The escalating threat of cybercrime: A looming risk for businesses…

Takeaways from the recent Seminar on Professional Risks hosted by SICOM General Insurance Ltd., a subsidiary of the SICOM Group.

19 Septembre 2023

In a world where information and technology reign supreme, the rise of cybercrime has become an unsettling reality. Businesses, large and small, are under constant threat from a sophisticated network of hackers, ransomware operators, and phishing scammers. This report delves into the insights presented at a recent seminar hosted by SICOM, shedding light on the growing menace of professional risks posed by cybercriminals.

The soaring costs of cybercrime

In a stark revelation, the seminar highlighted that cybercrime is now more profitable than the global drug trade. Criminals are increasingly turning to the digital world to maximize their gains.

The financial toll of cybercrime is staggering. It costs more per year than all natural disasters combined. This underscores the dire need for robust cybersecurity protocols.

Understanding incident insights (Source: *Tokio Marine 2023 Cyber Report*)

In 2022, the distribution of cyber incidents was as follows:

- Data breaches accounted for 7% of incidents.
- Ransomware attacks constituted 9% of incidents.
- Business Email Compromise (BEC) fraud made up a staggering 84% of incidents.

The alarming state of email security

Statistic	Percentage
Companies harmed by ransomware attacks	66%
Collaboration tools posing security risks	75%
Expecting harm from collaboration tools (2023)	72%
Believe stronger protection is needed	94%
Companies targeted by email phishing	97%
Increase in email domain misappropriation	50%
Risk of data leaks by employees	80%

These statistics (source: *Mimecast - The State of Email Security 2023*) underscore the vulnerability of organisations to email-based cyber threats.

Assessing the cost of an incident

Cybercriminals are increasingly resorting to victim-shaming tactics, compounding the psychological distress of those affected.

The technical barrier for entry into cybercrime has significantly lowered, thanks to ransomware-as-a-service offerings that provide easy access to powerful hacking tools.

Attackers are increasingly leveraging zero-day vulnerabilities, making it imperative for organisations to stay ahead in terms of security updates.

The broader scope of cyber risks

Cyber risks extend far beyond data breaches. They encompass cyber extortion, malware attacks, denial of service, downstream attacks, hacking, insider misuse, physical theft, and threats posed by third-party access.

Incident response and its components

Effective incident response involves a multi-faceted approach, including incident triage, data recovery, forensics, legal guidance, crisis management, notification costs, remediation services, and addressing cyber extortion.

Financial impact: The financial consequences of a cyber incident can be dire, encompassing business interruption, increased operational costs, fines, penalties, theft of funds, and physical damage.

Liability concerns: Cyber liability encompasses defence, settlement, compromised data, environmental damage, and digital media liability.

Real-world claim examples

Insuring Tomorrow faced a double extortion ransom demand of $500,000 after hackers exploited a firewall vulnerability. The incident resulted in a loss of approximately $300,000.

Legally speaking attorneys fell victim to a phishing email, resulting in a fraudulent payment of $50,000. Their response efforts and loss totalled approximately $75,000.

Smiley Faces Dentists experienced a third-party cloud platform compromise, leading to a double extortion ransom demand of $1,000,000. Their loss amounted to approximately $150,000.

5 Key controls to strengthen cybersecurity

- Authentication: Implement multi-factor authentication and promote the use of complex passwords.
- Resilience: Ensure robust backup strategies, with immutable and disconnected backups.
- Patching: Keep systems and software up to date to address vulnerabilities.
- Endpoint security: Employ next-generation antivirus solutions, artificial intelligence, behavioural detection, and secure remote working protocols.
- Human firewall: Invest in employee awareness, training, and vigilance against cyber threats.

Anticipating 2023 cybersecurity trends

As we look ahead to 2023, several trends are poised to shape the cybersecurity landscape:

- Ransomware attacks will persist.
- Focused cyberattacks on specific targets will increase.
- Vulnerabilities will remain widespread.
- Business Email Compromise (BEC) attacks will surge.
- Deep fake attacks will gain prominence.
- Business interruption losses will rise, especially in (Internet of Things) IoT-related incidents.
- Remote and hybrid work setups will present challenges related to patching, authentication, and rogue connections.
- The rapid adoption of cloud technology will necessitate secure migration and configuration.

The imperative of effective incident response

In an era where cybercrime knows no boundaries, no business is immune. Cyberattacks are indiscriminate, and no security measure is infallible. Businesses must recognise the importance of effective incident response as the key to mitigating the devastating consequences of cyber threats. In a world where reputation and finances hang in the balance, the choice is clear: act now or risk becoming another statistic in the escalating world of cybercrime.

Insurance coverage: your safety net

Insurance coverage offers a lifeline in the face of cyber threats. It encompasses a comprehensive array of first and third-party coverages, including expert incident response processes. Specifically, insurance not only offers financial protection but also provides a structured response to minimise potential damage.