County Cybersecurity Support Guidance Package

April 2026

Administrative Office of the Pennsylvania Courts

Contents

Executive Summary

The *County Cybersecurity Support Guidance Package* provides a comprehensive roadmap for enhancing the cybersecurity posture of county-level government organizations, specifically those within the Commonwealth of Pennsylvania. It emphasizes pragmatic strategies tailored to entities with limited resources, offering a mix of best practices, tools, and collaborative opportunities to build resilience against evolving cyber threats.

At the heart of the guidance is the recognition that cybersecurity hinges on the CIA Triad: Confidentiality, Integrity, and Availability. This document underscores the importance of foundational cybersecurity principles and the shared responsibility across all organizational levels.

To address the resource constraints often faced by counties, the package highlights a suite of free and open-source tools across various domains including email authentication, malware analysis, log aggregation, operating system platforms, open-source intelligence (OSINT), and asset/vulnerability management. These tools enable cost-effective implementation of cybersecurity controls with minimal overhead.

This document also highlights the importance of collaboration and partnerships, identifying key organizations such as CISA, CIS, MS-ISAC, and others. These entities provide counties with various free or low-cost services, including threat intelligence, vulnerability assessments, training workshops, and security operations support.

A strong emphasis is placed however on cybersecurity best practices, structured around process maturity and technical structure. Counties are encouraged to:

- Formalize cybersecurity programs and incident response plans.
- Conduct regular assessments and simulations.
- Educate users and promote a culture of security.

The document outlines a defense-in-depth approach, segmenting protection across networks, endpoints, data, and applications. It advocates for layered defenses such as firewalls, endpoint detection and response (EDR), encryption, secure software development practices, and multifactor authentication (MFA).

Overall, the guidance package empowers counties to build sustainable cybersecurity programs through accessible tools, informed strategies, and collective efforts, positioning them to better defend against modern digital threats even with reduced direct and indirect support from federal partners.

Preface

In October 2023, the Kansas State Judiciary experienced a major disruption that starkly highlights the risks courts face from inadequate cybersecurity practices. What began as an internal investigation into strange network behavior quickly escalated into one of the most significant cyber incidents in the history of a US state court system.

The attack was confirmed to be a sophisticated foreign-led breach, resulting in unauthorized access to the court's case management systems, exfiltration of sensitive data, and weeks of downtime across key public services. For over five weeks, court staff, litigants, attorneys, and judges were forced to revert to manual, paper-based filing and scheduling processes, echoing operations from decades past. Electronic filing (eFiling), online case lookup, and document access were all suspended statewide. Hearings and procedural deadlines were delayed.

The post-incident investigation revealed numerous systemic issues:

- **Unpatched Systems:** Legacy case management software and aging operating systems lacked recent security updates.
- **Flat Network Architecture:** Once inside, attackers moved laterally across the court network without encountering segmentation or containment barriers.
- **Insufficient Monitoring:** Indicators of compromise went unnoticed for days, allowing data exfiltration to occur quietly.
- **Lack of Preparedness:** While staff were capable and dedicated, the court system lacked a mature cyber incident response plan, slowing mitigation and communication.

Approximately 150,000 individuals' data was potentially exposed, including sensitive court records, personal information, and sealed case details. While the attack did not involve ransomware or overt system destruction, the reputational damage, operational paralysis, and restoration costs were substantial. Chief Justice Marla Luckert, Kansas's top judicial official, issued a public apology and outlined the response and recovery needs:

"We're sorry anyone was personally impacted by the actions of the criminals who attacked our court computer systems. The judicial branch respects the privacy of information given to us, and it's a high priority throughout the court system to keep that information secure."

This was not an exotic threat. It was a clear reminder that court systems, like all public institutions, are attractive targets. The combination of sensitive legal data, tight deadlines, and public accountability makes courts uniquely vulnerable to cyber threats. The Kansas breach reveals how close the justice process can be halted when cybersecurity is underprioritized.

Lessons Learned

"Give a man a fish and you feed him for a day; teach a man to fish and you feed him for a lifetime." -Unknown

The foundation of cybersecurity is grounded on the principles of the CIA Triad: Confidentiality (data is private), Integrity (data is accurate), and Availability (data is accessible). Violations of any of these three attributes can result in a loss of trust in the system, leading to damage to organizational reputation and potential legal issues. For counties, this task can be challenging due to limited funding, industry knowledge, and/or a dedicated cybersecurity workforce. However, there are resources available that can enhance the effectiveness of cybersecurity efforts. These include the use of free/open-source software, the benefits of collaboration and partnerships, and the implementation of cybersecurity best practices.

With limited capital for cybersecurity and decreasing federal support, Free and Open-source Software and Tools have become more common among Small and Medium-sized Business (SMB) and State, Local, Tribal, and Territorial (SLTT) government institutions. These tools often require minimal hardware resources and a modest time investment, allowing IT professionals to enhance county IT programs and improve their security posture. Additionally, Professional Development and Training is important to develop the capabilities of existing and often devoted personnel.

Collaboration and Partnerships are essential in establishing and advancing a cybersecurity program. By pooling resources, organizations can enhance the effectiveness and impact of their cybersecurity measures. This collaborative approach offers various benefits, including increased awareness, improved information sharing, and access to advanced tools that may otherwise be inaccessible to individual entities. Many of these partners also supply valuable information in the form of different publications and frameworks to help start and mature an organization's cybersecurity program.

