One click from chaos: what the risk manager should know about cybercrime and insurance coverage

Forensic & Integrity Services
Insurance & Federal Claims Services

October 2025

Shape the future with confidence

The better the question. The better the answer. The better the world works.

Imagine losing everything you've worked for — your systems, sensitive customer data, reputation in the market — in an instant. With one click, your entire digital infrastructure could be compromised. Sensitive information may be exposed, operations brought to a halt and your business left scrambling in the wake of possible financial and reputational ruin. This isn't a hypothetical scenario; it's a reality that organizations around the globe are facing with increasing regularity.

Cyberattacks have become everyday occurrences, wreaking havoc across industries and around the globe, increasing year over year. In a report published by SentinelOne,[1] it states, "35% of all attacks were ransomware, which increased 84% over the previous year," "Phishing attacks increased by 1,265% driven by growth of GenAI [generative artificial intelligence]" and "Cloud intrusions [i.e., unauthorized access or malicious activities within cloud computing environments] increased by 75% in 2023."

Every keystroke is now a potential vulnerability. Every digital transaction an entry point for malicious actors.

Why cybersecurity and insurance go hand in hand

The best defense against a cyberattack starts with robust cybersecurity measures. But even the most secure systems aren't impenetrable. That's why insurance for cyberattacks is critical — it helps organizations recover financially from cyber incidents and mitigates long-term losses. A strong cyber risk strategy doesn't just stop at prevention; it includes a well-crafted mitigation and recovery plan. Having risk mitigation strategies, such as duplicative servers, backups and mock attack simulations can be vital to the success of your program.

[1] "https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/

Recent cyberattacks: a stark reminder

These attacks don't just target small businesses, they hit giants, too. Between March and August 2021, one of the largest wireless carriers in the US suffered a massive breach affecting more than 76 million customers. Hackers claimed access to data from over 100 million users. Three years after the incident, the carrier agreed to pay $350 million in a settlement, the second-largest data breach settlement in US history (the largest was $700 million).[2]

Despite a swift response involving a cybersecurity firm, there was reputational damage due to the breach. News spread rapidly across media and cybersecurity blogs and the ramifications are still felt today.

Another large Fortune 100 retailer fell victim in 2013. Cybercriminals stole 40 million credit and debit card records and 70 million customer records. Beyond the $18 million settlement, the total estimated loss exceeded $200 million.[3]

Overall in 2024, the global average cost of a data breach was $4.88 million, a 10% increase over the previous year. The cost, frequency and severity of these attacks continue to trend upwards. Some forecasts even mention the cost of cybercrime potentially being $23 trillion annually by 2027.[4]

Beyond the financial impact of these losses, company brand reputations need to be considered. After a breach, it can be difficult to earn back the trust of customers and vendors. The fallout from these events can be tremendously difficult long after the attack.

Doom, gloom and the inevitable attack — what should risk managers do?

Pre-event preparation: planning ahead

Having a proactive plan is essential to reduce exposure and respond quickly:

- Review your insurance policies for potential gaps that may exist across your coverages: cyber, property, crime and ransom.
- Understand your insurer's requirements, including any pre-approved vendors or incident response procedures.
- Check your limits and sublimits, particularly for business interruption coverage for both your organization and how your policy responds if vital suppliers or customers are attacked.
- Verify what's covered or excluded under business continuity and cyber extortion provisions.

You were hit, what's next?

[2] https://www.strongdm.com/what-is/t-mobile-data-breach#:~:text=In%20August%202021%2C%20T%2DMobile,to%20access%20the%20IT%20servers.
[3] https://redriver.com/security/target-data-breach#:~:text=The%20Ultimate%20Cost%20of%20the,today%20to%20find%20out%20more.
[4] https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/

Post-event response: managing the fallout

What to do immediately:

- Notify your broker and insurer immediately to initiate the claims process.
- Hold leadership meetings to align on the scope of coverage and communication strategy.
- Activate your incident response and mitigation plan to contain further damage.
- Engage key stakeholders to coordinate recovery efforts.
- Notify clients and vendors transparently to maintain trust.
- Maintain clear communication to streamline the process and protect your reputation.

Essential materials include:

- A timeline of the breach and events
- A detailed incident report
- Documentation of affected systems
- Financial loss estimates

Finally, if you are planning to make a claim under your cyber coverage, what should you know?

Common issues in cyber claims

- Cyber claims lack a physical component of damage that many adjusters and insurers are used to dealing with. There is no way to touch or feel the damage, which can lead to a misunderstanding of the claim itself and the impact of the attack.
- It will be important to tell the complete story of the loss, how the intrusion happened, which systems were impacted, how long it lasted and what other aspects of your organization were affected.
- Reputational damage with customers in the market is difficult to quantify and prove to insurers.
- Linking the financial loss to policy provisions.
- Proving the cost of system replacement as it was vs. system upgrades that are needed post-loss to prevent further attacks. There can be provisions in your policy regarding this and the coverage needed.

Hiring experienced claim consultants can help you navigate the complex terrain of documentation, investigation and negotiations. Keep in mind, the claims process is often lengthy and may involve multiple rounds of information requests and forensic reviews. The scrutiny is intense and the effort is resource-heavy, especially when your organization is trying to get back on its feet post-attack.

Ernst & Young LLP (EY US) contacts

Allen Shank
Partner
Forensic & Integrity Services,
Insurance & Federal Claims Services
Ernst & Young LLP
+1 214 969 8932
allen.shank@ey.com

Michael Schilling
Senior Manager
Forensic & Integrity Services,
Insurance & Federal Claims Services
Ernst & Young LLP
+1 312 879 3050
michael.schilling@ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

2507-11535-CS
ED None
US SCORE no. 28441-251US

ey.com