September 11, 2024

Update: Trends in Cybersecurity and Considerations for Boards of Directors

Cybercrime losses continue to surge in the United States. In its 2023 Internet Crime Report (the "**Internet Crime Report**"), the Federal Bureau of Investigation's ("**FBI**") Internet Crime Complaint Center showed that cybercrime loss surpassed US$12.5 billion in 2023, marking a 22% increase from 2022 and setting a new record.[1]

A recent FBI report highlights the following trends, among others: (i) investment fraud; (ii) business email compromise ("**BEC**") incidents; (iii) ransomware attacks; (iv) social engineering schemes; and (v) artificial intelligence ("**AI**") use to commit such crimes.[2]

This legal update discusses such trends and highlights various cybersecurity practices companies may consider.

Cybercrime Trends

I. Investment Fraud

Investment fraud resulted in the highest reported losses among cybercrimes, reaching US$4.57 billion in 2023 — a 38% increase from the previous year.[3] In these schemes, cybercriminals deceive victims with promises of high returns, ultimately stealing their money.

Within this category, crypto-investment fraud losses rose to US$3.94 billion in 2023, up 53% from the previous year.[4] Attackers targeted cryptocurrency investors by claiming expertise or connections with reputable figures who could guarantee financial success. Advanced technologies, including AI, allowed fraudsters to create convincing investment platforms and use AI to impersonate company executives.

II. Business E-Mail Compromise

In 2023, BEC became the second-most prevalent cyber threat to Americans, with losses exceeding US$2.9 billion. BEC cybercriminals usually compromise an employee's business email account, access sensitive data, and then use the account for fraudulent purposes. They often impersonate the account holder to deceive users and businesses into making unauthorized fund transfers or disclosing corporate information.

BEC cybercriminals frequently target businesses and financial institutions that handle large wire transfers and use email for related communications.

The Internet Crime Report stated that BEC cybercriminals increasingly persuade targets to transfer funds to accounts at financial institutions used for cryptocurrency exchanges or third-party payment processors, making it harder for victims to recover their money.

[1] Federal Bureau of Investigation, Internet Crime Report 2023 [*Internet Crime Report*].
[2] *Ibid.*
[3] *Ibid.*
[4] *Ibid.*

Sangra Moller LLP
1000 Cathedral Place
925 West Georgia Street
Vancouver, BC Canada V6C 3L2
Tel: (604) 662-8808
Fax: (604) 669-8803
www.sangramoller.com

III. Ransomware

Ransomware attacks caused losses exceeding US$59.6 million in 2023.[5] Cybercriminals use ransomware to encrypt a company's data, rendering it and the system unusable. These attacks often begin through email. When a recipient opens a ransomware email, it can disrupt services, cause financial losses, and sometimes lead to permanent data loss. Even if a company pays the ransom and recovers its data, cybercriminals may threaten to disclose the encrypted data to extort additional payments.

IV. Social Engineering: An Overall Theme

Cybercriminals increasingly rely on social engineering tactics. By impersonating executives, vendors, or even romantic partners, they create a sense of urgency and exploit the victim's trust. Socially engineered attacks are rising, as human behaviour remains the weakest link in the security chain and an easy target for cybercriminals.

V. Looking Forward: Artificial Intelligence

AI enhances cybercriminals' schemes by speeding up, scaling, and automating cyber-attacks. Cybercriminals use both publicly available and custom AI tools to run highly targeted phishing campaigns. These AI-driven phishing attacks create convincing messages tailored to individual recipients with accurate grammar and spelling, increasing the chances of successful deception and data theft.

Beyond traditional phishing, malicious actors use AI-powered voice and video cloning to impersonate trusted figures like family members, co-workers, or business partners. For example, scammers who compromised a real estate company's email account used AI to redirect wire transfers to fraudulent accounts after a closing.[6]

Mitigating Practices

Companies, directors and their executives can face liability if they fail to establish adequate and reasonable cybersecurity measures.[7] Accordingly, companies' cybersecurity programs must be defensible in the wake of a breach.

To mitigate cybersecurity risks, individuals and companies should consider the following practices:

I. Technical and Training Solutions

Companies should explore various technical solutions to reduce phishing and social engineering emails and text messages targeting employees. In addition to implementing technical measures, ongoing employee education should focus on the risks associated with phishing and social engineering. Training should stress the importance of verifying the authenticity of digital communications, especially those requesting sensitive information or financial transactions. Companies should also urge caution with investment opportunities, particularly those involving cryptocurrencies.

II. Multi-Factor Authentication

Companies implementing multi-factor authentication ("**MFA**") add extra layers of security, making it harder for cybercriminals to access accounts and systems. With the growing trend of funds being sent to third-

[5] *Ibid.*

[6] FinCEN Analysis of Business Email Compromise in the Real Estate Sector Reveals Threat Patterns and Trends | FinCEN.gov

[7] *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996).

party payment processors, using two-factor or multi-factor authentication is crucial. Companies should also ensure that MFA is genuinely "multi-factor" and not tied to systems commonly compromised, such as email or devices.

III. Verify Payment and Purchase Requests

Companies with business emails should verify payment and purchase requests by making a secondary direct call to a known, verified number. Business email users making payments should avoid relying on the information or phone numbers included in the email communication that prompts these requests.

IV. Document and Validate

Companies should document their cybersecurity programs and conduct regular audits or assessments to ensure effectiveness, compliance with legal requirements and proper functioning. Periodic internal reviews and incident response exercises, including tabletop and "red team" drills, should be facilitated to evaluate the effectiveness of their systems.