Finally, it is important to recognize that Best Practices can be researched and implemented at minimal cost beyond the necessary time to adapt the organization's cultural and technological mindset. Items that should be considered include but are not limited to endpoint protection, network architecture, incident response, 3rd party agreements, and policies/procedures. It should be emphasized that *cybersecurity is a collective responsibility,* not solely that of IT personnel. By advocating for this mindset within an organization and facilitating this paradigm culture shift, business and cybersecurity best practices such as disaster recovery plans and incident response procedures become more feasible to implement and sustain.

Software and Tools

"Give us the tools, and we will finish the job." -Winston Churchill

Threat actors possess a variety of tools that can be employed to compromise a system. Conversely, defenders can leverage similar tools or utilize diverse forms of free, open-source software and tools to enhance their cybersecurity measures. Accordingly, the services listed below are valuable additions to a County IT department's cybersecurity arsenal. These tools and their documentation can be found through online searches via your preferred search engine. Note that some of these solutions may require extensive knowledge of a platform.

Email Authentication and Troubleshooting

Email authentication is essential for safeguarding organizations against phishing and other forms of email-based fraud. By implementing standards such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC), senders can verify their identity and ensure that only authorized sources are permitted to send emails on their behalf. Most email providers now mandate these records for sending emails to their users. Various free tools are available to assist organizations with their email authentication and general email troubleshooting, including:

- **MXToolbox** – Using a domain, IP, or hostname for a search, this tool can provide DNS results and check for record issues. In addition to these features, it can also check to see if an IP or host reputation is negative/blacklisted and resolve delivery issues.
- **dmarcian** – Although offering a paid service, dmarcian also offers numerous free tools such as SPF surveyors, DKIM validators, and DMARC inspectors. It even provides builders to help construct these records for an organization if none exist currently.
- **DMARCLY** – Similar to dmarcian, DMARCLY offers various tools for email authentication including record checkers and builders. In addition to this, it also offers a blacklist checker and an SPF/DKIM/DMARC wizard to have it ready in minutes.

Malware / URL Scanning and Analysis

The scanning and analysis of malware and URLs are essential elements of contemporary cybersecurity strategies, designed to identify and mitigate threats before they can affect systems or data. By proactively engaging in scanning and analysis of potential threats, organizations can substantially minimize the risk of malware infections, phishing attacks, and other cyber threats. A variety of freely available tools can accomplish these tasks, including:

- **ANY.RUN** – This is a free, online sandbox that lets you conduct an analysis into a file, program, or URL via an interactive sandbox. It can be utilized for detection and research of cyber threats in real-time, providing network traffic and active processes.
- **Hybrid Analysis** – A free malware analysis tool that can detect and analyze for threats via an uploaded file or URL. It utilizes CrowdStrike's reputable Falcon Sandbox as its analysis framework.
- **Site Safety Center** – Supported by Trend Micro, Site Safety Center is a tool that allows an individual to verify the safety of a URL that might be considered suspicious.
- **urlscan.io** – Much like Site Safety Center, urlscan.io is a sandbox for analyzing URLs, providing the domains/IPs of any redirects and a screenshot of the URL analyzed.
- **VirusTotal** – A browser-based tool that lets you analyze files, IPs, and URLs to detect malicious activity or if it is linked to any know breaches. Submissions are then shared with the cybersecurity community at large to raise awareness.

Log Aggregation / Security Information and Event Manager (SIEM)

Data collection is essential in cybersecurity, as logs offer a comprehensive view of an organization's security posture. Log aggregation, typically managed through a Security Information and Event Management (SIEM) system, allows organizations to respond to potential threats more swiftly, enhance incident response, and adhere to regulatory requirements. Several free and open-source SIEM solutions are available, including:

- **Graylog Open** – A self-managed log aggregation solution that can ingest just about every form of log from almost any device and view it in real-time. It is also capable of basic analysis and can be configured to alert administrators for system issues.
- **Logging Made Easy (LME)** – An application developed and supported by CISA that assists small and medium sized entities centralize log collection and enable real-time alerting. This is a great resource whether starting small or need to scale out.
- **Security Onion** – An application/appliance that can be used for threat hunting, network monitoring, and log management. Something advantageous to resource-strapped entities includes a Setup wizard that allows it to be built out in minutes.
- **Wazuh** – Another application/appliance that is used for threat prevention and log aggregation. In addition to functioning as a SIEM, the agents can function as XDR for workstations and servers. Cloud integrations are also available to ingest logs from.

Operating Systems (OS)

When approaching operating systems, there are various Linux distributions that solely exist for cybersecurity. These distributions are entirely built around the idea of cybersecurity, pre-

installed with dozens of tools that an IT department can use to mature their program. The two most well-known, cybersecurity focused operating systems are Kali Linux and Parrot Security OS. Both systems operate on a Debian-based Linux platform but require different hardware resources. They can also be run as virtual machines using a hypervisor. Kali Linux is primarily utilized for digital forensics and penetration testing. Parrot Security OS assists in identifying and evaluating vulnerabilities. Depending on the workforce's skills, either solution may be used to enhance a program's security posture by internal red teaming.

