JOINT TECHNOLOGY COMMITTEE
COSCA | NCSC | NACM

Cybersecurity Basics for Courts

JTC RESOURCE BULLETIN UPDATED | SEPTEMBER 2025

Abstract

As cybersecurity threats become increasingly sophisticated and pervasive courts must recognize cybersecurity as a core component of judicial operations and public trust. Courts hold sensitive data and rely heavily on technology to deliver justice and serve the public, making them high-value targets for malicious actors. This bulletin provides court leaders, administrators, and IT staff with a foundational understanding of cybersecurity risks, terminology, and best practices.

Through plain-language explanations and practical recommendations this bulletin outlines steps courts can take to strengthen their cybersecurity posture including implementing least-privilege access, securing physical and digital infrastructure, managing vendor risk, developing response plans, and cultivating a culture of awareness across all personnel. It highlights key areas such as ransomware, phishing, incident response, zero trust principles, cloud security, and interagency coordination.

By following the guidance provided courts can build greater resilience, improve their preparedness for cyber incidents, and maintain continuity of operations while reinforcing public confidence in the justice system.

Document History and Version Control			
Version	**Date Approved**	**Approved by**	**Brief Description**
4.0	9/15/2025	JTC	Released updated document.
3.0	9/15/2021	JTC	Released updated document.
2.0	12/4/2019	JTC	Released updated document.
1.0	2/17/2016	JTC	Released document.

Suggested Citation: *JTC Resource Bulletin: Cybersecurity Basics for Courts* (Williamsburg, VA: National Center for State Courts, 2025).

Acknowledgments

This document is a product of the Joint Technology Committee (JTC) established by the Conference of State Court Administrators (COSCA), the National Association for Court Management (NACM), and the National Center for State Courts (NCSC).

JTC MISSION

> **The Joint Technology Committee is a nexus that provides trusted and actionable thought leadership, guidance, education, and training for court use of technology to enhance administration and access to justice.**

JOINT TECHNOLOGY COMMITTEE

COSCA Appointments

Stacey Marz (Co-Chair)
Alaska Court System

David K. Byers
Arizona Supreme Court

Megan LaVoie
Texas Office of Court Administration

Amy Quinlan
Maine Administrative Office of the Courts

Greg Sattizahn
South Dakota Unified Judicial System

NACM Appointments

Paul DeLosh (Co-Chair)
Supreme Court of Virginia

T.J. BeMent
Georgia 10th Judicial Administrative District

Roger Rand
Oregon Multnomah Circuit Court

Kelly C. Steele
Florida Ninth Judicial Circuit Court

Jeffrey Tsunekawa
Texas Office of Court Administration

NCSC Appointments

The Honorable Scott Schlegel
Louisiana Fifth Circuit Court of Appeal

The Honorable Samuel A. Thumma
Arizona Court of Appeals

CITOC Appointments

Casey Kennedy
Texas Office of Court Administration

Winnie Webber
Illinois 19th Judicial Circuit

Ex-officio Appointments

Jim Cabral
IJIS Courts Advisory Committee

NCSC Staff

Shay Cleary

Contents

Executive Summary

In today's digital landscape cybersecurity is no longer an optional concern for courts; it is a critical operational imperative. Cyberattacks targeting government systems–including the judicial branch–have increased in frequency, sophistication, and impact. Courts hold vast amounts of sensitive information and provide vital public services, making them high-value targets for malicious actors.

This bulletin is designed to help courts develop a foundational understanding of cybersecurity and equip judicial leaders, administrators, and IT professionals with the knowledge needed to improve cyber resilience. It outlines key concepts, best practices, and actionable steps to help courts prevent, detect, and respond to cyber threats.

Topics covered include:

- The most common types of cyber threats facing courts from ransomware and phishing to zero-day exploits and supply chain attacks.
- Organizational strategies such as forming a cybersecurity response team, maintaining updated incident response plans, and fostering governance through cross-functional collaboration.
- Best practices for system access controls, password and account management, multi-factor authentication, patch management, and vendor oversight.
- Importance of budget planning, staff training, and regular testing of cybersecurity policies and procedures.
- The often overlooked role of physical security, including secure device handling, endpoint protection, and mobile device management.
- Legal and compliance considerations such as breach notification obligations and privacy requirements under state and federal law.
- Guidance for effective communication with court personnel, the public, law enforcement, media, and victims in the event of an incident.
- Considerations for cloud and software as a service (SaaS) governance, including shared-responsibility models and contract review protocols.
- Forward-looking strategies like adopting zero trust architecture to enhance long-term security posture.

