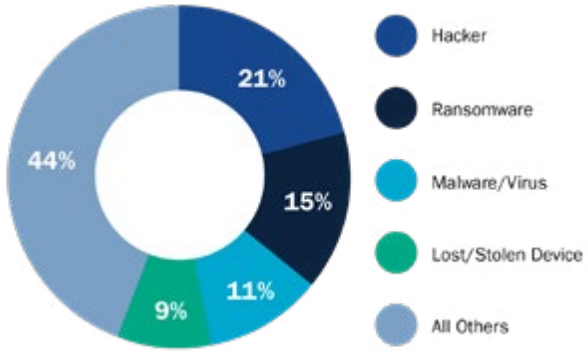
[1] https://www.ibm.com/security/data-breach

$229K was average total cost for Ransomware

Source: 2018 Cyber Claims Study from NetDiligence[2]

Malware attacks are a serious threat:

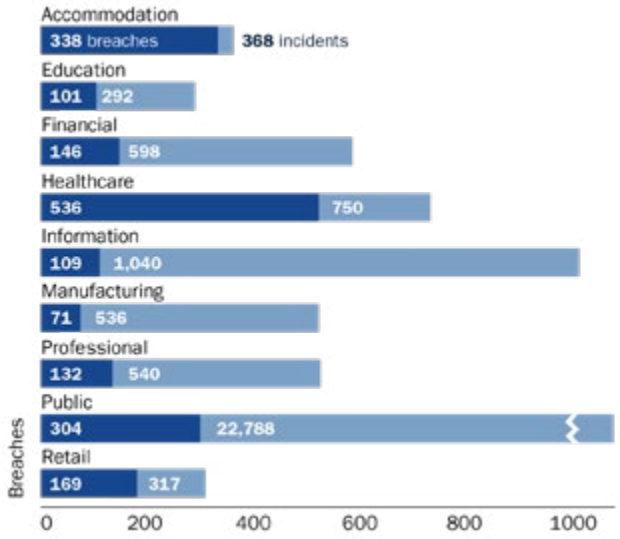
CAUSE OF LOSS



Source: 2018 Cyber Claims Study from NetDiligence[3]

Nearly every business and institution is a target of cyber-attacks:

NUMBER OF INCIDENTS AND BREACHES BY SECTOR



Source: Verizon's 2018 Data Breach Investigations Report[4]

[2] https://netdiligence.com/wp-content/uploads/2018/11/2018-NetDiligence-Claims-Study_Version-1.0.pdf

[3] https://netdiligence.com/wp-content/uploads/2018/11/2018-NetDiligence-Claims-Study_Version-1.0.pdf

[4] https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf

CONNER STRONG & BUCKELEW

ENSURING THE RIGHT INSURANCE COVERAGE IS IN PLACE

Business leaders normally associate a cybersecurity event with personal information and credit card numbers. But cybersecurity threats are a peril that can affect nearly every facet of an organization. Everything from physical property to an employee's health can be impacted by a cyber-attack. As such, an organization's coverage must reflect these myriad risks.

At a minimum, an organization should consider including the following parts in their insurance package.

Cyber Coverage Package Checklist:

1ST PARTY
(expenses incurred by entity; not third-party claims)

- ☐ Business interruption and extra expense
- ☐ Ransom payments
- ☐ Restoration of data/systems
- ☐ Legal and forensic costs

3RD PARTY
(claims by third parties affected by insureds breach)

- ☐ Privacy liability
- ☐ Security liability
- ☐ Regulatory defense
- ☐ PCI compliance
- ☐ Media liability
- ☐ If applicable: Professional liability

INCIDENT RESPONSE
(a first party coverage)

- ☐ Professional help: Legal, forensics
- ☐ Notification costs to potentially affected individuals
- ☐ Credit monitoring, call center and privacy monitoring for potentially affected individuals
- ☐ Public relations costs

