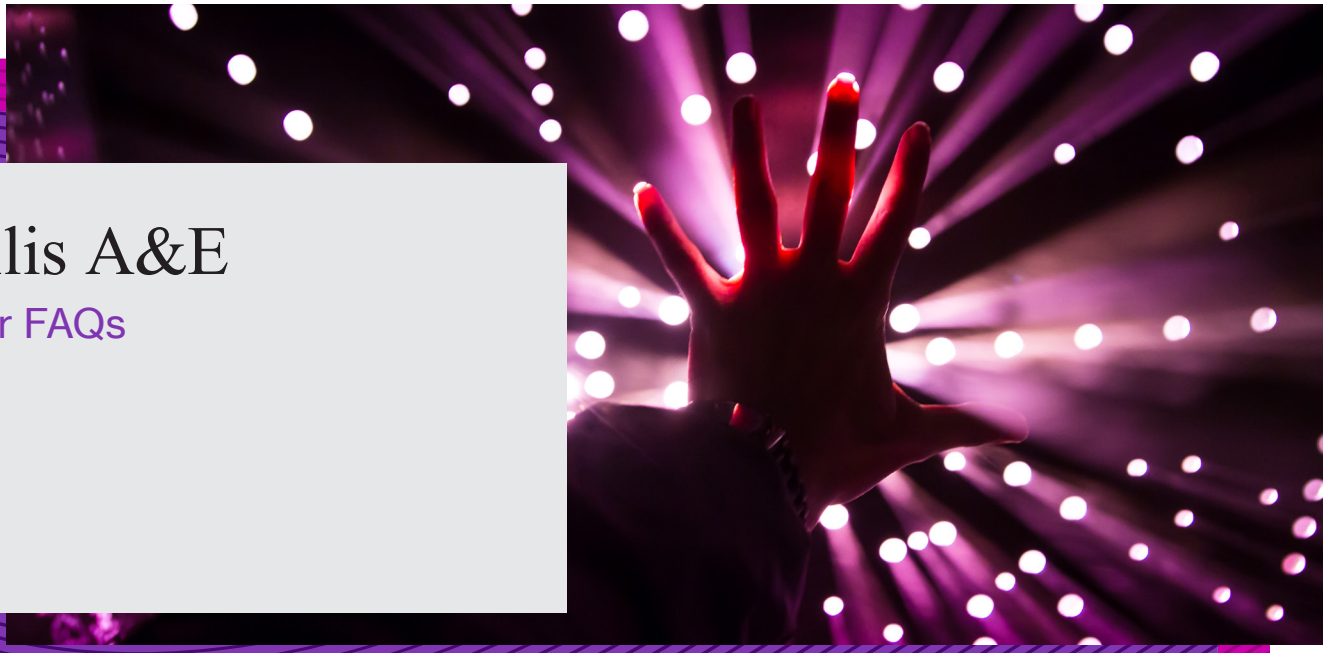

Willis A&E

Cyber FAQs

A&E Cyber Risk

Who is vulnerable to a cyberattack?

Everyone and anyone connected to the World Wide Web. Recommendations to reduce this vulnerability and mitigate the extent of an attack if one does occur include the use of a virtual private network, or VPN, security monitoring, two-factor authentication, frequent network back-ups, and limiting user access to confidential information.

Who is behind these cyberattacks?

Criminal organizations, professional hackers, amateur hackers, state actors and private persons can launch cyberattacks against enterprises. Insider threats or users who have authorized and legitimate access to a company's assets and abuse them either deliberately or accidentally also present exposure.

Why has ransomware become an emerging risk A&E firms need to be concerned about?

Ransomware has become an efficient way for hackers to make money. Data breaches, for example, require significantly more time, as the hacker needs to hack in, look for private or sensitive data, exfiltrate it, go to a dark web and find a buyer. That's a lot of hoops for the attacker to go through to get money in their pockets. With ransomware, on the other hand, hackers simply gain access to your system, lock up your data and hold it for a ransom. For that reason, any size company in any industry could be in the crosshairs.

How do these hackers commit ransomware?

