GRAHAM COMPANY

JANUARY 16, 2019

THE STATE OF INSURANCE IN 2019

The new year is upon us, and although what the next 12 months will hold is uncertain, it is part of our job to stay ahead of industry trends. We forecast the following trends will have an impact on the insurance industry, especially for organizations willing to modify existing processes in order to evolve.

Artificial Intelligence and Automation

There is significant promise for leveraging automation in the insurance industry. And for good reason.

For example, policy analysis – analyzing provisions of large commercial buyers' insurance policies – is still a relatively labor-intensive process to ensure the coverage that was negotiated is in place. Artificial intelligence can help to automate this process by leveraging machine learning to analyze the exact wording of the policy. For those insurance brokers that sell very customized policy packages, this can be especially helpful in ensuring accuracy. There may also be an opportunity to utilize artificial intelligence to determine vulnerabilities that leave an insurance buyer's organization exposed to uninsured or under-insured loss.

It is important to understand that the benefits of artificial intelligence cannot be realized overnight, because the machine will need to be taught the correct algorithm and the precise wording to look for by humans. In addition, there will be an ongoing role for humans in the process, as insurers are always changing policy forms and terms. However, once the machines are "trained," the opportunity is huge. Although the true impact of this technology is still to be seen, the consensus

in the insurance industry is that artificial intelligence is here to stay.

Cyber Protection

Everyone with access to the internet and a television knows that there has been an increase in data breaches at many major organizations, but companies of all sizes can risk exposing their data if preventative actions are not taken. Cyber liability insurance was created to address this exposure and help protect businesses from financial pain and reputational damage.

50 percent of healthcare, technology and retail companies in the U.S. currently have cyber liability insurance, but only 5 percent of manufacturing companies in the U.S. have coverage. We predict that these numbers will increase across all industries in 2019. In fact, my colleague Eric O'Neill recently wrote a blog on the rise in popularity and increasing need for cyber liability insurance.

Data Analytics

New technology is giving organizations access to data like never before, and new ways to make best use of that data are continuing to surface. For instance, Ann Hampson, our resident data expert, recently wrote about the different ways data is being used in the Health and Human Services space.

At Graham, we created GrahamAlytics™, a business analytics system that drills down on loss/claims information, because we believe in the power of data and the promise it can bring to our clients. GrahamAlytics™ provides our clients with a way to harness their data to drive actionable insights that improve business operations. This is how we are equipping our clients to uncover big picture trends and lower their long-term cost of risk and insurance.

If you're interested in learning more about the trends that will impact the insurance industry in 2019, check out this article published in *Insurance Business*.

I, along with other industry experts, had the opportunity to speak with the editor about these trends in more depth.

THOMAS P. MORRIN
Senior Vice President
tmorrin@grahamco.com
The Graham Building
Philadelphia, PA, 19102
215-701-5430

JANUARY 16, 2019

THE STATE OF INSURANCE IN 2019

In today's news headlines, a week doesn't pass without a mention of a large company experiencing some type of cyberattack or breach. Examples of high-profile cyberattacks in the news over the last year include the Equifax breach, which has cost the company over $242 million, and the WannaCry attack, which has cost companies a total of $4 billion. In fact, it was estimated that cyberattacks in 2017 cost companies over $500 billion.

The price tag of cyberattacks are not only limited to first party costs but can also result in millions – or in some cases, billions – in third-party costs, like regulatory fines. Uber recently settled an investigation into its 2016 data breach for $148 million, a consequence of not disclosing the breach in the required timeframe. Not

to mention Facebook could face a $1.63 billion fine from the EU for not adhering to the recently enacted General Data Protection Regulation (GDPR) standards.

Cyber liability insurance was created to address this exposure and help protect businesses from financial pain and reputational damage. Prior to this type of insurance, general liability policies typically excluded covering cyber exposures, leaving companies vulnerable and in a tough financial spot should an attack or breach occur. Now, with cyber liability insurance, companies have both first party coverages – such as data destruction, theft, business interruption, and denial of service attacks – and third-party coverages – like fines for failure to safeguard data. Other benefits that come with cyber liability policies include reimbursement for security audits, post-incident public relations and expenses that stem from the investigation of a breach or attack.

