Cyber Risks & Liabilities

March/April 2023

Understanding Cyberespionage

Cyberespionage is a type of cyberattack that involves an unauthorized user (or multiple users) accessing a victim’s sensitive information in order to secure economic benefits, competitive advantages or political gain. Also known as cyberspying, the primary targets of such cyberattacks include government entities, large corporations and other competitive organizations.

Cybercriminals may leverage cyberespionage to gather classified data, trade secrets or intellectual property from their victims—which can be sold for profit or used to expose organizations. With this in mind, it’s crucial that your organization understands cyberespionage tactics and takes measures to mitigate such incidents.

Cybercriminals may engage in a variety of tactics to execute cyberespionage, such as:

- Exploiting security vulnerabilities in websites or browsers
- Utilizing phishing scams
- Bribing actual employees or contractors to share a target’s sensitive information in exchange for payment
- Injecting different forms of malware (e.g., Trojans and worms) within updates from third-party software applications

Safeguard your operations from cyberespionage by implementing strong cybersecurity measures, including:

- **Educating employees—**Train employees on cyberespionage and related prevention tactics, including phishing awareness and password management.
- **Protecting critical data—**Encrypt and store all critical data in safe, secure locations.
- **Restricting access—**Only permit employees to access technology and data when it’s specifically needed to perform their duties. Additionally, require multifactor authentication whenever possible.
- **Leveraging sufficient software—**Protect all workplace technology (and the data stored on it) with proper security software, including endpoint detection tools, antivirus programs and firewalls.

Finally, it’s critical to secure adequate insurance to help protect against losses from cyberespionage and other attacks. Contact us today for further risk-management guidance.

Case Insurance Brokers Inc.
336 Millwood Road
http://www.caseinsurance.ca

Ways to Protect Operations From Ransomware Attacks

Ransomware is a significant cyberthreat facing organizations of all types and sizes. In fact, 61% of Canadian organizations dealt with ransomware in 2021, according to a report from marketing and research firm CyberEdge. Unlike lone threat actors, ransomware groups often reinvest a portion of their profits into hiring and training talented cybercriminals, making them potentially more dangerous to organizations as time goes on. Protect your organization from ransomware attacks with these three tips:

- **Keep all software up to date**. Cybercriminals can exploit security vulnerabilities, so timely patching is one of the most efficient and cost-effective ways to minimize cybersecurity risks. If possible, automate software security scanning and testing to proactively spot any security flaws.
- **Require multifactor authentication (MFA).** Utilize MFA for as many services as possible, particularly access-critical systems. Further, require all accounts with logins to have strong, unique passwords.
- **Implement user training.** Train all staff on cybersecurity best practices. Phishing attacks can install ransomware, so raise employee awareness about the risks of visiting suspicious websites, clicking on suspicious links or engaging with phishing emails.

Contact us today for more guidance on ransomware attacks.

The Zero-trust Model Explained

Traditional cyber-security protocols often can’t keep up with the rapidly evolving nature of modern workplaces. In particular, the complexity of hybrid work arrangements, the rising number of fully remote employees and the dramatic increase in the use of cloud-based systems may make traditional perimeter security ineffective. Fortunately, a new security model, known as “zero trust,” is needed to keep corporate networks safe.

Rather than trusting the identity and intentions of users within an organization, a data breach is presumed with every request under a zero-trust approach. Consequently, every access request must be authenticated and authorized as if it originated from an open network. As such, a zero-trust model can help reduce an organization’s attack surface area and prevent lateral movement—where attackers are able to move freely within the organization’s perimeter once access is gained. This is especially important, seeing as lateral movement was observed in 25% of all attacks, according to a recent global report by cloud computing company VMware.

Consider these tips for adopting a zero-trust approach in your organization:

- **Define the attack surface**. To adopt a zero-trust framework, your organization’s critical data, assets, applications and services must be identified. This critical information forms a “protect surface,” which is unique to every organization.
- **Create a directory of assets**. Determine where your sensitive information lives and who needs access to it. Additionally, understand how many user accounts your organization has and where these connect. Consider removing old accounts and enforcing mandatory password rotation measures.
- **Adopt preventive measures**. Give users the least amount of access necessary to do their work and use multifactor authentication to verify accounts. Also, establish micro-perimeters to act as border control within the system and prevent unauthorized lateral movement.
- **Monitor continuously.** Inspect, analyze and log all data and consider analytics to improve visibility and enhance defences. Further, make sure your organization swiftly escalates and stores logs with anomalous activity or suspicious traffic.

By adopting a zero-trust approach, your organization can significantly reduce the risk of becoming a cyberattack victim and better secure its network, applications and data.

Contact us today for additional risk management guidance and insurance solutions.