- Cybercriminals find vulnerabilities within your network that can be exploited through various methods. Many vulnerabilities impact popular software, placing the users of the software at a risk of a data breach or other attack.
- Ransomware attacks all begin with the initial compromise, which can happen in a variety of ways, including social engineering or spear phishing (causing somebody to click on something).
- Once that compromise occurs, the hacker establishes a communication link, which allows them to exploit the organization remotely. Once the communication link is established, they can move through the network and target many different parts of the network. The more areas of the network they get into, the more leverage they have to demand a higher ransom. Their goal is to move through as much of the network as they can, while remaining undetected.
- Once the hacker has infiltrated your network, they hit the proverbial red button, encrypt and lock as many systems as possible, and hold them until a ransom is paid in their preferred form of cryptocurrency (typically Bitcoin).

Insurance

Should design firms have stand-alone cyber coverage?

Yes, every design firm should strongly consider purchasing cyber coverage. Cyber liability insurance, specifically the first-party coverage components, helps companies address the financial aftermath of a cyberattack or another type of data breach that occurs on an internal system. Cyber liability insurance also pays for customer or regulatory claims resulting from the theft or breach of customer data on your network. There is no better insurance tool to protect the bottom line of a company's financials from cybercriminals

What about the cyber coverage in my professional liability policy?

The cyber coverage afforded under an A&E professional liability policy is not equivalent to the coverage afforded by a stand-alone cyber security liability policy. Professional liability policies only provide third-party liability coverage for data breaches on clients' systems as a result of covered A&E professional services. A&E professional liability policies (typically) offer no first-party coverage benefits and do not cover expenses incurred when the insured's own network is impacted by a cyber breach or ransomware attack. As cyber coverage is rapidly evolving, you should consult your broker when exploring coverage.

Is cyber liability coverage the same as technology errors & omissions coverage?

No. Technology E&O insurance is a type of coverage that protects the providers of technology products or services (web designer, software developer, etc.). While tech E&O insurance typically contains a cyber liability coverage component, cyber liability insurance is designed, for the most part, to protect the owner/user of technological devices and services.

Why is the cyber market so "hard," and why are insurance rates increasing so much?

- Cyber risk is an ever-evolving risk and is a moving target every day.
- The primary driver for the last couple of years is the concept of compounded risk. Unfortunately, the market is finding that a single hacking event can lead to several different perils, such as ransomware, data breaches and crypto-jacking (using the company's CPU power to mine for cryptocurrency). The possibilities are endless in that capacity.
- These examples have led to an increase in claim frequency and severity within the cyber market. The increase in claim dollars paid out creates an increase in premiums and heightened underwriter scrutiny.

What are cyber carriers providing in the area of risk management assistance and support?

- Carriers are providing various resources to their insureds, from IT provider discounts, free staff training exercises, emergency response services, to legal services and even mobile applications to assist in the management of IT security.
- What we're starting to see in our industry over the last couple of years are cyber carriers providing their insureds with risk management services to help them manage their risk.

What are the critical coverage components?

There are numerous cyber security liability policy coverage components, which vary from carrier to carrier. Coverage endorsements and exclusions are very common and should be carefully reviewed. A good cyber security liability policy should, at a minimum, cover first-party loss and third-party claims. Coverage should include "network security coverage," which covers your business and business interruption losses that result from a network security failure, such as a data breach, malware infection, cyber extortion demand, ransomware or business email compromise. Coverage should also include "privacy liability" which could arise if sensitive customer and/or employee information is compromised through a breach. Most cyber policies also provide "media liability" coverage. Some common cyber policy enhancements include coverage for "social engineering," "bricking" and "reputation harm."

What are the important cyber coverage definitions that I should be aware of?

- Breach response costs: May include costs incurred to hire breach counsel, complete a forensic investigation, hire a public relations firm, notify affected individuals, set up call center services, and provide ID theft restoration/credit monitoring
- Network security & privacy liability: Coverage for indemnity and defense costs for third-party claims and regulatory actions alleging a security failure or privacy event
- Regulatory fines & penalties: Monetary fines and penalties an insured is legally obligated to pay due to a regulatory proceeding by a governmental entity

- Media liability: Coverage for indemnity and defense costs for third-party claims alleging media wrongful acts, such as defamation, disparagement and copyright/trademark infringement in the dissemination of internet content and media
- Business interruption/system failure: Indemnification for loss of income, extra expenses and claim preparation costs that arise directly out of an unplanned network outage
- Dependent business interruption/system failure: Extends business interruption coverage to include lost income and extra expenses incurred due to a network interruption at one of your critical third parties or outsourced providers that you rely on to conduct business
- Data recovery loss: Costs to rebuild, restore, replace electronic data or software corrupted or deleted in a cyber event
- Cyber extortion/ransomware loss: Extortion payments and associated expenses to investigate a security threat to release or refuse to unencrypt sensitive information or to bring down a network unless a ransom is paid
- Cybercrime: May include direct financial loss due to telephone fraud, crypto-jacking, social engineering, invoice manipulation or funds transfer fraud
- Reputational harm: Loss of net profit an insured would have earned if not for an adverse media event
- Computer hardware replacement costs (bricking): Replacement costs for computer hardware and devices or equipment left unusable due to a cyber event

What are the proper limits and retention for my firm?