However, one new challenge has emerged related to cyber liability insurance: the crossover it has with other policies, such as professional liability and commercial property insurance. If an insured company doesn't have a common carrier for cyber and professional policies, it typically leads to finger pointing by the respective carriers since incidents can be covered by both policies.

An example of when this may occur is if Personally Identifiable Information (PII) or Protected Health Information (PHI) is compromised. This could be covered by the cyber liability policy as a cyber breach or by professional liability policies as the insured didn't do enough to protect the data. In this case, there would be unnecessary red tape trying to decide and recover the expenses for indemnification of individuals affected by the attack, payment card industry fines, and costs associated with regulatory defense and fines. Another example is when commercial property is intentionally damaged by a bad actor, such as a hacker setting off a building's sprinkler which causes damage to the property. This instance could be covered by both cyber liability insurance and commercial

property insurance.

While the interplay of various coverages may create some temporary challenges, those challenges should not diminish the value, and necessity, of cyber liability insurance. The numbers speak for themselves. Currently, the annual gross written premiums of cyber liability policies are over $5 billion, with the market expected to grow to $7.5 billion by 2020. Cyber liability insurance is increasingly embraced in industries where attacks or breaches are becoming more prevalent, yet, many industries still lack necessary protections. While 50 percent of healthcare, technology and retail companies in the U.S. currently have cyber liability insurance, only 5 percent of manufacturing companies in the U.S. have coverage. This exposes manufacturing firms to tremendous risk.

Regardless of industry, every company has cyber exposures that are not limited to only attack or breach expenses. For example, a manufacturing company could be affected by a cyber-attack that locks it out of its system, leading to no access to company orders, product designs or production equipment. Cyberattacks could also target companies' equipment or property and result in property damage by causing the equipment to malfunction. This was the case in 2014, when hackers caused a German steel mill's blast furnace to overheat, leading to millions of dollars in property damage.

The good news is that an insurance broker can help companies navigate any challenges and industry-specific risks. By working closely with an experienced broker, who understands these nuances, companies can ensure the appropriate policy is in place and there are no crossover issues. Each business needs a partner that understands the unique exposures it faces to be able to design a tailored risk management and insurance program that provides comprehensive protection from cyber threats.

ERIC O'NEILL
Producer
EOneill@grahamco.com
The Graham Building
Philadelphia, PA, 19102
(215) 701-5380

JANUARY 16, 2019

THE STATE OF INSURANCE IN 2019

From last year's Equifax breach to the highly publicized WannaCry and NoPetya attacks, cyber incidents have quickly become one of the top risks facing companies across almost every vertical. Chubb, the world's largest property and casualty insurer, found that 93 percent of small and midsized businesses have reported experiencing a cyber incident that severely impacted their operations.

Unfortunately, the construction industry is not exempt from this growing threat.

As contractors become more reliant on technological integrations such as Building Information Modeling (BIM) and telematics software, companies are simultaneously exposed to the increased risk of a cyber incident. Cybercriminals could gain access to intellectual property such as architectural assets, financial information and even personal employee data, if it's not properly protected. For example, Turner Construction was the victim of a company-wide breach in 2016 that exposed the

names and social security numbers of its nearly 6,000 workers, after an employee unknowingly sent sensitive data to a fraudulent email address.

However, there are several strategies construction firms should consider to decrease the likelihood of a cyber event. To start, employees are often unknowingly the initial source of the breach – such as the case with Turner Construction. According to the Identity Management Institute, 90 percent of all successful cyber-attacks began with an employee. Therefore, all personnel should be regularly trained on security procedures and required to frequently update passwords. In addition, if employees are accessing data from a mobile device, the company's network must have data encryption software and employees will need to have the device password protected.

Combined with frequent training and continued cyber education, companies can take several steps to guarantee its intellectual property is protected. For example, security software should be installed that offers automatic updates and real-time protection. Aside from computer software, data should be frequently backed-up using a reliable cloud storage provider. Having a robust security program is key to preventing a costly data breach and firms should seriously consider hiring an in-house security expert to ensure data is protected.