Cyber-attacks can cause physical damages

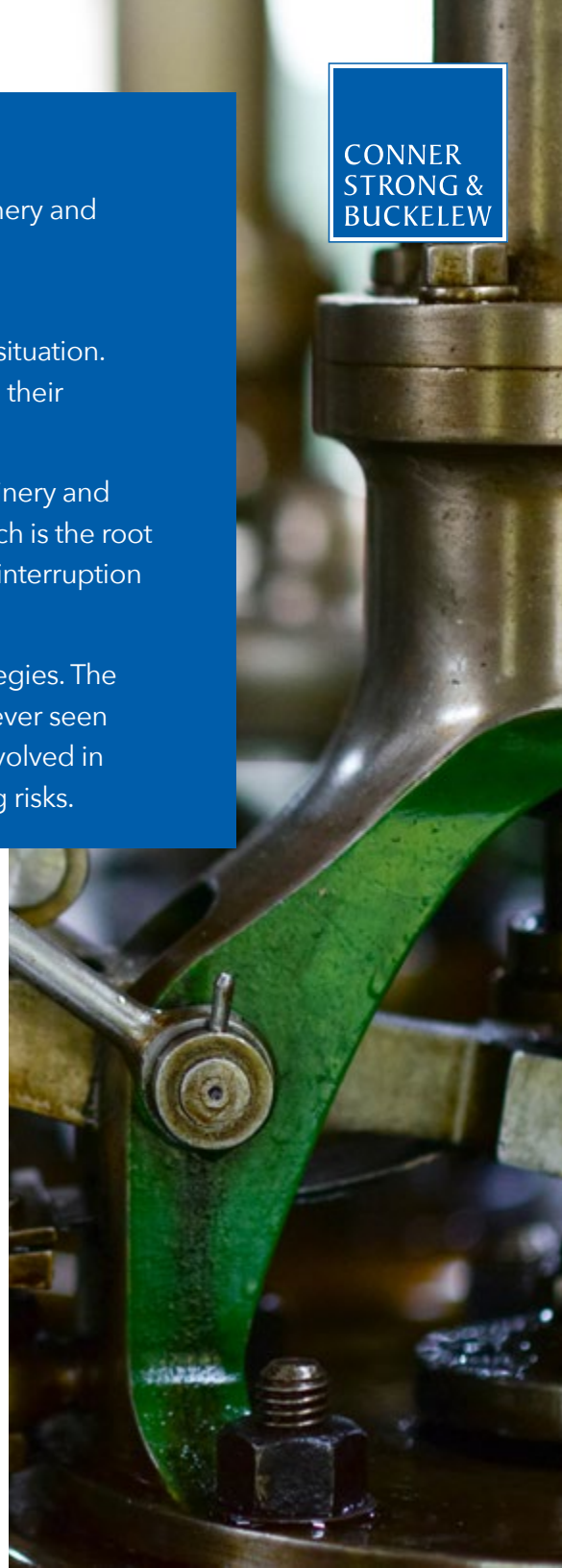
Cyber criminals are increasingly utilizing tactics that target the manipulation or complete shutdown of machinery and systems used to make everything from automobiles to clean water.

Take for instance FedEx, which lost $300 million due to business interruptions in 2017 when its systems were compromised by hackers. Shipping company Maersk also reported $200 million in losses thanks to a similar situation. Hackers are even disrupting electrical grids, gas providers, and other public utility systems that are increasing their reliance on internet-connected devices but lacking in cybersecurity standards.

Many organizations fail to prepare for the potential physical damage these breaches can cause to their machinery and inventory, as well as the business interruptions that could lead to significant financial loss. When a cyber breach is the root cause of an incident, there may be some gaps in coverage, or even outright exclusions, in standard business interruption or property insurance policies that could leave organizations fully on the hook for any resulting damages.

These threats are only becoming more sophisticated as hackers develop new malicious techniques and strategies. The potential damages of such an event are extreme, and the next significant hack could come in a form we've never seen before. Now more than ever, organizations with internet connected devices and machines that are directly involved in manufacturing a product must ensure their risk management and insurance packages address these evolving risks.

CONNER STRONG & BUCKELEW



The following cyber coverage nuance should be considered:

- "Terrorism" or "Cyber terrorism," however named, should be included. The traditional war/terrorism exclusions can potentially exclude some cyber-attacks.
- The period of restoration should be long enough to fully recover from an event, no less than 120 days and up to a year or more.
- Review the "Insured vs Insured" exclusion as you want to ensure you are protected when you allegedly/actually fail to protect employee information.
- Ensure the definition of "System" or "Network," by whatever name known, is broad enough to include network components you own, lease or rent, such as data center servers.
- Check if coverage is included for a system failure, an event that does not occur from a breach, but an accidental event.
- Are pre-emptive shutdowns to prevent future loss covered?

REACTING QUICKLY & EFFECTIVELY TO A CYBER-ATTACK

When an organization is the target of a cyber-attack, it can be difficult to know what to do first. Depending on the type of attack, a number of questions come to mind. How do I get my business back up and running as fast as possible? How do I keep my customers from leaving? How do I avoid a large legal fallout while doing right by my clients?

Thankfully, insurance carriers offering cyber coverage are well versed in these situations and can direct you to lawyers experienced with cyber events, access to additional experts and financial coverage. They've dealt with all kinds of cyber events and can connect the victims of cyber-attacks to the specialists needed to quickly and effectively remedy the situation.