Open-Source Intelligence (OSINT)

Attackers today can amass a significant amount of information directly from the internet without needing to interact with an organization. This type of information gathering is known as Open-Source Intelligence (OSINT), which involves collecting and analyzing publicly available data. The same tools that attackers utilize for OSINT and reconnaissance can also be employed by County defenders to understand their public footprint and overall attack surface. Some examples of OSINT tools include:

- **BGPView** – A tool that can be accessed from any internet browser that lets you track BGP routing information and IP address data.
- **DNSDumpster** – A domain research tool that can discover hosts related to a domain.
- **Have I Been Pwned?** – A website that can be used to verify if an account has been comprised. By providing an email, it will check against disclosed breach libraries if the email appears and possibly to which third party provider and/or breach.
- **Open Threat Exchange (OTX)** – Maintained by LevelBlue, OTX is one of the world's largest threat intelligence sharing communities with over 450,000 participants from across the globe reporting on indicators of compromise and potential threats.
- **Shodan.io** – A network security monitoring tool that enables users to explore indexed internet-connected devices, complete with their operating system, version, IP, and more.
- **Talos** – A free service provided by Cisco, the Talos Intelligence Center is a one-stop-shop for researching into IPs, URLs, domains, SHA values of files, and more. Included with Talos is a vulnerability report feed and a dedicated page to Microsoft advisories.

Vulnerability / Asset Management

Consider the scenario of knights being assigned to defend a castle they have never seen. This situation is analogous to IT teams attempting to protect systems without an understanding of their environment. A fundamental aspect of cybersecurity is inventory and asset tracking, as one cannot defend assets that are not known. This principle also applies to vulnerability

management. There are several free, open-source tools available that can assist with these tasks:

- **Faraday Community** – An open-source Vulnerability Management console that consolidates the vulnerability process into a single dashboard. Automated scanners can also be created to ingest new vulnerabilities with identified assets.
- **Greenbone Free** – Built on OpenVAS (Open Vulnerability Assessment Scanner), this tool can run basic scans for possible misconfigurations and/or vulnerabilities on targeted assets and networks.
- **Nessus Essentials** – This tool provides in-depth vulnerability scanning for up to 16 IP addresses. Once installed, it can be stepped up into an enterprise plan simply to then be able to scan an entire enterprise automatically with live results.
- **Nuclei** – An open-source tool developed by Project Discovery; Nuclei is a high-performance vulnerability scanner that can utilize thousands of templates to assess for vulnerabilities within an environment. It also hosts a free, cloud variant of Nuclei.
- **Snipe-IT** – An open-source asset management tool that is free if it is self-hosted, complete with LDAP integration and HTTPS standard. This also is available in a cloud-based range with support for a small annual fee.

Professional Development and Staff Training

"There are no secrets to success. It is the result of preparation, hard work and learning from failure." -Colin Powell

A tool is only as effective as its user. Understanding the threat environment helps us safeguard our lives and organizations. Defending against new technologies or lacking system knowledge can be challenging. The global cybersecurity workforce shortage, which numbers in the millions, exacerbates this issue. To address this gap, both the federal government and private companies offer free training courses to equip staff with necessary skills for securing their organizations.

CISA Learning

As a natural evolution from the Federal Virtual Training Environment (FedVTE), CISA Learning is an online platform maintained by the Cybersecurity and Infrastructure Security Agency (CISA) that hosts hundreds of courses for free to SLTT organizations and other external entities. Vetted by the Department of Homeland Security, these courses cover Active Directory, coding, cybersecurity, incident response, networking, risk management, and more. As a feature of this platform, it creates a transcript for all its users and records all completed classes along with their cumulative learning hours.

National Cybersecurity Preparedness Consortium (NCPC)

Funded by FEMA and the Department of Homeland Security, NCPC is a collaboration of universities from across the US, including the University of Arkansas, Texas A&M, and Norwich University, that provide free cybersecurity courses for SLTT entities. Like CISA Learning, many courses are available online through self-paced modules, and there are also in-person training sessions for larger groups. These training sessions cover topics such as cyber ethics, disaster recovery, incident response, digital forensics, and information sharing.

SANS Institute

The SANS Institute, founded in 1989, aims to support organizations in reducing cyber risk through comprehensive training, certifications, and degree programs. While it offers paid services, SANS also provides free events such as forums, summits, workshops, and course demonstrations focused on cybersecurity and risk management. For more structured courses and certifications, SANS frequently extends discounts to members of state, local, tribal, and territorial (SLTT) entities. Additionally, SANS offers free resources including newsletters, podcasts, policy templates, and cybersecurity tools.

Other Third-Party Companies

In addition to the previously mentioned organizations, other large private-sector companies provide free introductory training in cybersecurity or tool expertise. These include Cisco's Networking Academy, Fortinet's FortiGate Essentials Training, IBM's SkillsBuild Cybersecurity course, and the entire Microsoft training platform. Other options include TryHackMe, which offers hands-on training in cybersecurity for all levels using real-world labs, and Cybrary, which provides over 50 courses of content, labs, and certification preparation with a free account.