If the victim of a cyber incident, construction companies will incur heavy costs associated with the security failure. What many contractors don't realize is that the largest exposure is related to incident response and first-party loss – including forensics, business interruption, digital data recovery and extortion. For instance, what happens if a company can't access job data or order information because its systems were taken offline? This delay in operations alone could cause a significant loss in revenue. According to claims analyzed by Chubb over a three-year period, the average costs of forensics after a cyber incident was more than $230,000.

For many contractors, one of the most valued benefits of a cyber insurance policy is having access to a specialized incident response team and experienced claims representatives. Having these individuals as an extension of your team is invaluable, as they are trained to work closely with your organization to walk you through exactly how the breach occurred. Working hand in hand with your insurance broker to identify potential cyber risks facing your specific operation can also help to ensure you're protected with proper insurance policies and adequate limits. Your insurance broker can serve as a true risk management consultant, helping to identify and implement strategies that limit exposures.

SHANE RICCIO
Producer
sriccio@grahamco.com
The Graham Building
Philadelphia, PA, 19102
215-701-5299

JANUARY 16, 2019

THE STATE OF INSURANCE IN 2019

Why are cyber risks heightened during mergers & acquisitions (M&A)?
There will always be heightened risk when two organizations' information security programs merge, because the likelihood of a breach increases as the total cyber footprint expands. An August 2017 data breach at a Philadelphia-based health

group gave hackers access to the files of 300,000 patients, exposing private data including names, addresses and even social security numbers. The breached health group had recently completed a merger – and while the exact type of system failure that allowed this cyberattack to occur cannot be identified, this incident does shed light on cybersecurity, a potential liability that is often overlooked during M&A.

What are the potential cyber concerns of M&A?

It is important to understand that if the acquired organization has sub-standard safeguards, the acquiring company is at a greater risk of being hacked. During an acquisition, the damages resulting from a breach are inherited by the acquiring organization, which could result in significant expenditures. Organizations must also consider how their cyber risks will evolve. The acquiring company should first assess both the amount and the type of data being acquired. If one hospital network is acquiring another, the acquiring company will need to confirm they are able to properly protect an enlarged amount of sensitive patient information and are compliant with applicable Federal and State regulations. Because regulatory standards are determined by both industry as well as Federal and State protocols, the acquired company could also be held to different standards than the acquiring company.

How can cyber risk be reduced during M&A?

Businesses should first develop and implement a thorough plan to assess the risks associated with the acquisition. Any thorough pre-acquisition due diligence process must include a detailed cybersecurity and IT assessment of the organization being acquired. In addition to performing both vulnerability and penetration testing of the new network, a third-party security firm should be brought on to inspect the network for potential threats and bad actors that may have already breached their systems. Next, all employees should be regularly trained to recognize common

threats like social engineering fraud and phishing schemes. Email-born threats against employees are the easiest way for hackers to breach an organization, therefore representing the greatest risk. It is critically important that staff is trained to identify and report suspicious emails. Finally, organization executives should work closely with their insurance broker to ensure all cyber threats are properly analyzed and adequate coverage is in place, should a costly breach occur.

MARC D. LEONE, ESQ.
Producer
MLeone@grahamco.com
The Graham Building
Philadelphia, PA, 19102
215-701-5330

JANUARY 16, 2019

THE STATE OF INSURANCE IN 2019

According to the Insurance Institute for Highway Safety, there could be 3.5 million self-driving vehicles on the road by 2025. This outlook isn't surprising considering large automakers like Volvo, Audi, Tesla and even Cadillac announced plans in 2017 to begin testing this type of technology. As advancements in autonomous vehicle (AV) technology continue to gain momentum, the commercial impact is inevitable.

In 2016, Uber announced its self-driving commercial truck made its first delivery and most recently, Domino's and Ford publicized a partnership to test autonomous pizza delivery cars. There's no denying that the auto industry is changing. However, a complete market conversion is unlikely to happen overnight – but rather through incremental advancements. As the use of AV technology in the commercial sector evolves, manufacturing and distribution companies will need to prepare and adapt.