Cybersecurity is a shared responsibility. Everyone in the court system–from judges and clerks to public information officers and IT staff–has a role to play in protecting the integrity of court operations and maintaining public trust. By implementing the strategies outlined in this bulletin courts can build a stronger, more secure digital environment that supports justice and service delivery.

Introduction

In today's digital age courts are increasingly reliant on technology to manage records, conduct proceedings, and deliver essential services. With this growing dependence comes a heightened risk of cyber threats that can disrupt operations, compromise sensitive data, and erode public trust. Cyberattacks–whether opportunistic or targeted–are no longer rare anomalies; they are an ever-present risk that courts must proactively plan for.

Unlike private enterprises courts have unique responsibilities that include safeguarding confidential case information, protecting the rights of individuals, and maintaining the uninterrupted delivery of justice. These responsibilities make the judicial branch a prime target for cybercriminals seeking to exploit vulnerabilities for financial gain, political motives, or public disruption.

While there are no confirmed cases of cyberattacks altering court records to date, it is conceivable that such attacks could be used to manipulate judicial outcomes. For example, such attacks could aim to fabricate criminal records, modify case dispositions, or alter sentencing data. These potential threats underscore the importance of robust cybersecurity defenses, monitoring, and response protocols within court systems.

Why Cybersecurity Matters for Courts

Courts are prime targets. *Sensitive data and vital operations make the judicial system attractive to cybercriminals.*

Threats are constant. *Attacks range from broad, automated intrusions to highly targeted campaigns.*

Disruptions have serious consequences. *A breach can delay justice, expose confidential data, and damage public confidence.*

Preparation is key. *Understanding risks and planning coordinated responses enhances court resilience.*

Everyone plays a role. *Cybersecurity isn't just an IT issue – it involves judges, administrators, clerks, and staff at every level.*

The number, scope, and sophistication of cybersecurity incidents affecting public and private organizations continue to grow at an alarming rate. Courts are increasingly targeted with cybercriminals employing more advanced techniques such as ransomware, phishing, and supply chain attacks. Despite preventive measures most organizations–including courts–will experience some form of cybersecurity incident. Acknowledging this risk is the first step toward effective preparedness.

Cybersecurity Foundations for Court Leadership

This bulletin is designed to provide court leaders with a foundational understanding of cybersecurity risks and best practices. It outlines practical strategies for preventing, detecting, and responding to cyber incidents with an emphasis on building a culture of awareness and resilience across court personnel, IT teams, and administrative staff. The intent is not to transform judges or administrators into cybersecurity experts but to equip them with the knowledge necessary to foster secure environments and respond confidently when threats arise.

While numerous reputable organizations provide cybersecurity expertise, courts should begin with resources offered by four key U.S. government sponsored entities:

- **CISA (Cybersecurity and Infrastructure Security Agency)** is part of the U.S. Department of Homeland Security. CISA offers incident response services, risk assessments, cybersecurity tools, and timely alerts to help organizations prevent and mitigate cyber threats.[1]
- **NIST (National Institute of Standards and Technology)** is a federal agency that develops standards for industry and science. NIST's widely adopted Cybersecurity Framework provides standards, guidelines, and best practices that can be tailored to court systems of any size or technological maturity.[2]
- **CIS (Center for Internet Security)** is a nonprofit that develops globally recognized best practices for securing IT systems and data. CIS offers security benchmarks, configuration guides, and the CIS Controls—a set of prioritized actions to protect against common cyber threats.[3]
- **MS-ISAC (Multi-State Information Sharing and Analysis Center)**, operated by CIS and supported by CISA, serves as the key resource for cyber threat prevention, protection, response, and recovery for U.S. state, local, tribal, and territorial government entities. Membership provides courts with access to threat intelligence, security advisories, incident response support, and specialized tools at no cost.[4]

