How cyber insurance can enable business continuity.

As the scope and sophistication of cyber threats evolve, organizations of all sizes struggle to keep up. Cyber-attacks are becoming more sophisticated, with potentially severe financial consequences. Data breaches alone cost U.S. companies an average of $7.91 million in 2018, an increase of 7.6 percent over 2017. American firms also pay an average of $1.76 million in post-data breach response activities – the highest cyber crime figure in the world.[1]

While cyber threats facing middle market businesses are multifaceted – web-based attacks, ransomware, malware, compromised devices, phishing and distributed denial of service (DDoS) attacks – all have the potential to cripple an organization. Consumer data breaches receive the lion's share of media attention and have the potential to disrupt organizations by causing substantial financial and reputational damage. However, a recent cyber attack with massive implications has been far less reported: business interruption or continuity – the threat to a company's ability to keep the business up and running.

System disruptions from cyber-attacks can represent a substantial financial loss, even for companies that have invested heavily in proactive defenses and their cyber risk technology infrastructure. Those most potentially at risk are organizations whose core revenue is derived from creating and distributing products and remaining operationally available (e.g., manufacturers, e-commerce firms, logistics-dependent providers in the transportation space, etc.) or businesses that are highly data-reliant.

The potential scale of business continuity disruptions was underscored by the 2017 NotPetya incident, a watershed moment that exponentially increased awareness about cyber threats and business continuity. Called "the most devastating

[1] 2018 Cost Of a Data Breach Study

cyberattack in history" by WIRED magazine, it resulted in over $3 billion in net financial losses from interruptions to multiple companies' shipping, logistics and production cycles. NotPetya demonstrated that business continuity events have the potential to be just as severe, if not worse, than high-profile data breaches, and drove home the potential scale of financial damage.[2]

Evaluating and understanding cyber insurance

Cyber insurance policies address a wide range of costs incurred by an organization in connection with a cyber-event.

- Policies also typically cover both losses incurred directly by the insured (e.g., lost revenue, data restoration, extra expense, event management, costs spent on potential customer notification, etc.) and those incurred in connection with the insured's potential third-party liability for damages, regulatory fines, etc.
- Policies can cover lost revenue and extra expense resulting from a supplier or vendor cyber event, which doesn't necessarily have to be tied to a malicious threat actor, and can include unplanned system outages.
- From a reputation standpoint, cyber insurance policies can also cover costs related to public relations and crisis management services needed in the aftermath of an incident, as well as ascertained brand damage.
- The media liability portion of a cyber insurance policy can protect against online defamation and copyright infringement losses.

Leading organizations know that a crucial component to any cyber preparedness plan is the use of specialty insurance to mitigate financial risk by helping to cover anticipated business disruptions.

One of the most important roles cyber insurance can play is providing the financial protection and risk transfer needed to continue moving the company forward rather than letting cyber risks keep it behind.

[2] The Untold Story Of Notpetya, the Most Devastating Cyberattack in History - Andy Greenberg

Determining your coverage needs: A three-step approach

Because cyber insurance policies are complex and not standardized, companies should seek professional advice when considering their options. Cyber specialists understand, match and align a business' exposures with the appropriate types of coverage. They can also determine how cyber coverage might overlap with other insurance lines, minimizing duplication and maximizing return on investment.

When working with specialists to evaluate their cyber insurance options, businesses should consider their cyber risk the way they consider any other risk exposure – something they can manage but never eliminate or eradicate completely. Businesses can better understand exposures and options to arrive at a coverage plan by adopting a three-step approach:

1. **Map Risks:** Map out the range and boundaries of risk exposure. What are the threats based on the nature of your business? What are your cyber risk vulnerabilities based on your market presence, what you produce, intended audiences, and your supply chain? What are your core risks?

2. **Quantify Threats:** To better understand the frequency and severity of cyber events that could impact your business, look at the financial cost of previous events in both your industry and more broadly. Also, try to quantify the potential impact of emerging risks or loss scenarios.

3. **Create an Integrated Plan:** Cyber insurance should be a key part of your broader organizational cyber security plan, integrated with technology investments, enterprise risk management, breach response plans and incident response. Assess how much risk your company can offload via insurance and how cyber insurance coverages (and costs) mesh with your overall risk posture and appetite.The recent shifts in the marketplace mean that exceptional research is required to ensure that coverages are up to date and meet your expectations. Services such as M&T Insurance Agency's due diligence review process can help support your efforts.

Achieving and maintaining resiliency

Once coverage is in place, companies should regularly review their cyber insurance policy to adjust for new threats, a necessity given the dynamic nature of cyber risk.

Your insurance broker should be keeping pace with these rapid shifts, anticipating your needs and acting as your advocate with insurance carriers. First and foremost, your broker should act as a business risk advisor, not just an insurance guru. Threat actors are constantly evolving, and if your cyber risk awareness and preparedness is not keeping pace, the negative impact on your business could be devastating.

The objective of any optimal organizational cybersecurity strategy should be resiliency. From a business continuity standpoint, being cyber resilient means having the ability to take a punch, stand back up and minimize loss, downtime and outages. Having the right cyber insurance coverage in place is a key component of this resiliency.

To learn more about Cyber Risk & Insurance coverages, contact M&T Insurance Agency today at 1-800-716-8314.