Cyber-risks & Liabilities

Courtesy of **RS Risk Solutions Ltd**

Understanding Cyber-criminals: Motivations, Methods and Protection Strategies

Cyber-attacks can impact an organisation in numerous ways. They can create significant financial losses through regulatory fines and business interruptions, and they can cause reputational damage as clients and stakeholders lose trust in the company. As technology evolves, cyber-criminals are able to conduct more sophisticated attacks. However, understanding different types of cyber-criminals' motives and methods of attack can inform the protective measures employers may take to prevent damage to their businesses.

Cyber-criminal Motivations

There are many types of cyber-criminals, and their motivations vary. The following are examples of these threat actors:

- **Hackers** seek to infiltrate computer systems and networks by exploiting vulnerabilities and moving through networks once they gain unauthorised access. They may do so for financial gain, recognition or the challenge.
- **"Script kiddies"** is a term for inexperienced individuals who use pre-written scripts or other tools without understanding their underlying technology. They often engage in cyber-crimes for the thrill or recognition.
- **Insiders,** such as employees or contractors, have access to sensitive information. They misuse their privileges to steal data or sabotage computer systems. Their motives may include financial gain, revenge and coercion through blackmail, and their malicious activity may be difficult to detect.
- **"Hacktivists**" are individuals who use hacking to further political or social agendas. They often deface websites, leak sensitive information and disrupt services to draw attention to their cause.
- **State-sponsored hackers** are cyber-criminals backed by governments. They may use advanced persistent threats, espionage and sabotage to procure classified information and pursue their geopolitical goals.
- **Identity thieves** steal personal information for financial gain by impermissibly accessing client information.
- **Cyber-terrorists** are individuals or groups who seek to advance political or ideological goals. They may target critical infrastructure, looking to spread fear and chaos and create financial damage.

Cyber-criminal Methods

Threat actors utilise various methods to carry out their cyber-crimes. Tactics they use include:

- **Phishing—**This type of cyber-attack involves using fraudulent communications (eg emails) to trick users into revealing confidential information after they click on a malicious link or open a harmful attachment. Threat actors such as hackers, script kiddies, identity thieves and state-sponsored actors use this technique because it is relatively low cost and exploits psychology rather than technical vulnerabilities. It can also be more easily deployed on a large scale.

- **Social engineering—**These attacks are manipulative techniques where individuals are tricked into divulging confidential information. Phishing is a type of social engineering tactic, as is baiting, where a threat actor tempts users with an offer (eg a free prize) to lure them into giving up sensitive data. Social engineering exploits human trust and curiosity. Insiders might use this technique for sabotage or data theft, while hackers and identity thieves use it to bypass technical defences by preying on human error.

- **Malware deployment—**Cyber-criminals deploy malware, or malicious software (eg viruses and ransomware), designed to provide access to a computer system or disrupt it in several ways, such as phishing emails, compromised websites or infected downloads. Once loaded, malware can spread within networks. It can provide long-term access to the compromised system, be used to steal data and be leveraged to extort businesses. Malware is versatile; hackers may use ransomware for financial gain, while state-sponsored actors could use it for espionage or sabotage. Cyber-terrorists might deploy malware to disrupt critical infrastructure, and identity thieves could use it to steal personal information.

- **Denial-of-service (DoS) attacks—**Threat actors carry out a DoS attack to overwhelm systems or networks with traffic. This can cause significant business disruption and serve as a distraction from other attacks. Hacktivists might use them to protest, cyber-terrorists for disruption and hackers for extortion, demanding ransom to stop the attack or restore services.

- **Credential stuffing—**This occurs when threat actors use stolen credentials to try to gain access to multiple services. This tactic exploits password reuse and can be automated for large-scale attacks to allow cyber-criminals access to accounts. This straightforward and automated approach makes it a popular choice for identity thieves and hackers looking to maximise return on their efforts.

Protecting Organisations

With knowledge of the motivations and methods of various cyber-criminals, organisations can design their cyber-security systems and strategies to thwart them. Measures to consider include the following:

- **Implement strong cyber-security measures** with multiple layers, including firewalls, antivirus software and intrusion detection systems. Organisations should also have strong patch management and software update procedures critical for closing vulnerabilities.

- **Educate employees** and develop a culture of security awareness. This can be accomplished by providing training on proper cyber-hygiene and common cyber-criminal tactics such as phishing and social engineering.

- **Utilise multifactor authentication** to strengthen access controls. It adds a layer of security beyond passwords, making it more difficult for cyber-criminals to gain access through stolen credentials. Employees should also be trained to strengthen passwords, keep them private and not reuse them.

- **Back up data** in secure places to prevent data loss. Organisations should consider storing their backup data off-site or in a cloud. This is critical for protecting against data loss from ransomware as well as other threats like hardware failure and natural disasters.
- **Conduct vulnerability tests** to identify weaknesses in cyber defences. These vulnerabilities can then be strengthened to make networks and systems more secure.
- **Create and maintain incident response plans** to quickly and efficiently respond to a cyber-security incident. Organisations should establish a crisis response team and regularly test their incident response plans.
- **Purchase cyber-insurance** to cover losses from a cyber-attack or data breach. Cyber-insurance can fill gaps left by other insurance policies, and many policies include benefits such as access to 24/7 support from cyber-specialists following a breach.

Conclusion

With the many types of cyber-criminals, there are various methods of attack and motivations that drive these attacks. However, by understanding this, organisations can position their cyber-security defences to prevent cyber-incidents from occurring and mitigate their impacts if they do. Contact us today for more information.