Amid the uncertainty, companies can take several steps to proactively evaluate their business strategy and begin preparing their operations:

1. **Refine overall corporate strategy.** The organization first needs to consider what autonomous vehicles will mean for their specific operation – analyzing both weaknesses and strengths. Because this advanced technology will need to be layered into a business' infrastructure over time, organization executives should develop an implementation timeline to include their immediate, short term, and long term goals.

1. **Prepare to incorporate technology into the supply chain.** The next step for many manufacturing and distribution companies is to begin considering how to integrate these advancements into their supply chain. Telematics systems can be incorporated into fleets first to analyze relevant data like driving patterns and servicing and maintenance upkeep schedules. While we naturally associate autonomous technology with self-driving cars on the road, this technology is also impacting logistics as a whole. For example, auto pallet movers and autonomous loading could transform traditional warehouse operations.

1. **Identify new opportunities and threats.** While autonomous technology has many safety benefits like collision avoidance systems and vehicle-to-vehicle communication capabilities that can reduce the likelihood of an accident for distribution fleets, this technology will also create new liabilities for the organization. For instance, self-driving fleets will be reliant on complex software, which could create a large exposure if the vehicle is hacked by cybercriminals. Organizations need to make sure cybersecurity and data management are a top priority.

1. **Contractual risk transfer.** As advanced autonomous technology grows in popularity, one of the primary concerns for both businesses and insurers is identifying accountability in the event of an accident. For example, if a self-driving commercial truck causes a collision, which organization is responsible – the operating company, the truck manufacturer, or the automation software company? As a legal strategy, manufacturing and distribution companies can utilize contractual risk transfer to limit their liability.

As autonomous technology enters the marketplace, lawsuits and court rulings throughout the country will undoubtedly shape legal responsibility. Businesses must understand emerging government regulations and insurance standards. Organization executives should consult their insurance broker to make sure that they are compliant with all evolving regulations and to evaluate both the potential opportunities and threats facing their operation. By working to develop a proactive risk management strategy, companies can identify exposures and reduce risk, to better protect their employees, property, equipment and balance sheet.[whitepaper-washkalavitch]

GRAHAM COMPANY

JANUARY 16, 2019

THE STATE OF INSURANCE IN 2019

Last month, a data breach at a Philadelphia-based health group gave hackers access to the files of 300,000 patients, exposing private data including names, addresses and even social security numbers. The breached health group had recently completed a merger – and while the exact type of system failure that allowed this cyberattack to occur cannot be identified, this incident does shed light on a potential liability that is often overlooked during mergers and acquisitions (M&A). As the growing threat of cyberattacks and the aftermath of successful breaches continues to play out for organizations across the U.S., it is becoming an increasingly important consideration for businesses to examine prior to executing a merger or acquisition.

In 2016, the global M&A market reached volumes of $39 trillion – the third highest year on record, with comparable levels predicted throughout 2017, according to a report by J.P. Morgan. While M&A contracts are frequently executed by companies across many verticals under a variety of circumstances, the goal is typically the same – to increase strength and resources and ultimately improve profitability. To ensure the overall long-term success of the transaction, organizations will now need to consider both the potential cyber concerns associated with the acquired company and also work to identify solutions to reduce risk as part of the M&A due diligence process.

Cybersecurity Considerations

As the number of M&A transactions continues to increase in volume and

complexity, organizations acquiring a secondary entity will first need to assess the target entity's information security programs to ensure proper and sufficient precautions are in place. This is especially important because if the acquired organization has sub-standard safeguards, the acquiring company is at a greater risk of being successfully hacked.

Unfortunately, when one enterprise is in the process of acquiring another, the acquired organization could already have unknowingly been breached, setting the acquiring company up for a significant exposure once the target company is acquired. In 2017, the Ponemon Institute's Cost of Data Breach Study found that the average cost of a data breach was $7.35 million. Therefore, this is an especially important consideration during an acquisition, as the damages resulting from a breach are inherited by the acquiring organization, which could result in significant expenditures.

