Risk Management Spotlight

Cyber Risk and Insurance
Managing Your Evolving Cyber Risks

Insurance options to address or mitigate security, privacy and crime exposures or liabilities

Across every business sector, digital technology plays an increasingly essential role in helping companies innovate and grow. More and more, a business’s technology capabilities are driving efficiencies and competitive advantage. However, as organizations adopt new technology, the scope and sophistication of cyber threats steadily grow. Firms in every industry are at risk, with new types of danger, intrusion and disruption emerging on a regular basis.

Attacks carry massive costs

Cyberattacks can lead to serious damage and enormous liabilities. They have the potential to disrupt operations temporarily – or even permanently.

Incidents can mean private data loss, damage to customer relationships and, ultimately, lost revenue. When a business is attacked, it also can face serious reputational injury and a multitude of legal exposures, cost burdens associated with wide-scale notification to partners and customers, and other expensive impacts.

On a global basis, breaches and their damages are consistently on the rise. Worldwide, the average total cost of a data breach in 2018 is $3.86 million, up 6.4 percent over 2017, according to a recent global study. However, expenses are far higher in the U.S. The same study found that data breaches cost U.S. companies an average of $7.91 million, an increase of 7.6 percent over 2017. U.S. firms also pay an average of $1.76 million in post-data breach response activities, the highest in the world.

---

1 2018 Cost of a Data Breach Study: Global Overview Sponsored by IBM Security and independently conducted by Ponemon Institute LLC.
2 Ibid.
Where do threats originate?

Cyber threats can come from outside an organization or inside a company, both intentionally and unintentionally. External threats that can arise from both individual hackers and organized criminals can include:

- Email scams (phishing, spear phishing, etc.)
- Ransomware
- Malware and malicious code
- Identity and password theft
- Distributed denial-of-service (DoS) attacks that render networks inaccessible to users

Internal threats (specifically, human error) can be just as dangerous. In fact, according to a recent study, individuals inside an organization were responsible for 45% of incidents when private or sensitive information was unintentionally exposed. Insider threats include:

- Untrained/negligent employees
- Malicious employees
- Lost or stolen devices containing sensitive information (smartphones, laptops, etc.)

Three ways to mitigate your cyber risk

Today’s best practices call for a proactive approach to assessing and mitigating your digital risks. When it comes to effective risk management, it’s critical to have a comprehensive, strategic blueprint in place that spells out your organization’s incident response plans to help ensure a rapid recovery.

1. Get smart on the issue
   Organizations need to know what their level of real-world vulnerabilities looks like and educate themselves on the impact cyber events can have on their business. This requires a comprehensive risk assessment that should include network intrusion testing. Organizational leadership should also be fully engaged in understanding the scope of cyber risk facing their business, and then later identifying and implementing mitigation solutions.

2. Create a two-part plan
   Companies should devise and implement both a comprehensive prevention plan and a continuity plan:

   Prevention: Working with a qualified security expert, companies should set up proactive defenses around their network, systems and data. Networks must be shielded from external intrusions by firewalls and other suitable technology. Moreover, businesses should take appropriate steps to prevent a full range of internal threats.

Ways to mitigate potential costs and damage include:

• Encrypting information that needs to be secured
• Creating and enforcing a record retention policy
• Regularly reviewing and updating security protocols
• Implementing training procedures to educate employees

**Continuity:** Organizations need to anticipate and walk through what could happen if various cyberattack scenarios take place. It’s important to understand the potential consequences of events of all kinds.

Equipped with this knowledge, companies should prepare a continuity plan that takes into account these consequences – and be prepared at all times to deploy it.

If networks are disrupted, for example, the plan needs to address how the business will manage impacts on daily operations and revenue, spelling out the steps to restore network operations. The plan also needs to address public relations approaches for managing customer responses to an interruption in operations.

