10 Essential Cybersecurity Controls

Cyber incidents—including data breaches, ransomware attacks and social engineering scams—have become increasingly prevalent, impacting organizations of all sizes and industries. Such incidents have largely been brought on by additional cyberthreat vectors and growing attacker sophistication. As these incidents continue to rise in both cost and frequency, it's crucial for organizations to take steps to address their cyber exposures and bolster their digital security defenses.

Doing so not only helps organizations prevent cyber incidents and associated insurance claims from happening, but can also help them secure adequate cyber coverage in the first place. After all, the heightened severity of cyber incidents has motivated most cyber insurers to increase their premiums and be more selective regarding which organizations they will insure and the types of losses they will cover. As such, many underwriters have begun leveraging organizations' documented cybersecurity practices to determine whether they qualify for coverage—whether it's a new policy or a renewal—as well as how expensive their premiums will be.

With this in mind, here are 10 essential cybersecurity controls that organizations can implement to help manage their cyber exposures.

1. Multifactor Authentication (MFA)

While complex passwords can help deter cybercriminals, they can still be cracked. To help prevent cybercriminals from gaining access to employees' accounts and using such access to launch potential attacks, MFA is key. 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. Through MFA, employees must confirm their identities by providing extra information (e.g., a phone number or unique security code) in addition to their passwords when attempting to access corporate applications, networks and servers.

This additional login hurdle means that cybercriminals won't be able to easily unlock accounts, even if they have employees' passwords in hand. It's best practice for organizations to enable MFA for remote access to their networks, the administrative functions within their networks and any enterprise-level cloud applications.

2. Endpoint Detection and Response (EDR) Solutions

EDR solutions continuously monitor security-related threat information to detect and respond to ransomware and other kinds of malware. They provide visibility into security incidents occurring on various endpoints—such as smartphones, desktop computers, laptops, servers, tablets, and other devices that communicate back and forth with the networks in which they are connected—to help prevent digital damage and minimize future attacks.

Specifically, EDR solutions offer advanced threat detection, investigation and response capabilities—including incident data search and investigation triage, suspicious activity validation, threat hunting, and malicious activity detection and containment—by constantly analyzing events from endpoints to identify suspicious activity. Further, these solutions provide continuous and comprehensive visibility into what is happening in real time by recording activities and events taking place on all endpoints and workloads. Upon receiving alerts regarding possible threats, organizations and their IT departments can then uncover, investigate and remediate related issues.

As a whole, implementing EDR solutions is a critical step in helping organizations enhance their network visibility, conduct more efficient cybersecurity investigations, leverage automated remediation amid potential incidents and promote more contextualized threat hunting through ongoing endpoint data analysis.

3. Patch Management

Patches modify operating systems and software to enhance security, fix bugs and improve performance. They are created by vendors and address key vulnerabilities cybercriminals may target. Patch management refers to the process of acquiring and applying software updates to a variety of endpoints.

The patch management process can be carried out by organizations' IT departments, automated patch management tools or a combination of both. Steps in the patch management process include identifying IT assets and their locations, assessing critical systems and vulnerabilities, testing and applying patches, tracking progress and maintaining records of such progress. Patch management is necessary to ensure overall system security, maintain compliance with applicable software standards set by regulatory bodies and government agencies, leverage system features and functionality improvements that may become available over time, and decrease downtime that could result from outdated, inefficient software.

From a cybersecurity standpoint, a consistent approach to patching and updating software and operating systems helps limit exposure to cyberthreats. Accordingly, organizations should establish patch management plans that include frameworks for prioritizing, testing and deploying software updates.

4. Network Segmentation and Segregation

When organizations' networks lack sufficient access restrictions and are closely interconnected, cybercriminals can easily hack into such networks and cause more widespread operational disruptions and damage. That's where network segmentation and segregation can help.

Network segmentation refers to dividing larger networks into smaller segments (also called subnetworks) through the use of switches and routers, therefore permitting organizations to better monitor and control the flow of traffic between these segments. Such segmentation may also boost network performance and help organizations localize technical issues and security threats. Network segregation, on the other hand, entails isolating crucial networks (i.e., those containing sensitive data and resources) from external networks, such as the internet. Such segregation gives organizations the opportunity to leverage additional security protocols and access restrictions within their most critical networks, making it more difficult for cybercriminals to penetrate these networks laterally.

Both network segmentation and segregation allow organizations to take a granular approach to cybersecurity, limiting the risk of cybercriminals gaining expansive access to their IT infrastructures (and the vital assets within them) and causing significant losses. When implementing network segmentation and segregation, it's imperative for organizations to uphold the principle of least privilege—only allowing employees access to the networks they need to perform their job duties—and separate hosts from networks based on critical business functions to ensure maximum infrastructure visibility.

5. End-of-Life (EOL) Software Management

At some point, all software will reach the end of its life. This means manufacturers will no longer develop or service these products, discontinuing technical support, upgrades, bug fixes and security improvements. As a result, EOL software will have vulnerabilities that cybercriminals can easily exploit.