In addition to evaluating potentially unidentified cyber exposures, organizations need to consider how their cyber risks will evolve. The acquiring company should first assess both the amount and the type of data being acquired. For instance, if the acquired organization frequently handles credit card information, the acquiring company will need to confirm they are able to properly protect this specific type of data and are compliant with applicable Federal and State regulations. Because regulatory standards are determined by both industry as well as Federal and State protocols, the acquired company could also be held to different standards than the acquiring company.

Solutions

When acquiring an organization, it is crucial to take steps to improve cybersecurity measures as the likelihood of a breach increases as the total cyber footprint expands. Businesses should first develop and implement a thorough plan based on appropriate Federal and State requirements to assess the risks associated with the

acquisition. In addition to performing both vulnerability and penetration testing of the new network, a third-party security firm should be brought on to inspect the network for potential threats and bad actors that may have already breached their systems.

Next, all employees should be regularly trained to recognize common threats like social engineering fraud and phishing schemes. According to an IBM Security report, 60 percent of cyberattacks in 2015 resulted from within the organization. Email-born threats against employees are the easiest way for hackers to breach an organization, therefore representing the greatest risk. It is critically important that staff is trained to identify and report suspicious emails.

Finally, organization executives should work closely with their insurance broker to ensure all cyber threats are properly analyzed and adequate coverage is in place, should a costly breach occur. Appropriate coverage not only provides necessary coverage when a breach occurs, but can also provide front-end resources to lessen exposures and protect against a breach occurring. As cybersecurity continues to become an increasingly bigger business risk, vigilant brokers can help executives stay informed about the latest industry developments and protections, providing them with peace of mind that their business is secure.

MARC D. LEONE, ESQ.
Producer
MLeone@grahamco.com
The Graham Building
Philadelphia, PA, 19102
215-701-5330

MARK R. ALBERTO, M.B.A.
Vice President - Information Technology
MAlberto@grahamco.com
The Graham Building
Philadelphia, PA, 19102
215-701-5282

JANUARY 16, 2019

THE STATE OF INSURANCE IN 2019

Every company, regardless of size, is a potential target for commercial crime. Whether it's employee dishonesty, forgery or alteration, theft of money and securities, burglary or computer fraud, these types of criminal acts costs businesses billions of dollars each year.

Because crime-related losses are not typically covered by most property insurance policies, commercial crime insurance protection, also known as fidelity insurance, is a necessary component of a comprehensive insurance plan for any business. Unfortunately, the majority of businesses overlook commercial crime protection because employers don't think it can happen to them or that their employees are too loyal to commit acts of crime. Studies have shown that the majority of employee thefts are carried out by long-term employees.

Nearly 30 percent of all business losses are a result of employee theft, according

to the Better Business Bureau. In fact, a study by the Association of Certified Fraud Examiners (ACFE) estimates the average business is losing five percent of its total annual revenue to fraud, which translates to a potential fraud loss of more than $3.7 trillion worldwide.

Protecting Your Business from Commercial Crime

Commercial crimes can happen at any time. The changing economic environment, advancements in technology and expansion of operations overseas makes the threat even greater for businesses. No business should be a victim of crime. Here are some steps to better protect your company from potential threats.

Insure your business.

Liabilities covered by crime insurance typically fall into two categories:

- Employee dishonesty coverage – This type of coverage pays for losses caused by dishonest acts of employees, including embezzlement and theft, forgery or alteration and computer hacking.
- Money and security coverage – This coverage protects companies from securities taken by burglary, robbery and theft inside the company.

Employee background checks.

The first way to prevent fraudulent employee behavior is to hire the right candidates. Pre-employment background checks are especially important for employees handling cash or other sensitive financial data. Keep in mind that if a company hires an individual who has a prior criminal record and they steal from a company, it may impact the type of crime coverage the employer is holding. Sometimes the policy will not cover another criminal act committed by an employee who was hired with a prior criminal record. An important enhancement available on employee dishonesty insurance is to modify this prior criminal record

exclusion to only apply to prior acts that exceed a threshold of $10,000 or $25,000 (so an employee previously caught shoplifting isn't excluded from the company's crime coverage).

