9 Controls to Know this National Cybersecurity Month

October is National Cybersecurity Awareness Month. During this annual event, government and cybersecurity leaders and the insurance community come together to raise awareness about the importance of cybersecurity.

It is important to remember that businesses must stay cyber-secure to safeguard company data, protect customers' personal information and ensure employee privacy. Here are 9 essential cybersecurity controls that organizations can implement to help manage their cyber exposures.

2024 marks the 21st annual **Cybersecurity Awareness Month.**

Endpoint Detection and Response (EDR) Solutions

EDR solutions record and store events from endpoint, 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.

Network Segmentation and Segregation

Network segmentation refers to dividing larger networks into smaller segments, whereas network segregation entails isolating crucial networks from external networks, such as the internet. Both processes limit the risk of cybercriminals gaining expansive access to organizations' IT infrastructures.

End-of-Life 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, 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.

Email Authentication

This technology monitors incoming emails and determines the validity of these messages based on specific sender verification standards that organizations have in place. Such technology can help keep potentially dangerous emails out of employees' inboxes.

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.

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. Organizations should enable MFA for remote access to their networks.

Employee Training

Employees are widely considered organizations' first line of defense against cyber incidents, making cybersecurity training crucial. This training should occur regularly 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

This document is not intended to be exhaustive, nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.