All Companies Need Cyber Security and Cyber Insurance

Cyber threats affect all companies, regardless of their size or industry. Cyber criminals or malicious insiders conduct cyber-attacks aimed at accessing, changing, or destroying sensitive or proprietary information; extorting money from users (ex. ransomware); negatively impacting public image (ex. Data breaches); and/or interrupting normal business processes (ex. malware). Cyber security and cyber insurance are two aspects companies should implement to protect against such cyber-attacks.

Cyber security is the practice of protecting systems, networks, and programs from digital attacks. Having protection in place for computing systems helps protect companies and their employees from cyber threats, namely data breaches, which can result in operational disruption, damages to financial security, damage to reputation, and legal liabilities. Types of cyber security measures that companies can implement to protect their employees include the following:

- Network Security: Firewalls and intrusion detection systems
- Endpoint Security: Antivirus, malware, and data encryption software to secure end-user devices such as desktops, laptops, and mobile devices
- Password Policies: Use of complex passwords with length and character type requirements
- Multi-factor Authentications: Require users to provide two or more verification factors to gain access
- Security Awareness Training: Educate employees to help them identify and mitigate cyber-attacks and understand the role they play to help combat information security breaches.

Cyber insurance provides protection to mitigate the financial risk associated with cyberattacks, which often are not covered by commercial liability policies and traditional insurance products. The financial protection against damages caused by cyber incidents includes expenses for investigations; costs associated with data breaches; credit monitoring services; potential legal responsibilities; restoration of lost or damaged data; regulatory fines; and compensation for business interruption helps to offer financial security caused by cyber incidents. In addition, legal assistance is frequently included with cyber insurance, to help navigate the complex and dynamic nature of cyber incidents. While cyber insurance is applicable for businesses of all sizes across various industries, the extent of insurance coverage depends on multiple factors:

- Business industry or sector
- Company revenue and potential financial impact
- Employee and network size
- Geographical and remote presence
- Industry regulations
- Type of data and personally identifiable information
- Volume of sensitive data

As cyber security advancements continue to evolve, cyber criminals are also adapting to circumvent and defeat traditional safeguards. To prevent attacks and mitigate risk from such attacks, all companies should implement cyber security measures and subscribe to a cyber insurance plan. With both in place, good cyber security solutions will help reduce the cost of cyber insurance by minimizing the risk of experiencing a major cyber incident, reducing the likelihood of needing to make a claim, and helping keep premiums down in the future.