BANK OF AMERICA

Cyber Insurance

Know the basics before getting started

Technology has changed the way the world does business, fueling tremendous growth and economic advancement. Business risks, in particular, cyber risks, have grown exponentially, hand in hand with this technology-fueled growth. From malware, ransomware and phishing to network outages, data exposure and human error, it seems that not a week goes by without hearing of another cyber event. In fact, the average number of security breaches has grown 67% in the last five years to an average of 145 breaches in 2019 alone.[1]

Five-year increase in security breaches

Compounding the growth in breaches is the rising cost of remediation, with the cost of a data breach rising 12% over the past five years to $3.92 million on average.[2]

Rising global concern over this trend is evidenced by the World Economic Forum's 2020 Global Risks Report, in which **750 global experts and decision-makers named cyber attacks and data fraud or theft within the list of top 10 global long-term risks.**

Be prepared

Preparedness is key when it comes to cyber security and cyber insurance plays a key role in protecting businesses. Yet according to one cyber insurance expert, **while companies never question the need for property or casualty insurance, many continue to question the need for cyber insurance** despite today's technology-driven world.

A security event can have wide-reaching impacts, such as business interruption, regulatory fines and loss of client confidence. **One of the best ways to protect your business is a strong cyber security program to prevent a cyber event from happening in the first place,** but it is equally important to be prepared for how to protect your business when/if a cyber event happens.

Best practices

As you explore the world of cyber insurance possibilities, keep in mind a few best practices:

- Know your unique risks
- Understand the current and evolving threat landscape
- Use a sophisticated insurance broker who understands the marketplace, the risks and your business
- Have the right internal subject matter experts involved in policy evaluation (legal, risk, IT, etc.)
- Involve outside legal counsel, where appropriate
- Carefully evaluate policies and providers — not all coverage is created equal
- Understand what is and is not covered by your existing business insurance

Average data breach cost

$3.92 million

What exactly is cyber insurance?

According to *CIO*, "a cyber insurance policy, also referred to as cyber risk insurance or cyber liability insurance coverage (CLIC), is designed to help an organization mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach or similar event."[3]

You insure your business, but did you know that policy might not cover a cyber event?

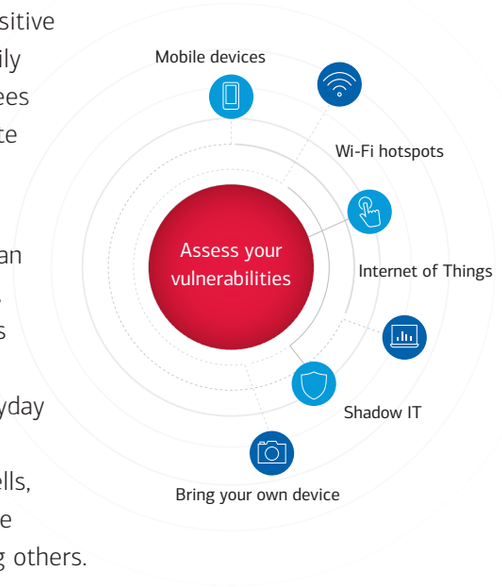
Cyber insurance has been available since about 2005, but **with cyber crime projected to cost businesses $5.2 trillion in potential future revenue opportunities worldwide in the next five years,**[4] companies should review policies and consider whether coverage meets business needs.

Understanding the threat landscape

In an ever-changing world of technology, you can't effectively protect your business if you don't adequately understand the risks you face. **Every industry has unique threats, so as you begin to explore cyber insurance, a good first step is taking the time to understand your threat landscape.**

Cyber security experts point to several key factors that influence the threat landscape:[5]

- **Shadow IT** — Put simply, Shadow IT is when business functions use applications or other IT solutions that have not been approved by the IT department. As noted by one expert, IT cannot manage what it cannot see…discovering Shadow IT is critical.[6]
- **Mobile and flexible working/Bring your own device** — Mobile and flexible working, as well as allowing employees to use their own device, is a perk for employees and undoubtedly saves employers money, but the potential for an inadvertent compromise via use of unsecure Wi-Fi hotspots, lost/stolen devices or other compromises cannot be ignored. Public Wi-Fi networks are simple to sabotage, and sensitive information is easily lost when employees lack the appropriate security training.[7]
- **The Internet of Things** — More than just smart phones, the term describes the smart devices embedded in everyday objects including appliances, doorbells, lights and wearable technology, among others.