Educate employees.

Hold a training session on typical security threats that can hurt the company through the cyber world, as well as offline. Proper training helps employees understand what the security risks are and how they can contribute to a safer environment. Training should cover password policies, email and web usage, and mobile guidelines that can impact the company's network.
In the cyber world, Spear Phishing, also known as Social Engineering Fraud or Fraudulent Impersonation, which targets a specific individual via email with the intent of deceiving that person into transmitting funds and releasing confidential information has increased. Make your employees aware of the ways cybercriminals can hack your systems. Teach staff members to recognize the signs of a breach or a suspicious email, so you can identify and address as soon as possible.

Secure your network.

In case of a cyber attack, every business should invest in an anti-virus, malware and spyware detection software.

Businesses should be proactive about instituting policies and procedures before criminal incidents or events occur that could ultimately leave that company vulnerable to threats.

G. MARTIN IRONS, CPCU, CIC, ARM
Vice President - Technical Development Department
mirons@grahamco.com
The Graham Building
Philadelphia, PA , 19102
215-701-5266

JANUARY 16, 2019

THE STATE OF INSURANCE IN 2019

Have you or any of your employees received an email requesting that you transfer funds to a bank or vendor? Did you transfer the funds to only find out later that the email was a fake and now the funds are gone? If so, you, like so many others, were the victim of a Spear-Phishing Attack!

Spear Phishing, also known as Social Engineering Fraud or Fraudulent Impersonation, targets a specific individual via email with the intent of deceiving the individual into transmitting funds, releasing confidential information, etc. In most cases, once the funds have been transmitted, it is extremely difficult to recover them.

So how does this happen? The criminals, who are generally located outside of the United States, target corporate executives and gain access to their emails. They

make minor changes to the executive's email address and then send an email to an employee requesting that funds be wired. This has cost corporations millions of dollars in not only the loss of the funds, but also the investigation and potential litigation costs.

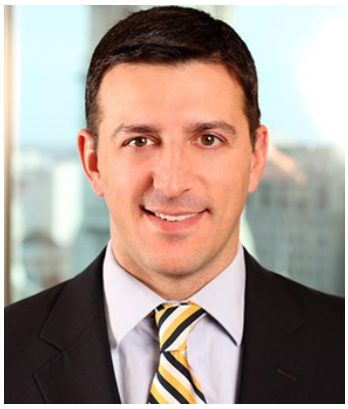
Insurance coverage is available for this type of fraud. It is generally provided by way of an endorsement to your Crime Insurance policy. While purchasing the insurance is advisable, the best defense to a claim like this is prevention.

Spear Phishing Prevention Tips

So how do you prevent becoming a victim of Fraudulent Impersonation? The following are some suggested practices for mitigating these types of losses.

- Education and training are the number one avenues to risk mitigation.
- Develop procedures requiring two or more employees to sign off on any wire transaction.
- Prior to transmitting funds to a new bank or vendor, a telephone call must be made to the original bank/vendor and specifically to a previously established contact.
- Provide frequent communication to employees regarding Social Engineering Fraud and what to do if an employee suspects suspicious activity or a potential attack.
- Conduct third party computer network penetration testing on a regular basis to monitor the effectiveness of the corporation's controls, training, etc.

It is highly unlikely that Social Engineering Fraud will lessen. In fact, it is projected to increase in both frequency and sophistication. But knowing what it is, how it is perpetrated and how to avoid it will help your organization from becoming a victim to it.



NICHOLAS M. CUSHMORE, ARM
Assistant Vice President
NCushmore@grahamco.com
The Graham Building
Philadelphia, PA, 19102
215-701-5422

JANUARY 16, 2019

THE STATE OF INSURANCE IN 2019

For years there's been an increase in cyber security issues. It's hard to go a single day without reading a story about how companies large and small are threatened by cyber risks. As a matter of fact, Graham recently released survey findings showing that cyber security risks are one of the top business threats keeping them up at night.