Collaboration and Partnerships

"Coming together is a beginning, keeping together is progress, working together is success." – Henry Ford

In the current cyber landscape, SLTT entities face an innumerable array of threats. With a vast number of potential adversaries possessing varying levels of attack capabilities and resources, it can be challenging for a County IT department to defend against all known and unknown scenarios independently. To support this formidable task, numerous associations, groups, and organizations exist to help SLTT entities pool their collective resources and provide mutual support in protecting their systems and data.

Cybersecurity and Infrastructure Security Agency (CISA)

CISA is the operational arm of the US Department of Homeland Security responsible for understanding, managing, and reducing risk to the nation's cyber and physical infrastructure. They coordinate cybersecurity efforts and serve as a resource for government entities and critical infrastructure in the United States. CISA handles incidents such as multi-state ransomware attacks and AI-powered phishing campaigns, coordinating responses, sharing threat intelligence with industries, and shaping national cyber policy. Some services that CISA facilitates and provides at no cost to SLTT entities include:

- Cyber Hygiene services
    - External Vulnerability Scanning
    - External Web Application Scanning
- Cyber Priority and Resilience Assessments
- Cyberthreat Information and Automated Indicator Sharing
- Malware Analysis via Malware Next Gen (MNG)
- Vulnerability Assessments/Penetration Testing
- Tabletop Exercise Planning and Execution
- Stakeholder Training Workshops

Center for Internet Security (CIS)

CIS is a nonprofit aiming to "make the connected world a safer place" by developing best-practice content and offering cyber-defense services to public and private sectors. CIS supports the MS-ISAC and its members. From the well-known CIS Controls to Albert sensors detecting ransomware in US county networks, CIS offers a mix of standards and operational strength. Some free* services for SLTT entities via MS-ISAC membership include:

- CIS Critical Security Controls Framework
- Automated CIS Controls Assessment Tools
- Vendor Neutral Benchmarks and Guides
- Hardened Images
- General Risk Assessment Tools
- Community Forums

*As of October 1st, 2025, many of these products and services will only be available to paying members of the MS-ISAC. See below.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

The MS-ISAC, part of CIS and funded by CISA, focuses on preventing, protecting, responding to, and recovering from cyber threats for state, local, tribal and territorial (SLTT) governments. Its mission is to enhance SLTT cybersecurity through information-sharing, incident response, and free tools. With over 18,000 members, the MS-ISAC's communal defense model often prevents significant cyber incidents. However, due to budget impacts on CIS in May 2025, the MS-ISAC will begin charging membership fees. CIS provides several services, including:

- 24x7x365 Security Operations Center (SOC)
- Stakeholder Engagements and Webinars
- Cyberthreat Information Sharing
- NIST Cybersecurity Framework Assessment Tool
- Albert Network Monitoring and Management
- Endpoint/Managed Security Services (ESS/MSS)
- Malicious Domain Blocking and Reporting (MDBR)
- Nationwide Cybersecurity Review (NCSR) Assessment

Pennsylvania Cybersecurity Threat and Intelligence Communications Unit (PA CyberCom)

The Pennsylvania Cybersecurity Threat and Intelligence Communications Unit, also referred to as PA CyberCom, is the primary entity for promoting cybersecurity awareness throughout Pennsylvania. It serves as the central resource for cyber defense information sharing within the Commonwealth. Operated and maintained by the Pennsylvania State Police, PA CyberCom offers the following services:

- Coordinating information sharing/collaboration with Commonwealth entities
- Establishing a community of trust between the different entities of Pennsylvania
- Coordinating incident response when requested
- Conducting training to educate partners
- Pennsylvania-focused Threat Intelligence Listserv Email Group

National Center for State Courts (NCSC)

NCSC is a nonprofit organization that was founded to improve the administration of justice in state courts across the US. It provides research, consulting, education, and technology support to courts and justice system partners. It also helps enhance efficiency, transparency, and accessibility by developing best practices, offering data-driven insights, and supporting innovations such as case management systems and online dispute resolution. NCSC serves as a

national-level resource for policy guidance and collaboration, working with judges, court administrators, and government leaders to strengthen public trust and the rule of law. Available resources include:

- NCSC Library for best practices, reports, tabletop exercises, and more
- AI Sandbox to help courts evaluate AI tools
- Risk Assessments based on the NIST Cybersecurity Framework
- Education program to assist advancing court and justice leaders

County Commissioners Association of Pennsylvania (CCAP)

CCAP is a statewide, non-partisan membership association representing the elected officials of all 67 Pennsylvania counties. It serves as "the voice of Pennsylvania counties." By combining expertise and speaking collectively, CCAP assists counties in securing funding, shaping state policy, managing risk, and sharing best practices. Additionally, they offer a Technology Services segment that provides cost-effective technology services. Some services that CCAP facilitates and provides free to members include:

- Listserv Email Group for County IT Leadership
- Phishing Tool Exercises
- Cyber Assessments
- Strategic Planning
- Geographic Information System (GIS) Assistance
- Aggregate Agreement Program for Vendor Product/Service Cost-Savings

National Association of Counties (NACo)

NACo is a national, bipartisan organization that represents all 3,069 county, parish, and borough governments at the federal level. It advocates county priorities, promotes best practices, nurtures leadership, and aims to save taxpayer dollars by supporting nearly 40,000 elected officials and 3.6 million county employees. From a cybersecurity/IT perspective, NACo manages the County Tech Xchange, an online portal where county CIOs and CISOs can collaborate and innovate. Membership fees are based on a county's 2010 Census population data. The County Tech Xchange provides services such as:

- Listserv Email Group for County IT Leadership
- Community Forums
- Policy, Proposal, and Job Description Libraries
- Monthly Newsletters

- Stakeholder Webinars
- Member Surveys

Technology Council of Central Pennsylvania (TCCP)

Different from the other groups mentioned as it is cross sector, TCCP is a Harrisburg-based nonprofit membership association that serves as the regional tech chamber for 22 counties across the mid-state. Its mission is to "connect members and organizations to promote technology and fuel economic development." By convening the public, private, and academic sectors around shared tech interests, TCCP aims to keep talent, innovation, and contract dollars circulating inside Central PA. There is an annual fee for membership with TCCP, depending on the number of individuals that would be participating.

Some services that TCCP facilitates and provides include:

- Conferences and Showcases
- TechNet Networking Events
- Peer-Learning Groups
- Tech Leader Forums
- Discounts for Harrisburg University Classes

News Resources and Publications

"The only true wisdom is in knowing you know nothing."- Socrates

While significant awareness information can be acquired through the previous section of collaborations and partnerships, additional insights may be obtained from various publications and cybersecurity/IT-related news sources. These resources are invaluable for understanding current events, trends, and technologies. All the resources listed below are freely accessible and can be viewed using any web browser.

News Websites

- **Bleeping Computer:** Established in 2004, Bleeping Computer is an information security and technology news publication. It serves as a valuable resource by publishing articles on security threats and technological advancements, as well as providing tutorials on uninstalling malware and ransomware decryptors.
- **CyberScoop:** This channel is dedicated to reporting on news and events related to IT security and technology. Another variation, **StateScoop**, concentrates on technology within state and local governments.

- **Dark Reading:** Recognized as one of the leading cybersecurity news platforms, Dark Reading offers readers a wealth of articles and updates on current trends, vulnerabilities, attacks, and best practices. The content ranges from brief updates to comprehensive analyses, and the site also hosts virtual events and publishes surveys.
- **The Hacker News:** Widely recognized and frequently accessed, The Hacker News receives over 50 million visits annually. It offers a comprehensive range of cybersecurity information, from brief updates to in-depth analyses, similar to Dark Reading.
- **KrebsOnSecurity:** This blog is maintained by Brian Krebs, a former reporter for The Washington Post, and focuses on cybersecurity investigative reporting. With over a million views a month, KrebsOnSecurity provides detailed insights into various events or trends.
- **The Record:** Established in 2020, this platform is dedicated to reporting on cyber trends, events, and activities. The Record prioritizes the "democratization" of information, striving to be accessible to a broad audience while maintaining accuracy and truthfulness.

Podcasts

- **Cybersecurity Where You Are:** Produced by the Center for Internet Security, this podcast typically releases on Wednesdays and covers cybersecurity topics at a high level, reviews existing issues, and explores best practices.
- **CyberWire Daily:** A cybersecurity-news focused podcast released each weekday. The program features overviews of recent events, active research, new technologies, interviews with industry experts, conference coverage, and more.
- **Darknet Diaries:** This esteemed monthly podcast delves into the darker aspects of the internet, including hacktivism, cybercrime, and data breaches. It provides in-depth analyses and features interviews with industry experts and well-known hackers.
- **Priorities Podcast:** A weekly podcast published by StateScoop that discusses state and local government technology news, trends, and analysis with government executives.

Publications & Frameworks

- **NIST Cybersecurity Framework 2.0:** Also known as the NIST CSF, this framework provides a structured approach for organizations to manage their cybersecurity risk. It addresses desired outcomes from a strategic, high-level perspective. Additionally, it aligns well with CISA's Cybersecurity Performance Goals (CPG) assessment, which is

typically required if an organization wishes to pursue further activities in cooperation with CISA.

- **NIST SP 800-53 Rev. 5:** In contrast to the CSF, this publication emphasizes prescriptive, technical controls that can be implemented at the system or process level. For instance, it includes guidance on collecting logs that are reviewed weekly for anomalies. Addressing these elements helps achieve compliance with the NIST CSF or other strategic-level frameworks.
- **CIS Critical Security Controls:** The CIS describes the Controls as "a prescriptive, prioritized, and simplified set of best practices designed to enhance your cybersecurity posture." Similar to NIST SP 800-53 Rev. 5, this publication addresses organizational cybersecurity by recommending specific actions or maintaining certain statuses to ensure compliance across an environment.

Cybersecurity Best Practices

"It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it." - Stephane Nappo

In the constantly changing environment of digital threats, it is essential to adopt cybersecurity best practices to protect an organization's assets and maintain operational resilience. These practices can be designated into two categories: cyber-hygienic processes and the configuration of appropriate structures for controls.

Structure

When discussing cybersecurity best practices and structures, a layered approach proves to be highly effective. One critical method for bolstering an organization's resilience against potential cyber incidents is the "defense-in-depth" strategy. Like the layered defense mechanisms of a castle which include elements such as a moat, walls, and a keep, securing technology infrastructure necessitates the use of firewalls and antivirus programs. Beyond securing networks and endpoints, it is essential to protect an organization's data and applications. Furthermore, administrative controls such as policies, procedures, and standards should be implemented to enhance the security framework of an organization. The following sections expand on these concepts in greater detail.