### The highest frequency of breaches occurred within these five sectors:

- **Financial Services**: 77
- **Services**: 71
- **Industrial Manufacturing**: 66
- **Technology**: 62
- **Retail**: 35

### The five sectors bearing the highest per capita costs

- **Health**: $408
- **Financial Services**: $206
- **Services**: $181
- **Pharmaceutical**: $174
- **Technology**: $170

---

**3. Protect yourself with insurance coverage**

As the final component in a comprehensive strategy, companies should work with an experienced insurance cyber risk specialist to explore all of their specialty insurance possibilities to mitigate their risks.

Despite some marketplace misperceptions, cybersecurity events are usually not covered by General Liability, Professional Liability, Umbrella Liability, Property, Crime, Directors & Officers (D&O) or Errors & Omissions (E&O) policies. Indeed, many of these types of policies affirmatively exclude cyber risk.
Leading organizations are increasingly turning to dedicated cyber insurance policies as a risk mitigation option. Cyber insurance is designed to cover a wide range of costs incurred by an organization in connection with a cyber event. Cyber events are wide ranging in scope; some examples include:

- **Data breaches** resulting in the loss of personally identifiable information
- **Technology-related outages** resulting in lost revenue and extra expense
- **Vendor or cloud service provider outages** or cyber incidents impacting the insured
- **Fines and penalties** relating to non-compliance with a privacy regulation

Coverage in connection with such cyber events should account for both first-party and third-party losses.

First-party losses impact the insured. Losses might include, for example, the costs incurred for notifying customers whose credit card data was stolen and paying for credit monitoring services for them. First-party losses also include lost revenue, extra expense incurred in the aftermath of a cyber incident, and system failure.

Third-party losses impact other people or groups, which the insured in turn may be liable for. This type of coverage helps protect the insured if, for example, customers sue for damages arising from the data theft and regulatory actions.

Cyber insurance policies can also help companies manage reputational damage by covering costs related to public relations and crisis management services needed in the aftermath of a data breach. Additionally, the media liability portion of a cyber insurance policy will cover online defamation and copyright infringement losses.

Cyber insurance policies typically do not cover costs to improve technology or security following an incident, future revenue losses, or the lost value of first-party (i.e., the insured’s) intellectual property (IP). However, such policies do intend to cover the lost value of third-party IP.

Companies should have their cyber insurance coverage reviewed regularly to adjust for new threats.

Cyber criminals and other opportunists aren’t just targeting enterprise-level organizations. Small businesses are often perceived as easier to infiltrate because their systems are usually more vulnerable and porous. In 2017, **47% of small businesses suffered at least one cyberattack**, according to insurer Hiscox. Of those, **44% experienced two to four attacks**.

---

Four reasons to work with a cyber risk advisor when making insurance decisions

There are four compelling reasons why companies need professional advice when considering their coverage options:

1. **Experienced specialists are uniquely qualified to understand a firm’s specific exposures**—and then carefully match and align those exposures with the appropriate types of coverage. Businesses require the right mix of tailored coverage to protect themselves from potentially massive economic losses.

2. **There are no standardized cyber insurance policies on the market.** With so many differences in coverage options, experienced professionals are best qualified to clearly discern and explain the variations.

3. **The world of cybersecurity is changing rapidly.** Technology is evolving quickly, and the breadth of cybercrimes is steadily expanding. A specialist is in the best position to keep pace with these rapid shifts—and help ensure that coverage aligns with current threats.

4. **While most companies can benefit from cyber insurance,** there is sometimes a degree of overlap with other insurance lines. A specialist can help organizations identify coverage that minimizes duplication and maximizes return on investment.

Risk management as a competitive advantage

In almost every type of business, digital technology has evolved from a nice-to-have to a critical, strategic component of operations. Advanced technology has become essential for helping organizations function effectively and efficiently. Moreover, for most companies today, a firm’s digital capabilities have become central to their competitive advantage in the marketplace.

But with this rush of technology comes a surge of new risks. New systems, networks and devices now expose companies to an expanding range of vulnerabilities.

At MTIA, our deep experience, our skilled professionals and our proven processes make us the ideal partner to help any organization assess and mitigate cyber risk. Tap into our expertise to help protect your business, your stakeholders and your future.

For questions, please call 1-800-716-8314.