While many of us are familiar with hacking, it's quickly being elevated to a whole new level through the increased prevalence of cyber extortion threats. If you're unfamiliar with how cyber extortion works, let me explain. It's the process where cyber criminals deny user access to an organization's website, network or computer to extort payment in exchange for renewed access. This is a frightening proposition, and what's even scarier is that companies aren't doing enough to protect themselves from these threats.

As of late there's been an increase in cyber criminals using ransomware because it allows them to encrypt data on a server or computer and deny service to the

device until the victim makes payment for a “key” to unlock their data or files. While cyber liability insurance policies are available to combat this risk, there are certain broad exclusions you should be aware of so your company is protected if a cyber-criminal should attack.

Whether you’re a law firm, a manufacturer or a retail store, you’re at risk and need to take the right precautions to prevent or mitigate the risk associated with cyber extortion threats. A good IT team is always working to stay ahead of the curve and implement the best and most sophisticated cyber protection strategies available, but sometimes it’s not enough.

Combatting Cyber Extortion Threats

You might be wondering: *What can my business do to combat this risk?* The first step is to develop a robust risk management assessment aimed at uncovering the coverage gaps in your existing insurance program. General liability policies tend to be the industry standard, which covers things like bodily injury, property damage arising out of an insured’s operations, products or premises, as well as personal and advertising injury.

However, these policies were never intended to provide coverage for liability and first party notification expenses resulting from the disclosure of sensitive personal information. Only recently have insurance carriers begun adding exclusionary endorsements to ensure that their policy language doesn’t provide coverage for any of these potential claims.

The good news is that the insurance industry is tackling this issue head-on, and has already developed new cyber liability policies whose structure resembles a standard business automobile policy. In other words, one that provides coverage for both third-party liability claims against the insured, and first-party claims the insured makes against their own policy.

Four Things to Contemplate when Evaluating Cyber Liability Coverage

However, just getting your company any “off-the-shelf” cyber liability policy will not do the job. There are exceptions in those standard policies you need to be aware of, and here are four things to contemplate when evaluating coverage for your company:

1. **Failure to Encrypt Exclusions**
   Do not accept a policy that includes a “failure to encrypt” exclusion. You should consider encrypting data anyway to better protect your business from a breach but you do not need to buy a policy that will exclude coverage for loss of unencrypted data.
2. **Business Interruption**
   Many carriers include the option to purchase business interruption coverage for lost revenue due to your computer system being shut down. You need to understand if your policy is providing the coverage, many will not include this automatically.
3. **Governmental Fines and Penalties**
   A large exposure for most companies is the potential legal action brought by the Office of the Attorney General, the Office of Civil Rights, and the Department of Health and Human Services, among others. Failure to provide at least defense cost coverage, or coverage for fines and penalties, can leave a gap in protection.
4. **Be Aware of Your Data Vendor**
   When a company entrusts data to a third-party vendor (e.g., a third party processor or cloud provider) and the breach occurs on the vendor’s system, you’d like to be protected for vicarious liability by your cyber policy. However, some cyber liability carriers include exclusionary endorsements to take this coverage away.

Conclusion

As technology continues to evolve and cyber criminals become more skilled, it's not a question of if your company will be hacked, but when it will occur. This means that in addition to a strong IT department you need to adopt a cyber liability policy to further insulate your company from cyber extortion. But to make sure your policy is structured properly and that you have the coverage you need, make sure to enlist the help of your insurance broker.

NICHOLAS M. CUSHMORE, ARM

Assistant Vice President

NCushmore@grahamco.com

The Graham Building

Philadelphia, PA, 19102

215-701-5422

JANUARY 16, 2019

THE STATE OF INSURANCE IN 2019

The common movie theme where a wild robot wreaks havoc on an unsuspecting human populace (i.e., Terminator) has not happened yet (at least not that we are aware of); nor have people starting using metal maids on a mass scale like Rosie from the Jetson family. That being said, cyber liability exposure is a growing risk, and sometimes a multi-million dollar concern depending on a company's

operation. For manufacturing, engineering and distribution companies, cyber liability is or should be one of the first coverages to consider reviewing. If you don't think your company's firewall can be breached, think again.