While the extent of a cyber/ransomware attack is often difficult to measure, the limits appropriate for a firm are dependent on numerous factors, from financial size, visibility/popularity, client insurance requirements to risk appetite, etc. The retention will likely be dictated by the marketplace, largely dependent on the organization's financial size and claim history.

What controls and protective measures are cyber underwriters now requiring of their insureds?

Some of the more common requirements are virtual private networks (VPNs), multi-factor authentication (MFA), frequent backups and protected backup storage, and a disabled or protected remote desktop protocol (RDP). Supplementary cyber application forms specifically addressing ransomware controls have become the norm.

Are extortion payments insurable?

Yes, except where it's not permitted by law to pay an OFAC sanctioned entity.

What is the expected cost of cyber insurance?

The cost of cyber security liability insurance, similar to other types of insurance, is dependent on several factors, such as an organization's revenue, claim history, limits sought and the deductible/SIR. Premiums are also largely reliant on existing cyber procedures and protocols to protect the firm's network from outside intruders and can vary from less than $1,500 annually for the smallest of companies to well over six figures for large organizations.

Is there anything I can do to jeopardize coverage?

From the onset, it is critical that you accurately complete the application, which will become part of the issued policy, either physically or through policy language, pertaining to misrepresentation. Furthermore, cyber policies always contain explicit provisions concerning how and when an insured must provide notice of a claim, which is ever more important given the claims-made nature of the coverage. It is also critical that you don't panic when a claim arises and ensure that you obtain the insurer's "prior written consent" before expending funds in connection with a covered event.

What is NOT typically covered by my cyber insurance?

Potential future lost profits, betterment of technology systems after a cyber event, contractual penalties, decreases in company valuation, etc.

Incident Response Plan (IRP)

What is an incident response plan?

An IRP provides a structure for an organization to follow when a cyber incident is discovered. Most such plans are technical and intended to be used by IT professionals, but others are intended for the business stakeholders (non-IT professionals).

Should firms have an incident response plan in place to be prepared for a cyber-attack – and what would be included in this plan?

- Yes! Despite a firm's best efforts, all businesses are vulnerable to a cyberattack and should be prepared with a proper IRP.
- IRPs are not drafted overnight; companies can spend months building them out. IT professionals generally maintain their own series of response plans for different types of events.
- In addition to the IT team response plans, many companies build response plans for the business stakeholders as well. This would include the leadership team, legal, risk management and your HR department. There might be six to eight stakeholders that go outside of IT– all of which need to have a plan and be prepared in the event of a cyberattack on the firm.
- It's important to note that just about every top line cyber liability insurance carrier will offer resources around formulating or crafting an IRP. It is highly recommended that you take advantage of those resources.

What are the fundamental sections of an incident response plan?

- Background
- Incident response team
- Incident management
- Incident triaging
- Data breach universe definitions
- Notification procedures
- Mitigation and remediation

What are some of the high-level best practices for creating an incident response plan?

- The IRP is a "living document" that should be routinely updated and kept current.
- The incident response plan should be clear and easy to use during a crisis. Keep it succinct and make sure it is organized by sections. It should not be a "phone book" nor a "leaflet."
- It should include background information on regulations and laws, detailed incident management procedures and contact details of the incident response team.

What should firms be doing to educate their staff on managing cyber liability?

- Employees should be educated on strong passwords and the signs of social engineering and phishing malware attacks so they are not tricked into opening legitimate looking emails, attached files and links.
- Many companies these days do what's known as ethical spear phishing exercises. Essentially, they will send scammed emails to their workforce and see how many of their employees fall for the scam. The more and more you keep your employees on their toes the less likely – when a scam may get through your IT preventative systems – that they will click on something they shouldn't have. So again, simple things really can mean a big difference in terms of the preparedness a company has in place.
- Firms should implement tabletop exercises, so all staff and key stakeholders go through drills to test their IRPs. This would include arranging a fictitious incident to see how the plan works. Having a prepared team that has gone through regular and routine drills will be invaluable when a real cyberattack occurs.
- An organization that has demonstrated that its employees have completed tabletop exercises and routine drills will place itself in a much better position with a regulator.