Types of coverage

Cyber insurance policies can vary greatly, so understanding the products that exist is key to ensuring your business is adequately covered. **You don't want the surprise of finding out that the coverage you have will not support as intended after a breach occurs.**

Like the Internet itself, the cyber insurance market is continually evolving, but coverage is comprised of two main types: **first-party coverage** and **third-party coverage.** First-party coverage insures against the direct impact of a security breach on the policyholder, whereas third-party coverage protects the policyholder from claims made by others as a result of a breach. When making your assessment, it is critical that you and the insurer understand what you want and need in a policy.

Coverage needs will vary depending on the types of data involved, the size of the company and the type of cyber event, so it is important to understand what exactly a policy covers. As noted in *Forbes*, "…some cyber insurance may not protect against insider threats such as fraud or employee theft…" and "…nation-state threats that may be considered acts of war, which might make them covered under the federal Terrorism Risk Insurance Program and exclude them from general cyber insurance coverage."[8] These are all points you will want to clarify with a provider.

Keeping all of this in mind, industry sources suggest the importance of coverage that protects against three main risk areas: privacy, information and operations. Let's look at a few key types:

- **Network security/breach response** — This type of policy provides coverage for the costs a company might incur to manage its response to a network security issue, investigating the cause and getting the business back up and running. This may include coverage for and access to legal counsel, credit monitoring services, public relations and crisis-management counseling, IT forensics, notification to customers and setting up a call center, among other things.
- **Network and business interruption** — If your network goes down, it will more than likely have an impact on your revenue. Network Business Interruption coverage protects your business from some forms of lost income, as well as the extra expenses incurred due to a security event. This coverage can protect you against losses not only from incidents triggered by cyber criminals but also from those that are the result of human error.
- **Information security and privacy liability** — Many states are enacting laws protecting individuals against exposure of personal customer or employee data, which can create a huge liability for your organization. Information Security and Privacy Liability coverage protects a company against the damages related to a breach. This may include legal fees associated with defending against litigation, as well as paying settlements and regulatory fines. Coverage may also extend to the company's vendors who may have been impacted by the breach.

- **Cyber extortion** — Cyber extortion is the act of cyber criminals demanding payment through the use of or threat of some form of malicious activity against a victim, such as business email compromise, ransomware or denial of service attack.[9] According to the International Risk Management Institution's (IRMI) website, **cyber extortion insurance covers extortion payments and the cost of hiring computer security experts to prevent future extortion attempts, as well as professionals to deal/negotiate with cyber extortionists.**[10] IRMI advises that similar protection may also be available under kidnap and ransom policies.

- **Errors & omissions** — Errors & omissions insurance protects against liability for committing an error or omission in performance of professional duties. Technology Errors & omissions insurance covers providers of technology *services* or *products for l*osses resulting from technology services, technology products, media content and network security breaches. Both types of coverage offer protection to a business that is unable to perform its services because of a cyber security issue.[11]

Ask questions...lots of them

As you research cyber insurance coverage, you will likely have many questions — and you should ask all of them. **Potential providers are your best source for answers; the most important questions can be thought of as falling into three main areas — who is covered, what is covered and how extensive the coverage.**

Key areas to ask questions about include:

- The types of cyber incidents covered (hacking, ransomware, human error, data breach, etc.)
- Coverage exclusions and limits (dollar amount, timeframe, first party vs. third party, domestic-only incidents or global, etc.)
- Who the policy covers (vendors, suppliers, customers, etc.)

[1] Accenture "Ninth Annual Cost of Cybercrime Study," March 2019

[2] Ibid

[3] Kim Lindros and Ed Tittel, *CIO*, "What is cyber insurance and why you need it," May 4, 2016

[4] Sherri Davidoff, "Data Breaches: Crisis & Opportunity," Addison-Wesley Professional, 2020, pages 361–362

[5] Dave Shepherd, *CSO*, "Cyber security in the cloud: so many 'flying blind'," February 3, 2020

[6] Stuart Sharp, *TechRadar.pro*, "Remote workers prime targets for cyber attacks," February 2020

[7] Brad Noe, *Forbes,* "What to Know About Cyber Insurance," November 27, 2019

[8] "Cyber Extortion: An Industry Hot Topic," no date, Center for Internet Security, http://www.cisecurity.org

[9] International Risk Management Institution, no date, https://www.irmi.com/term/insurance-definitions

[10] Ibid

BANK OF AMERICA