

Cybersecurity Risks & Social Media

Managing Threats Through Risk Management and Insurance

What is cybersecurity and digital environment risks?

- Cybersecurity is the practice of protecting our computer systems, digital networks and environments and digital information
- Cybersecurity risks involve threats to these systems and networks. These risks target information, data, systems and networks
- Increased digital connectivity (accessing internet, mobile networks, and data exchange) leads to a greater cyber vulnerability
- Cyber incidents, such as attacks, can occur through human error unintentionally, or through intentional threats, as well as system failures.
- With these potential incidents, both company data, organizational information and personal information is at risk.

Common Cybersecurity Threats

Malware & Ransomware: Software used to extort money from an individual or organization by blocking access to their applications or files until a sum of money is paid to the attackers.

Phishing Attacks: A type of attack where attackers use impersonation to trick persons into revealing sensitive information or to click on something that will allow attackers to infiltrate systems.

Data Breaches: An incident where sensitive or confidential information/data, is viewed, accessed, stolen or exposed by an unauthorized entity.

Insider Threats: A cybersecurity risks originating from inside a company or organization (i.e. an employee) who misuses their access to data and information to cause harm to a person or the company either maliciously or unintentionally.

Distributed Denial-of-Service (DDoS): An attack where attackers use a compromised computer to mob or flood a server with heavy internet traffic disturbing network availability.

Social Media Risks

Social media has its own cybersecurity risks, as it creates a new and evolving platform with thousands of everyday users. These users are often unaware of the possible risks when they use these applications. Users risk having their accounts hacked into and having their personal information exposed, as well as getting fraudulent messages putting their personal devices at risk.

Some social media cybersecurity risks include:

Oversharing: Revealing personal or company details (locations, schedules, internal processes) that attackers can exploit.

Social Engineering: Hackers impersonate trusted individuals to manipulate users.

Impersonation & Fake Accounts: Criminals create fraudulent profiles to scam followers or damage reputation.

Reputation Damage: Negative posts, leaks, or viral misinformation can harm brands quickly.

Exposure of Sensitive Media: Screenshots, photos, or videos that reveal confidential data.

Cybersecurity & Social Media Scams Targeting Individuals

Social media platforms have become a primary vector for cyber threats, enabling a constant barrage of targeted scams against individual users. These threats exploit psychological vulnerabilities, from urgency and trust to financial incentive, across all demographics. This slide examines the prevalent schemes that compromise user security and financial well-being.

Phishing & Spear Phishing: Attackers send personalized messages with links to malicious websites or fake login portals to steal credentials.

Impersonation & Account Takeover: Creation of fake profiles of friends, family, or companies to solicit emergency funds, gift cards, or sensitive personal data from connections.

Romance & Investment Scams: Sophisticated long-game tactics where threat actors build trust to coerce victims into sending money, often via cryptocurrency platforms.

Malicious Applications & Quizzes: Third-party social media apps or quizzes that require users to grant extensive permissions, leading to unauthorized data harvesting and privacy violations.

Business Impact of Cyber & Social Media Risks

Cyber and social media threats are increasingly problematic in that they can immediately or more slowly impact a business. Cyber events such as hacking, ransomware, and online theft can end up being major financial losses in terms of stolen data, system outages, and expensive restorations. These types of incidents can also lead to legal liability, particularly if customer data, financial statements, or sensitive information is exposed, which could bring fines, lawsuits, and additional regulatory attention.

Beyond the direct operational and legal consequences, organisations risk significant reputational damage. Stories can trend on social media in a matter of minutes, and negative stories go viral so quickly, it very quickly becomes damaging to a reputation. Once customer trust is gone, you may find it hard to restore it, and unspoken doubts might impact your customer's loyalty, relationships, and future business.

Introduction to Risk Management

Risk management refers to the systematic approach institutions employ to identify, assess, and respond to risks that present threats to the organization's assets. It makes sense to have a good cycle: Identify → Assess → Mitigate → Monitor. Make sure your risks are dealt with before they become serious problems. By planning ahead and predicting vulnerabilities, companies fortify defenses, enhance decision-making, and assure continuity and resilience for the long haul.



Cyber Risk Management Strategies

“Strong cyber hygiene is the first line of defense against modern threats.”

Key Strategies for Reducing Cyber Risks:

- Employee cybersecurity training to build awareness and reduce human error.
- Strong passwords and multi-factor authentication
- Regular software updates and patches
- Incident response planning
- Secure data encryption

