Essential Cybersecurity Controls for Organizations

As cyber incidents become more prevalent, it's vital for organizations to bolster their security posture. Doing so not only helps organizations prevent such incidents, but can also allow them to secure adequate cyber insurance. After all, many underwriters have begun leveraging organizations' cybersecurity practices to determine whether they qualify for cyber coverage. Here are some controls organizations can implement to manage their cyber exposures:

Multifactor authentication (MFA)–

MFA is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify their identity for login. It's best for organizations to enable MFA for remote access to their networks.

Endpoint detection and response (EDR) solutions–

EDR solutions record and store events from endpoints (e.g., smartphones, desktop computers, laptops and servers), utilize various data analytics techniques to detect suspicious system behaviors, provide contextual information, block malicious activities and offer remediation suggestions to help organizations restore affected technology.

Patch management–

Patches are software and operating system updates that address security vulnerabilities within programs and products. A consistent approach to patching and updating software and operating systems can help organizations limit their cyber exposures.

End-of-life (EOL) software management–

When software reaches the end of its life, manufacturers will discontinue technical support and security improvements for these products, thus creating vulnerabilities that cybercriminals can easily exploit. As such, EOL software management (e.g., having plans for introducing new software and phasing out unsupported products) is critical.

Remote desk protocol (RDP) safeguards–

RDP ports allow users to connect remotely to other servers or devices. Although these ports are useful, they can also be leveraged as a vector for launching ransomware attacks. To safeguard their RDP ports, organizations should keep these ports turned off when they aren't in use and ensure such ports aren't left exposed to the internet.

Secure data backups–

Organizations should determine safe locations to store their critical data, generate concrete schedules for backing up this information and outline data recovery procedures to ensure swift restoration amid possible cyber events.

Employee training–

Employees are widely considered organizations' first line of defense against cyber incidents, making cybersecurity training crucial. This training should occur on a regular basis and center around helping employees identify and respond to common cyberthreats.

For more cyber risk management and insurance guidance, contact us today.

SCS AGENCY INSURANCE