CTSI
TECHNICAL UPDATE
Volume 28 Number 14 | April 2, 2024

CYBERSECURITY CONTROLS: PART ONE

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 cyber threat vectors and growing attacker sophistication. As these incidents continue to rise in both cost and frequency, counties must take steps to address their cyber exposures and bolster their digital security defenses.

CTSI is presenting a three-part series on essential cybersecurity controls. April focuses on multifactor authentication, endpoint detection and response, and patch management. Future highlights include network segmentation and segregation, remote desk protocol safeguards, and secure data backups. Taking the time to review these risks and liabilities helps counties prevent cyber incidents and associated insurance claims from happening. It can also help secure adequate cyber coverage in the first place.

MULTIFACTOR AUTHENTICATION (MFA)

While complex passwords can help deter cybercriminals, they can still be cracked. MFA is key to helping prevent cybercriminals from gaining access to employees' accounts and using such access to launch potential attacks. 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. It's best practice for counties to enable MFA for remote access to their networks, the administrative functions within their networks, and any enterprise-level cloud applications.

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, 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. 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, counties and their IT departments can then uncover, investigate, and remediate related issues.

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 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. Counties should establish patch management plans that include frameworks for prioritizing, testing, and deploying software updates.

WHAT THIS MEANS FOR COUNTIES

CTSI recommends counties implement these essential cybersecurity controls to help manage their cyber exposures. Not only will it help safeguard and reduce digital vulnerabilities at the county level, but it will also assist in obtaining coverage with higher limits and lower premiums for CAPP. For more information, contact CTSI at (303) 861-0507.

County Technical Services, Inc.
Technical Updates are available online at ctsi.org
800 Grant St., Suite 400, Denver, CO 80203
(303) 861-0507 | Fax: (303) 861-2832