Networks

Traditionally, the network would be considered the outer rim for an organization. To protect the network effectively, several key practices towards structure must be established. Using firewalls as a primary defense mechanism helps to block unauthorized access while allowing

legitimate communication to proceed. Web Application Firewalls (WAF) on the edge protect web applications from cross-site scripting and other vulnerabilities. Intrusion detection and prevention systems (IDS/IPS) are crucial for monitoring network traffic for suspicious activities and responding to potential threats in real-time.

Network segmentation is another essential practice, where the network is divided into smaller segments or subnetworks. This isolation minimizes the impact of security breaches, as attackers cannot easily move laterally across the network. Virtual Private Networks (VPNs) also play a significant role in securing remote access by encrypting data transmitted over the internet, making it inaccessible to unauthorized parties. Email authentication standards like Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC) should be established to protect the integrity of the brand, prevent abuse by attackers, and ensure delivery of emails.

Endpoints

Securing endpoints, which include devices such as laptops, desktops, and mobile devices, is a critical component of a comprehensive cybersecurity strategy. Implementing endpoint protection measures involve deploying antivirus and anti-malware software, which can detect and neutralize threats before they can compromise the system. Regularly updating and patching software on all endpoints is essential to fix vulnerabilities that could be exploited by cyber attackers.

Moreover, enforcing strong authentication mechanisms, such as MFA, adds an additional layer of security by ensuring that only authorized users can access sensitive data and systems. Endpoint detection and response (EDR) solutions are also invaluable, as they provide continuous monitoring and analysis of endpoint activities, enabling rapid detection and response to potential threats. Mobile device management (MDM) policies and systems can also be implemented to maintain compliance and secure configurations for mobile devices.

Data

Data protection is vital in the overarching structure of cybersecurity. Data, often referred to as the crown jewels of an organization, requires a multifaceted approach to security. One of the primary methods of securing data is through encryption, which converts data into a coded form that is unreadable without the proper decryption key. Both data-at-rest and data-in-transit should be encrypted to prevent unauthorized access. Additionally, implementing strong access control mechanisms based on the classification of data ensures that only authorized personnel can access sensitive data, thereby reducing the risk of insider threats.

One of the most important concepts that an organization can implement for protecting data is backups. Regular data backups are essential, as they provide a recovery mechanism in case of data loss due to cyberattacks or other incidents. These backups should be immutable and stored securely, ideally in an off-site location or a cloud environment with robust security measures. Moreover, data loss prevention (DLP) technologies can be employed to monitor and control data transfer activities, ensuring that sensitive information does not leave the organization's secure environment without proper authorization.

Applications

Application security is a critical aspect of protecting an organization's digital assets and ensuring the integrity and confidentiality of its data. As applications become increasingly complex and interconnected, they also become prime targets for cyberattacks. One fundamental practice in application security is securing the software development lifecycle (SDLC). By integrating security measures at every stage of development, CISA's rallying cry of "Secure by Design," organizations can identify and rectify vulnerabilities early. This approach, known as DevSecOps, fosters a culture of security awareness among developers and ensures that security is not an afterthought.

Another crucial element of application security is the use of secure coding practices. This involves following established guidelines and standards, such as OWASP (Open Web Application Security Project) principles, to mitigate common threats like SQL injection, cross-site scripting (XSS), and insecure deserialization. Regular code reviews and static application security testing (SAST) can help identify potential security flaws before the application goes live. Additionally, dynamic application security testing (DAST) and penetration testing should be conducted to simulate real-world attacks and uncover vulnerabilities that might be missed during development.

Policies and Procedures

In today's digital landscape, robust cybersecurity policies and procedures are essential for protecting organizational assets, sensitive data, and the overall integrity of information systems. These policies serve as a blueprint for expected behavior, roles, and responsibilities, helping ensure that all stakeholders are aligned in their approach to managing cyber risks. Without clear guidance, even the most sophisticated security tools can be undermined by human error or inconsistent practices.

One fundamental purpose of cybersecurity policies is to establish baseline expectations for system access, data handling, and incident response. For instance, an *Acceptable Use Policy* (AUP) outlines what users can and cannot do on the organization's electronic resources, helping

reduce the risk of malware infections or unauthorized data transfers. Similarly, password policies that require complex credentials and regular updates help prevent brute-force attacks and credential stuffing. These rules not only reduce vulnerabilities but also create a culture of accountability. Other examples of technology related policies can include but are not limited to an IT Security Policy, Vulnerability Management Policy, Data Breach Policy, Privacy Policy, and more.

Procedures complement policies by providing step-by-step instructions to implement security controls effectively. For example, a *Data Backup Procedure* ensures that critical files are regularly copied and stored securely, which is vital for recovery in the event of ransomware attacks or system failures. An *Incident Response Procedure* guides staff through identifying, containing, and recovering from breaches, helping to minimize damage and comply with regulatory requirements. When tested and updated regularly, these procedures can significantly reduce response time and improve outcomes during security incidents.