At Conner Strong & Buckelew, we have years of experience counseling our clients throughout the claims process. Below are the first three steps every victim should consider taking after suffering from a cyber-attack:

1. Immediately contact your broker to engage your cyber carrier

According to Verizon's latest Data Breach Investigations Report[5], roughly two-thirds of breaches in 2018 took months to discover. Only 3% of attacks were discovered within minutes. By the time most cyber events are discovered, organizations are already behind the ball and cannot afford to waste a single minute to respond. It is critical that affected organizations immediately make their broker and insurance carrier aware of the issue. These experts are trained in responding quickly and effectively, and can bring in the right expertise to control the issue and contain the damages.

[5] https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf

2. Engage pre-approved legal counsel (breach coach)

Considering the massive financial and reputational damages that can result from a cyber-attack, now is not the time to try to save a few dollars by hiring inexperienced or subpar law firms. The best lawyers have years of experience dealing with the fallout from a cyber-attack and can counsel your business through the process, but it is important they be pre-selected before the breach happens and brought in right away. These experts can determine how to report the issue as well as protect your firm from outside litigation. Maintaining attorney client privilege is essential. Without it, the findings of the investigation into the cyber-attack could wind up in the hands of regulators or litigators that may wish to bring a lawsuit against the organization. The best cyber security law firms can direct a forensics investigation while preventing the findings from going public without the organization's permission and control.

When large-scale cyber-attacks are discovered, class-action lawsuits almost always follow. For example, former directors of Yahoo recently agreed to pay $29 million[6] to settle a lawsuit that stemmed from the organization's data breaches, and many believe this case will set a precedent for more to come.

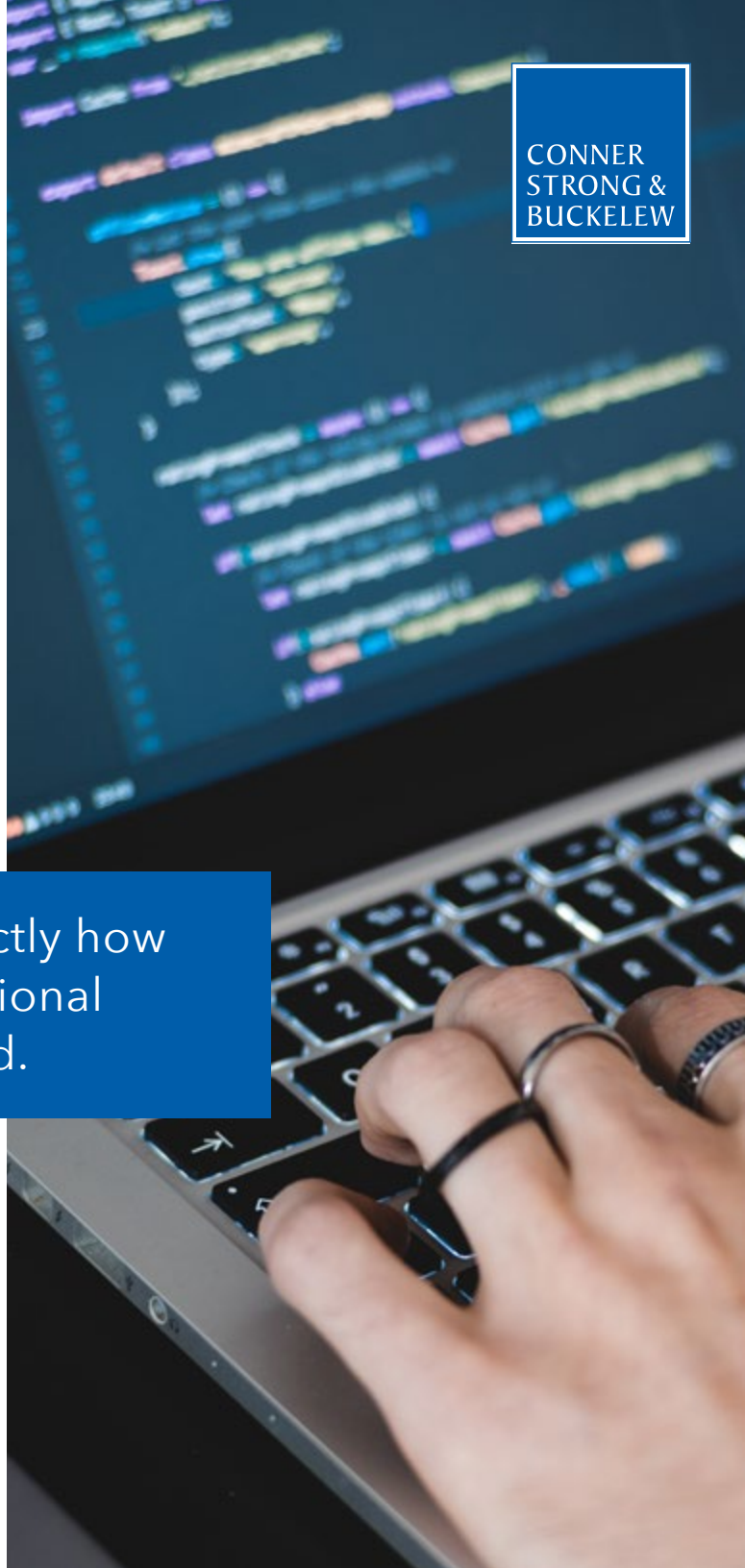
[6] https://www.nytimes.com/2019/01/23/business/dealbook/yahoo-cyber-security-settlement.html