Risk management in the manufacturing and engineering industries should be an *ongoing* conversation, rather than an annual presentation. Societal advancements, culture and the way we live our lives requires that technology play an important part in a company's risk management process. Direct focus on risk assessment and consideration should run through the whole organization.

Understanding Cyber Security & Liability Coverage

Cyber security is perhaps the biggest risk to technology operations, while product design and innovation is the largest risk to a business over the next several years. Rather than having a board or audit committee being responsible, risk management is better served by a dedicated staff and/or committee. This will ensure that the right people will be able to address and protect the company where exposure exists, whether it's because of years of experience in the industry or having the ability to understand a company's operation. Better yet, a broker with industry experience can really save you time and headaches, because he or she will understand operational exposures.

Cyber liability coverage is oftentimes misunderstood. People believe coverage is only available for electronic data protection or losses involving computers and networks. But this is not the case. Cyber liability coverage also protects paper files containing protected information, such as employee records and medical files. While cyber liability coverage may not be a common purchase for companies today, in the next several years we expect it to become the norm.

Trends

The world is trending toward mobile devices and away from stationary machines. Warehouses are being updated with miles of conveyors, controls and control software. No one company can do it all, and as a result the risk compounds upon itself exponentially. Contractors hire sub-contractors for each main function of the systems. New employees must be hired, varying in skill level and job function, but with different access to systems throughout a manufacturing plant, warehouse or distribution center.

Think about how our phones connect to machines like our cars, home security and audio systems. Many companies are doing the same with handheld devices and machinery in manufacturing, distributing and conveying operations. Because we want information, we create a need for information. This trending need exposes personal information on social media by allowing companies to see what we like or don't like. We become more predictable and in turn make company exposures more predictable. We want things to happen at the click of a button, and we want immediate technological gratification. To get instantaneous responses, companies and people sacrifice personal information and sometimes procedures. Cyber liability coverage will develop over time to account for advancing technology risk concerns.

Everything in today's world requires speed and accuracy. It's what we feel is needed to function. Yes, automation makes things faster and easier. However, since so many vendors are needed to create an automated warehouse or controlled distribution center, each one of them brings their risk of access to information. Many times, in order to support the information being available immediately, 24/7 support includes a Virtual Private Network (VPN connection). This type of *always-on* support creates new avenues to breach a system and gain information.
With all of the potential risks that come along with interconnected technologies,

what steps can you take to better protect your information?

Cyber Security Best Practices for Manufacturing & Engineering Industries

Vet Your Sub-Contractors

Prior to working with a subcontractor, make sure you thoroughly vet them first. Require them to perform certain activities for a system ahead of time and make sure they tell you exactly when they're going to do it. You should also incorporate clear language in your sub-contractor contracts regarding indemnification terms. This will ensure that you're protected should things go South.

Broaden Your Coverage

It can be very easy to assume that you're covered if something should go wrong, but there's only one way to know for certain. Make sure your policy language is broadened to pay for credit monitoring for affected individuals. Your policies should also be written so they cover any public relations expenses you incur as a result of any crisis communications services you need to mitigate reputational harm.

Have an Emergency Plan

The time for planning is before a crisis occurs, not afterward. Therefore, having an emergency response plan in place is critical. If this is your first time creating one, you don't have to do it alone. Loop in your broker, your legal team, your head of communications, and any other stakeholders who can provide you with insight into what needs to be accounted for should a cyber-crisis occur.

Conclusion

The cyber risks associated with interconnected technologies are a reality of

modern-day business operations and they aren't going away anytime soon. However, this doesn't mean you're helpless. By vetting your subcontractors, making sure you have the right insurance policies in place and creating a comprehensive emergency plan, you'll keep the wild robot at bay.
[whitepaper-Phillabaum]

LUKE ATKINSON FOLEY
Producer
LFoley@grahamco.com
The Graham Building
Philadelphia, PA, 19102
215-701-5332