Ultimately, well-developed and consistently enforced cybersecurity policies and procedures are the strategic tools that protect an organization's digital ecosystem and foster trust among customers, partners, and regulators. Organizations that invest in formalizing and maintaining their cybersecurity framework are far better equipped to navigate the evolving threat landscape.

Processes

Adopting robust cybersecurity best practices is paramount for any organization seeking to protect its digital infrastructure against the ever-evolving landscape of threats. When considering best practices, various processes can be applied to enhance the maturity of a cybersecurity program. These can include but are not limited to:

- Establishing a Formal, Documented Cybersecurity Program
    - Creation of policies, procedures, and standards outlining the entity's program
- Defining Roles within the Organization for Incidents and Strategy
    - Designation of assignments via assigned duties to qualified staff
- Conducting Annual Vulnerability Assessments/Penetration Testing
    - Evaluation of the organization's attack surface and response capabilities
- Maintaining Strong Access Controls
    - Implementation of strong password policies and access is reviewed regularly
- Fostering an Environment of Awareness and Education
    - Simulation of phishing scenarios and mandated cybersecurity training

- Testing Incident Response, Disaster Recovery, and Business Continuity Plans
    - Operations are executed according to business needs and mission criticality

Special consideration must be taken when reviewing processes and implementing them for the purpose of cybersecurity. Many of the examples, as well as others, can have extensive impacts and implications on the business. These should be evaluated through a business impact analysis (BIA) conducted among stakeholders of affected systems and organization senior leadership.

To enhance existing processes or introduce new ones, they should be supported by actionable knowledge and intelligence regarding industry trends. Various sources and mediums can assist in these efforts, such as newsletters, whitepapers, podcasts, and threat intelligence channels like those provided by MS-ISAC and PACyberCom. Conducting interviews and meetings with business process participants is an effective initial step in mitigating resistance to cybersecurity initiatives, while also fostering relationships that can facilitate future projects.

Agreements, Contracts, and Memorandum of Understandings (MOUs)

As counties increasingly rely on shared services, state partners, and third-party vendors to strengthen cybersecurity, clear and well-structured agreements are a necessity. Contracts and Memoranda of Understanding (MOUs) play a critical role in defining expectations, managing risk, and ensuring accountability. In addition, counties should give special attention to third-party risk management and service level agreements (SLAs).

Cybersecurity language should not be an afterthought in procurement. Prior to starting any type of agreement, a county should consider the risk allocation i.e. is there more or less risk being transferred obtaining this product/service. Another acknowledgement should be that the agreement clearly defines its purpose and boundaries. Vague language increases risks during an incident, when time and clarity matter most. Agreements should specify the services being provided, the systems/data that are covered, and the duration of the agreement. Instead of using the catch all “industry best practices,” pursue language to maintain alignment with known cybersecurity frameworks or accreditations like the NIST CSF, the CIS Critical Security Controls, SOC, ISO, and other. This creates the foundation for measurable expectations.

Third-party risk is one of the most significant cybersecurity challenges an organization can face. To help reduce this risk, counties can attach a third-party agreement to a contract or questionnaire to be completed prior to services beginning. At a minimum, some of the items that should be evaluated are the vendor’s own cybersecurity program, their alignment with the previously mentioned recognized standards, their incident response capabilities, and their use of subcontractors/cloud services. Vendors that are generally considered to be of higher risk like

cloud hosting providers, public safety technology providers, and financial system operators should warrant deeper scrutiny.

SLAs transform general security expectations into measurable commitments. In cybersecurity contexts, this often includes time-to-detect and time-to-respond metrics, incident notification timelines, and system availability guarantees. Crucially, SLAs should not exist without consequences. Without accountability mechanisms, SLAs risk becoming aspirational statements rather than operational guardrails.

Insurance

Integrating cybersecurity insurance into an organization's risk management framework is crucial for mitigating the financial and operational impacts of cyber incidents. While technical controls and user training are vital elements of a robust security posture, insurance serves as an additional layer of protection by providing financial reimbursement and access to specialized response resources following incidents such as ransomware attacks, data breaches, or system outages. As part of a county's formal cybersecurity program, evaluating and procuring cybersecurity insurance should be treated as an ongoing process, aligned with annual risk assessments and incident response planning. Counties are advised to engage with insurers proactively to understand policy terms, coverage exclusions, and required security controls such as multi-factor authentication (MFA), logging, and documented incident response plans. Through organizations like the County Commissioners Association of Pennsylvania (CCAP), counties can join the Pennsylvania Counties Risk Pool (PCoRP) program to obtain cybersecurity insurance coverage at stable prices.

Maturity Model and Self Assessments

A cybersecurity program should be dynamic, evolving through ongoing evaluation and refinement. Counties are advised to use a maturity model framework to guide the structured development of their cybersecurity capabilities over time. Maturity models such as the NIST Cybersecurity Framework (CSF) or CIS Controls provide a tiered approach for assessing a county's current status. Regular self-assessments using these models help counties identify strengths, uncover gaps, and prioritize improvements based on available resources and risk exposure. Tools like the CISA Cybersecurity Evaluation Tool (CSET) or the CIS Risk Assessment Tool can assist in performing these evaluations at no cost. By institutionalizing periodic maturity assessments, counties can align cybersecurity investments with strategic goals, demonstrate progress to stakeholders, and ensure that policies, controls, and response capabilities remain relevant in an evolving threat landscape.