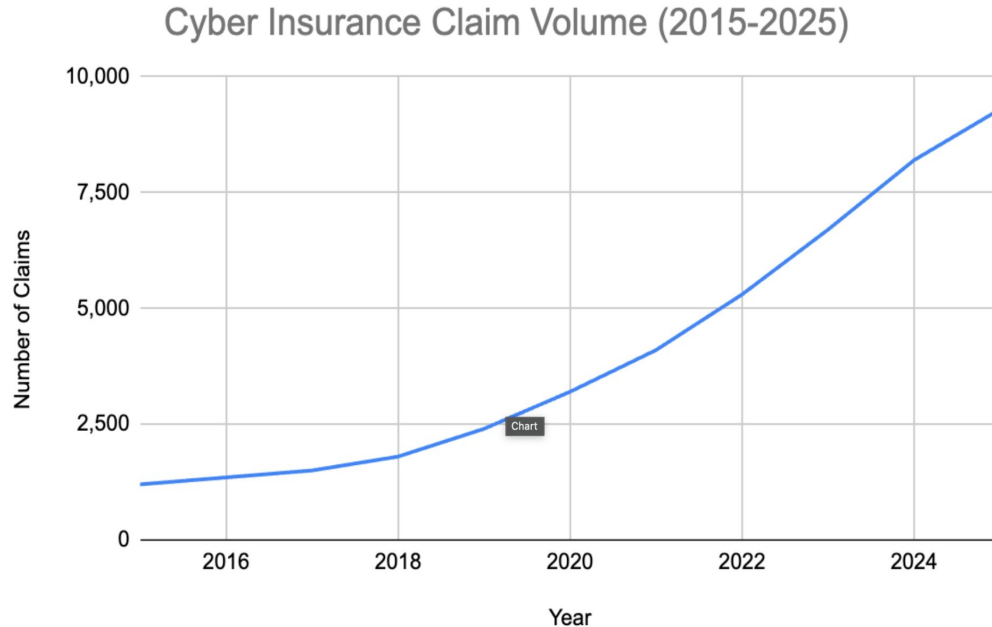
Role of Cyber Insurance

Cyber insurance is a proactive cybersecurity measure that provides financial protection during and after a cyber attack incident. Cyber insurance may also provide operational assistance to assist companies or organization with recovery after an incident.

A cyber insurance policy may:

- Cover incident response costs such as legal fees, forensic investigations and public relation costs
- Mitigate lost incomes by assisting with compensation for lost revenue
- Assist with data recovery and restoration of networks and systems
- Cover cyber extortion and ransomware demands
- Aid in regulatory compliance

The Rise of Cyber Insurance Claims



A graph from PNC Learning shows the drastic increase of cyber insurance claim volume from 2015-2025. The article on the rise of cyber insurance claims states “But it’s not just about more incidents, it is also bigger, more dangerous and expensive. Claim severity and frequency are at all-time highs. Insurers are taking an active role in risk management by offering ongoing monitoring and early attack detection, but when disaster strikes, recovery can still take years and cost millions.”

<https://pnclearning.com/2025/08/19/rise-of-cyber-insurance-claims/>

The Cost of NOT Being Insured

When an organization chooses to retain cyber risk without transferring it via insurance, it must bear the full financial burden of a security incident. The absence of a policy shifts catastrophic first-party costs and third-party liabilities entirely back to the balance sheet, threatening solvency and long-term viability. It could cost anywhere from hundreds of thousands to millions of dollars when someone or a business is not insured against cyber attacks. This shows the importance of having insurance against cyber attacks. Below are a few key costs that would be retained by a business that has been under cyber attack without being insured:

Financial Catastrophe: Out-of-pocket payment for forensic investigation, data restoration, and mandatory customer notification costs.

Legal & Regulatory Penalties: Retaining all expenses for defense and settlement of third-party lawsuits, as well as significant government fines.

Business Interruption: Unmitigated loss of revenue and profit during the system downtime and operational paralysis following an attack.

Reputation Damage: Long-term loss of customer trust and brand credibility, which is uninsurable and often the most expensive long-term consequence.

Cost-Benefit Analysis of Cyber Insurance

Cyber insurance enables businesses to mitigate the financial consequences of cyber incidents by covering expenses related to data breach response, legal issues, system restoration, and business interruption. Although premiums and coverage costs are great, with increased frequency and severity of cyber attacks, in most cases, the benefits surpass the costs. Cyber insurance offers financial protection, accelerates the recovery process, and can also enhance an organization's cyber strategy. By setting policy costs against the potential cost of losing out on a large breach, businesses can assess whether cyber insurance is a worthwhile investment for long-term stability.

Conclusion & Key Takeaways

Conclusion: The modern digital landscape, amplified by social media, presents a constant threat of cyber incidents that can lead to major financial losses, legal liability, and long-term reputational damage for organizations. Effective risk management is a cycle of identifying, assessing, and mitigating vulnerabilities. Ultimately, however, cyber insurance is a critical mechanism for financial risk transfer and operational resilience.

Key Takeaways:

Cyber Hygiene is the First Defense: Strong security measures, like employee training, multi-factor authentication, and regular updates, are essential for reducing the frequency of attacks and minimizing human error.

Social Media is a Critical Risk Vector: Platforms create unique cybersecurity risks, including oversharing, social engineering, and reputation damage, which must be specifically managed with governance policies.

The Cost of Retention is Catastrophic: Choosing not to be insured means bearing the full financial burden of forensic investigations, legal defense, and lost revenue, which can cost millions and threaten a business's solvency.

Cyber Insurance is a Financial Necessity: Due to the drastic increase in the volume and severity of cyber claims, a policy is necessary to cover high-cost incident response fees, mitigate lost income, and aid in regulatory compliance.