Organizations may be hesitant to transition away from EOL software for a number of reasons, such as limited resources, a lack of critical features among new software or migration challenges. This is especially true when EOL systems are still functioning. However, continuing to use EOL software also comes with many risks, including heightened cybersecurity exposures, technology incompatibilities, reduced system performance levels, elevated operating costs and additional data compliance concerns.

As such, it's clear that proactive EOL software management is necessary to prevent unwelcome surprises and maintain organizational cybersecurity. In particular, organizations should adopt life cycle management plans that outline ways to introduce new software and provide methods for phasing out unsupported software; utilize device management tools to push software updates, certifications and other necessary upgrades to numerous devices simultaneously; and review the EOL status of new software before selecting it for current use to avoid any confusion regarding when it will no longer be supported and plan for replacements as needed.

6. Remote Desk Protocol (RDP) Safeguards

RDP—a network communications protocol developed by Microsoft—consists of a digital interface that allows users to connect remotely to other servers or devices. Through RDP ports, users can easily access and operate these servers or devices from any location. RDP has become an increasingly useful business tool—permitting employees to retrieve files and applications stored on their organizations' networks while working from home, as well as giving IT departments the ability to identify and fix employees' technical problems remotely.

Unfortunately, RDP ports are also frequently leveraged as a vector for launching ransomware attacks, particularly when these ports are left exposed to the internet. In fact, a recent report from Kaspersky found that nearly 1.3 million RDP-based cyber events occur each day, with RDP reigning as the top attack vector for ransomware incidents. To safeguard their RDP ports, it's important for organizations to keep these ports turned off whenever they aren't in use, ensure such ports aren't left open to the internet and promote overall interface security through the use of a virtual private connection (VPN) and MFA.

7. Email Authentication Technology/Sender Policy Framework (SPF)

Many ransomware attacks and social engineering scams start with employees receiving deceiving emails, such as those from fraudulent senders claiming to be trustworthy parties and providing malicious attachments or asking for sensitive information. To protect against potentially harmful emails, it's paramount that organizations utilize email authentication technology.

This technology monitors incoming emails and determines the validity of these messages based on specific sender verification standards that organizations have in place. Organizations can choose from several different verification standards, but the most common is SPF—which focuses on verifying senders' IP addresses and domains.

Upon authenticating emails, this technology permits them to pass through organizations' IT infrastructures and into employees' inboxes. When emails can't be authenticated, they will either appear as flagged in employees' inboxes or get blocked from reaching inboxes altogether. With SPF, unauthenticated emails may even be filtered directly into employees' spam folders. Ultimately, email authentication technology can make all the difference in keeping dangerous emails out of employees' inboxes and putting a stop to cybercriminals' tactics before they can begin.

8. Secure Data Backups

One of the best ways for organizations to protect their sensitive information and data from cybercriminals is by conducting frequent and secure backups. First and foremost, organizations should determine safe locations to store critical data, whether within cloud-based applications, on-site hard drives or external data centers. From there, organizations should establish concrete schedules for backing up this information and outline data recovery procedures to ensure swift restoration amid possible cyber events.

9. Incident Response Planning

Cyber incident response plans can help organizations establish protocols for detecting and containing digital threats, remaining operational and mitigating losses in a timely manner amid cyber events. Successful incident response plans should outline potential attack scenarios, ways to identify signs of such scenarios, methods for maintaining or restoring key functions during these scenarios and the individuals responsible for doing so.

These plans should be routinely reviewed through various activities, such as penetration testing and tabletop exercises, to ensure effectiveness and identify ongoing security gaps. Penetration testing refers to the simulation of actual attacks that target specific workplace technology or digital assets (e.g., websites, applications and software) to analyze organizations' cybersecurity strengths and weaknesses. In contrast, tabletop exercises are drills that allow organizations to utilize mock scenarios to walk through and test the efficiency of their cyber incident response plans. Based on the results of these activities, organizations should adjust their response plans when necessary.

10. Employee Training

Employees are widely considered organizations' first line of defense against cyber incidents, especially since all it takes is one staff mistake to compromise and wreak havoc on an entire workplace system. In light of this, it's crucial for organizations to offer cybersecurity training. This training should center around helping employees properly identify and respond to common cyberthreats. Additional training topics may also include organizations' specific cybersecurity policies and methods for reporting suspicious activities.

Because digital risks are everchanging, this training shouldn't be a standalone occurrence. Rather, organizations should provide cybersecurity training regularly and update this training when needed to reflect the latest threats, attack trends and workplace changes.

Conclusion

In today's evolving digital risk landscape, it's vital for organizations to take cybersecurity seriously and utilize effective measures to decrease their exposures. By leveraging proper cybersecurity controls, organizations can help safeguard their operations from a wide range of losses and reduce the likelihood of related insurance claims. Furthermore, documenting these controls can allow organizations to demonstrate to cyber insurers that they consider cybersecurity a top priority, potentially increasing their ability to secure coverage. For more risk management guidance, contact us today.