Cybersecurity Incident Response (IR)

An effective incident response is crucial in the current landscape. Within emergency management, incidents may encompass a range of events including facility fires, neighborhood flooding, loss of essential utilities, nuclear meltdowns, or cyber-attacks. Although many incidents typically follow a similar path to resolution, this is not universally applicable. Given the increasing prevalence of cybercrimes and the heightened risks associated with emerging technologies, it is imperative for IT departments and courts to maintain comprehensive incident response plans. Regarding cybersecurity, a fundamental approach includes:

1. Preparation
    - Formulate IR teams, establish tools and procedures, develop checklists, and create communications and contact lists.
2. Identification
    - Identify and categorize deviations from typical behavior.
3. Containment
    - Control the situation to stop any more harm and collect information for later.
4. Eradication
    - Reimage or restore affected systems and continuously monitor for any further anomalies
5. Recovery
    - Address vulnerabilities that caused the incident and harden systems to prevent further attacks
6. Lessons-Learned
    - Evaluate actions taken and identify enhancements for future incidents.

During the incident response process, it is vital to consider available resources and follow reporting protocols. If your organization has cybersecurity insurance, it is imperative to notify the insurer immediately, as they should be the first external contact. Alerting other external parties beforehand may result in invalidating your coverage. The insurer can also provide legal and vendor support. Furthermore, it is essential to include key organizations that can assist on your Incident Response contact list, such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the United States Secret Service (USSS), and the Pennsylvania Army National Guard (PAANG).

Disaster Recovery and Business Continuity

When an incident escalates or significantly impacts an organization, necessitating a disaster recovery plan's implementation, it is crucial to differentiate it from an incident response plan. A

disaster recovery plan primarily focuses on how an organization will resume normal operations following a critical breach or impactful event. These plans adopt a comprehensive approach to cyberattacks and provide a detailed strategy for restoring services.

In contrast, business continuity typically involves an organization-wide initiative to ensure that operations and services can continue following a disaster or significant event. At the county level, this may be referred to as a Continuity of Operations (CooP) or Continuity of Government (CoG) Plan. Depending on the county's structure and size, the responsibility for maintaining this plan may fall under a public safety department like emergency management or an administrative department like risk management. Courts should also be cognizant, participating in their county's CooP/COG planning. Regardless of who maintains it, the IT department plays a crucial role in business continuity and should be integral to the development and implementation of a business continuity plan.

Tabletop Exercises

The best approach to verifying if a plan is appropriate in an incident is to rehearse it via a tabletop exercise (TTX). Used extensively by the emergency management sector for first responders and emergency personnel during man-made or natural disasters, these have now evolved to include numerous other possible scenarios like cybersecurity incidents and data breaches. In essence, a TTX is a guided scenario-based discussion that walks participants through the steps of responding to an event, testing personnel, processes, and communication. It is important for these exercises to be blame-free and realistic, while also being accessible to non-technical staff. Key stakeholders for a TTX include but are not limited to:

- President Judge
- Court Administration
- County Commissioners
- Chief County Clerk
- Public Information Officer or Communications
- Director of IT or Another IT Representative
- Sheriff's Department Representative (if physical security is included)

As for example scenarios:

- Ransomware outbreak encrypts internal systems and backups.
- Phishing campaign leads to credential compromise and data exfiltration.
- Third-party vendor breach exposes customer data.
- DDoS attack disrupts critical public services.

Following the scenario introduction and injections with responses, an After-Action Report/Hot Wash should be completed. This is perhaps the most important aspect of a TTX because it allows all the stakeholders involved to deliberate on the simulation and decisions made. Reflection on the overall performance and outcomes can help reveal inconsistencies, highlight outdated procedures, and identify other areas for improvement, leading to more successful plans and responses in the future. TTX information and templates are available from both CISA and the National Center for State Courts (NCSC) on their respective websites.

Afterword

Cybersecurity has become one of the most pressing responsibilities of local governments. As the stewards of your counties' digital infrastructure and services, you are on the front lines of defending not just systems, but the trust and continuity of local government itself.

This guidance package was designed with your realities in mind: limited budgets, small teams, and ever-expanding responsibilities. It acknowledges the complexity of your roles and offers a roadmap grounded in practicality, emphasizing free tools, strategic partnerships, and scalable best practices. More than anything, it reinforces this essential truth: progress is possible, even without extensive resources.

The tools and strategies included here are not theoretical, as they reflect what works in real county environments. Whether you are building a cybersecurity program from the ground up or enhancing an existing one, the lessons and frameworks provided can help you move forward with purpose and confidence.

However, technology alone will not ensure the security of your county. True resilience is attained through the commitment of both technical and administrative leadership to a unified vision. Your decisions establish the direction. By advocating for security awareness, investing in staff development, and endorsing structured processes, you create the foundation for long-term protection and responsiveness.

Cybersecurity requires ongoing effort. It is an iterative process of continuous learning, adaptation, and collaboration. It is essential to maintain ongoing dialogue, continually evaluate requirements, and strengthen relationships with colleagues and strategic partners. Through effective leadership, the counties of Pennsylvania can achieve not only enhanced security but also greater preparedness, unity, and resilience in addressing digital threats.