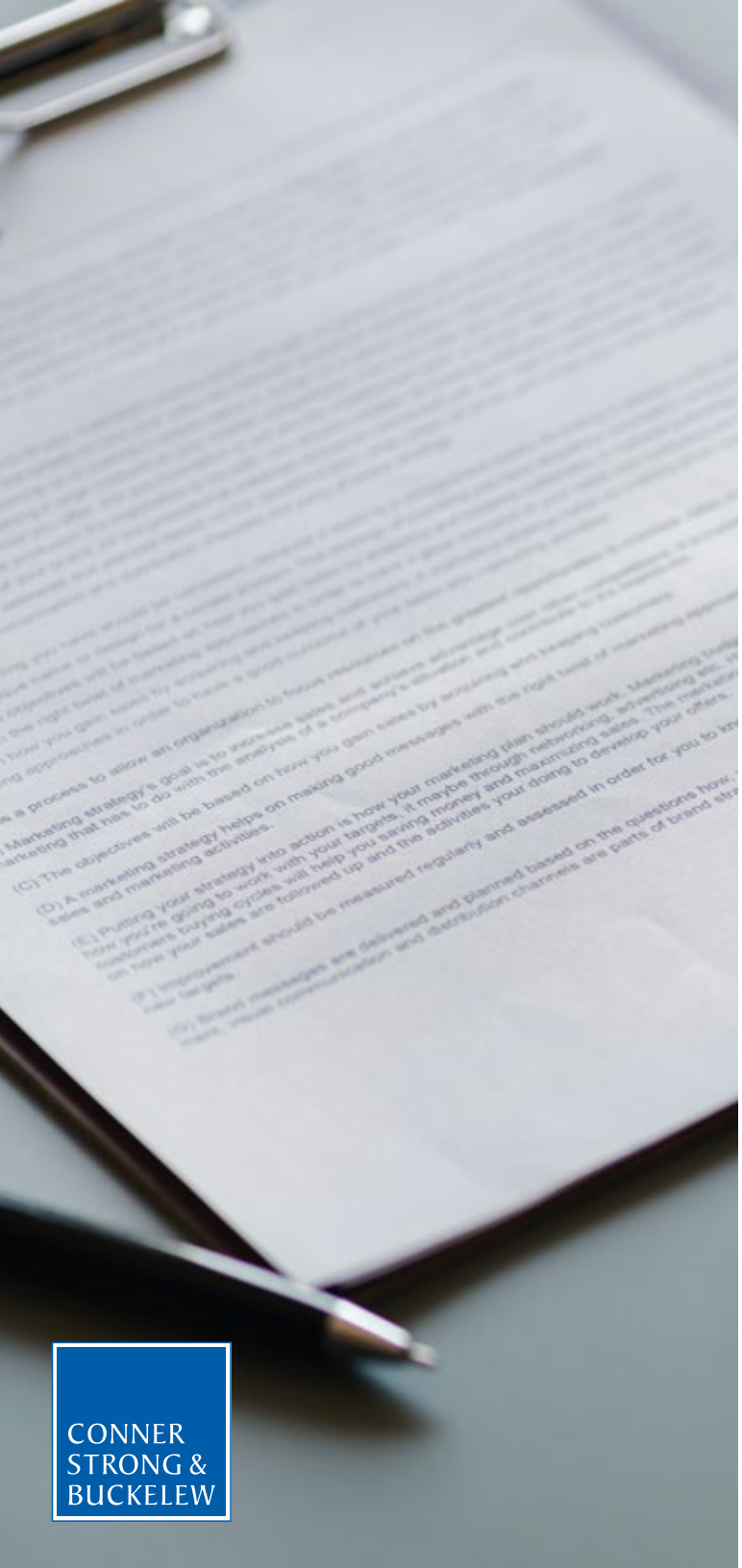
3. Have your breach coach engage computer forensics