What is a tabletop exercise?

A tabletop exercise is a structured incident response drill that triggers your IRP for testing purposes and involves members of your incident response team (IRT) (both internal and external). It tests the effectiveness and accuracy of the workflow of your current IRP.

Why should an organization conduct a tabletop exercise?

The exercise allows the IRT to identify any holes in your current IRP that need to be resolved and updated. It assures that members of your IRT and their contact details are current and accurate and that members of your IRT (both internally and externally) know of one another before any real incident. Finally, it demonstrates to inquiring regulators your team's readiness and "seriousness" in conducting a sound incident response methodology.

Any single bit of advice on how to conduct a tabletop exercise?

- Leak the hypothetical facts.
- Break up the facts into realistic pieces.
- Start with a minimal amount of information, similar to what you might receive when the cyber incident is discovered.
- Take a reasonable amount of time to come up with the plan and identify response activities.
- Continue dishing out factual information, giving the IR team time with each additional piece of information to develop a plan and prepare a list of their response activities.

Claims Management

Who is the first person(s) to contact when an internal cyber incident/breach is identified?

Your company's internal IT professionals or contracted IT service provider should be involved first, since they will be most familiar with the system and able to identify and contain the breach, so it doesn't spread and cause further damage to your business. If you can disconnect affected devices from the Internet, do so. Nothing should be done that will destroy valuable evidence that can be used to identify the entry point and formulate a plan to prevent it from happening again. Once emergency response and prevention have been taken care of, or while they are in the process of being addressed, the company's insurance provider should be contacted, via the claim reporting protocols outlined in the policy or on the declarations page of the policy, in order to trigger coverage.

Who is the first person(s) to contact when a third party/client alleges liability in cyber incident/breach?

Your insurance provider should be contacted immediately, via the claim reporting protocols outlined in the policy or on the declarations page of the policy, in order to trigger coverage. A claim representative and (most likely) counsel will be assigned to assist in the response to the allegations. Similar to professional liability claims, you should not admit any wrongdoing or do anything to compromise your defense.

Should I pay a ransom? Is it legal to pay a ransom?

- At this time, there is no federal legislation or law that prohibits the payment of a ransom, the only exception being the OFAC-sanctioned entities.
- Ultimately, it is a corporate decision whether to pay, but from a legal standpoint in the U.S., it's the OFAC-sanctioned entities we need to be concerned about regarding the legality of payment.

Should a company get a Bitcoin wallet for that rainy day?

- We do not advise that firms get a Bitcoin wallet, because these Bitcoin wallets are not FDIC insured. Since there is no regulated industry, there is no regulatory standard. If the wallet gets hacked and Bitcoins are siphoned out before or during an incident, it would be a total loss.
- Further, if an extortion payment must be made, a provider retained would have the ability to facilitate the payment on your behalf, and they would absorb the risk of their own Bitcoin reserve being stolen.
- If you need to make a payment, engage a professional payment facilitator and ransom negotiator through external resources (i.e., your insurance carrier) that would help you through that process.

Contact

Dan Buelow
Managing Director, Willis A&E
Architects and Engineers Center of Excellence
+1 312 288 7189
dan.buelow@willistowerswatson.com

Willis Towers Watson hopes you found the general information provided in this publication informative and helpful. The information contained herein is not intended to constitute legal or other professional advice and should not be relied upon in lieu of consultation with your own legal advisors. In the event you would like more information regarding your insurance coverage, please do not hesitate to reach out to us. In North America, Willis Towers Watson offers insurance products through licensed entities, including Willis Towers Watson Northeast, Inc. (in the United States) and Willis Canada Inc. (in Canada).

About WTW

At WTW (NASDAQ: WTW), we provide data-driven, insight-led solutions in the areas of people, risk and capital. Leveraging the global view and local expertise of our colleagues serving 140 countries and markets, we help you sharpen your strategy, enhance organizational resilience, motivate your workforce and maximize performance. Working shoulder to shoulder with you, we uncover opportunities for sustainable success – and provide perspective that moves you. Learn more at wtwco.com.

wtwco.com/social-media

WTW42250/04/2022

wtwco.com