Leading computer forensics firms are trained to determine the existence, cause and scope of a cyber-attack. They can also engage other professionals as needed to figure out the specifics of exactly what happened. Many victims of cyber-attacks fail to determine exactly how widespread the damage is, which can lead to additional cybersecurity vulnerabilities going left unaddressed. Other organizations fail to realize that far more sensitive information was compromised than was originally thought. This can lead to additional customer relations problems when the firm is forced to alert clients once again about more of their information that may be at risk. Organizations should always look to engage external IT professionals who focus solely on the type of breach that you may have suffered. This allows your IT staff to concentrate on business continuity issues, while leaving the breach to experts.

Many victims of cyber-attacks fail to determine exactly how widespread the damage is, which can lead to additional cybersecurity vulnerabilities going left unaddressed.

While completely preventing cyber-attacks from occurring at your business is unfortunately nearly impossible, organizations can mitigate the long-term damage caused by an attack by bringing in the right help and responding quickly and effectively.





CONNER STRONG & BUCKELEW

COMMON CYBER CLAIM MISTAKES

Unfortunately, we've seen our share of mistakes organizations can make when responding to a cyber-attack. Given, the relative novelty of these attacks, many organizations are unsure how to properly respond. Avoid these common mistakes when handling a cyber event:

- Going alone and not engaging insurance carrier, legal or forensics
- Waiting to report the claim
- Incurring costs before reporting a claim
- Hesitating to engage forensics
- Failing to properly alert customers in a timely manner
- Failing to offer credit monitoring to affected individuals
- Improper documentation of evidence
- Forgetting to check vendor contracts to see if they have notice obligations

[6] https://healthitsecurity.com/news/fda-unveils-mitres-medical-device-security-playbook

WHAT ORGANIZATIONS SHOULD DO NOW

One of the biggest mistakes we see in the market is organizations waiting to take cybersecurity seriously until after they've fallen victim to an attack. With cybercrime happening with increasing frequency, businesses can no longer afford to wait to take action. Below are three steps every business should take today to step up their cybersecurity preparation:

1. Take inventory of your cyber policy, protections and resources

   Despite taking the time to secure a policy, many business leaders are unclear or simply unaware of the full scope of coverages and protections the policy contains. The first step in protecting an organization from a cyber-attack is to completely understand your cyber liability insurance policy and resources available. These policies typically go far beyond offering financial coverage to include access to experts, training programs and much more.

2. Set and practice an incident response plan

   Having the proper policies and procedures in place, such as a cybersecurity incident response plan and a business continuity plan, can make all the difference when disaster strikes. Business leaders must ensure they can access these policies if their computer network is down. Practicing your response plan can help limit the scope of the damage, both financially and reputationally, once an attack is detected.

3. Provide regular employee cybersecurity training:

   Employees are an organization's the first line of defense against a cyber-attack. According to IBM and the Ponemon Institute[7], 27% of data breaches were cause by inadvertent or negligent employee behavior. An investment in security awareness training for employees today can pay dividends down the line.

[7] https://www.ibm.com/security/data-breach

REVIEW YOUR COVERAGE TODAY

Cybercriminals are attacking business with increasing frequency and sophistication. This threat has evolved into one of the largest and most pertinent liabilities facing businesses today. While these attacks may be extremely difficult, if not impossible, to ward off entirely, organizations must ensure they have proper protections in place in order to respond effectively, limit the scope of the damage and recover quickly.

Considering the complexity and breadth of these risks, securing these protections can be difficult do go at alone. At Conner Strong & Buckelew, we've been on the front lines of this issue for years, and specialize in cyber liability coverage for businesses of all sizes and types. The worst mistake an organization can make is to delay.

To learn more about Conner Strong's Cyber Insurance practice, visit:

CONNERSTRONG.COM

AUTHORS

TERRENCE J. TRACY, CPA
Managing Director, Executive Vice President
267 702 1458
ttracy@connerstrong.com

JORDAN CARTER
Associate Producer
856 552-4590
jcarter@connerstrong.com

CONTRIBUTORS

HEATHER STEINMILLER
Managing Director, General Counsel
267 702 1366
hsteinmiller@connerstrong.com

EDWARD J. COONEY, MBA
VP, Account Executive
973 659 6424
ecooney@connerstrong.com

BRADFORD BARRON, ARM
Vice President | Deputy General Counsel
267 702 1471
bbarron@connerstrong.com