---

[1] Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). *CISA — Cybersecurity and Infrastructure Security Agency*. Retrieved July 28, 2025, from https://www.cisa.gov/

[2] National Institute of Standards and Technology. (NIST) (2025, July 18). *Cybersecurity Framework (CSF) 2.0* [Web page]. https://www.nist.gov/cyberframework

[3] Center for Internet Security. (n.d.). *CIS controls and benchmarks*. https://www.cisecurity.org

[4] Multi-State Information Sharing and Analysis Center. (n.d.). *MS-ISAC services and resources*. https://www.cisecurity.org/ms-isac

This bulletin introduces core cybersecurity concepts in plain language to help non-technical court personnel collaborate effectively with IT professionals and external partners responsible for their court's cybersecurity. It is intended as both a conversation starter and a catalyst for meaningful action.

Essential Terminology

A cybersecurity incident is defined as a past, ongoing, or threatened intrusion, disruption, or other event that impairs or is likely to impair the confidentiality, integrity, or availability of electronic information, information systems, services, or networks.[5] Cybersecurity incidents take many forms.

A cyberattack is a deliberate attempt–typically by malicious actors–to disrupt, damage, or gain unauthorized access to a computer network or system. A data breach (or cyberbreach) involves unauthorized access, viewing, use, or retrieval of sensitive, protected, or confidential information. Exfiltration refers to the successful transfer and theft of data from a system or network. See Appendix A for more detail on opportunistic and targeted attacks.

Common types of cyberattacks include:

- Malware and viruses
- Denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks
- Ransomware
- Zero-day exploits
- Unauthorized access, either by insiders (e.g., current or former personnel) or external threat actors, including nation-state actors and organized cybercriminal groups

Attacks may be targeted–specifically directed at a court or judiciary–or opportunistic–taking advantage of broader system vulnerabilities.

Hidden Costs of Cybersecurity Decisions

Cybersecurity incurs financial, convenience, and system performance costs. Court leaders often face difficult decisions about which security measures to implement. Decisions made tougher when coupled with the reality of limited resources. However, as recent attacks have shown, prioritizing convenience over security can have devastating consequences. Sound security practices and policies should not be compromised for the sake of ease.

---

[5] NIST. (2024, February 26). *Incident response playbook: Cybersecurity event definitions and guidance*. NIST Computer Security Resource Center. https://csrc.nist.gov/publications/detail/ir/8374/final

Cybersecurity by the Numbers: 2025 Snapshot

<table>
<tr><th rowspan="2">Average time to identify and contain a breach (breach lifecycle)</th><th colspan="3">Average cost of a data breach</th></tr>
<tr><td>Global</td><td>US</td><td>Healthcare Sector</td></tr>
<tr><td rowspan="2">241 days</td><td>$4.44M</td><td>$10.22M</td><td>$7.42M
(highest of any sector)</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><th colspan="2">Most common initial attack vector</th><th colspan="2">Malicious or criminal attack</th></tr>
<tr><td colspan="2">Phishing (16%)</td><td colspan="2">51%</td></tr>
<tr><th colspan="4">Average cost savings with a cybersecurity incident response team and testing</th></tr>
<tr><td colspan="4">$1.49M[6]</td></tr>
</table>

Breach detection and response capabilities can significantly impact financial and operational outcomes. For courts investing in cybersecurity is not optional; it is a critical component of operational resilience and public trust.

Cybersecurity is a team effort that requires the diligence of every technology user and the commitment of the court's executive leadership to plan, prevent, and respond effectively to incidents. It begins with strong preventive practices including regular training, testing, monitoring, and the implementation of best practices for data protection and recovery.

Effective cybersecurity planning enables courts to identify, categorize, and prioritize the recovery of mission-essential functions and the systems and services that support them. In environments where IT services are shared it is also critical for courts to coordinate and cooperate with other entities to ensure a cohesive and comprehensive response.

[6] IBM Security. (2025, July). *Cost of a data breach report 2025*. IBM & Ponemon Institute. https://www.ibm.com/reports/data-breach

Figure 1 highlights the steps related to a cybersecurity breach after an attack has been confirmed.

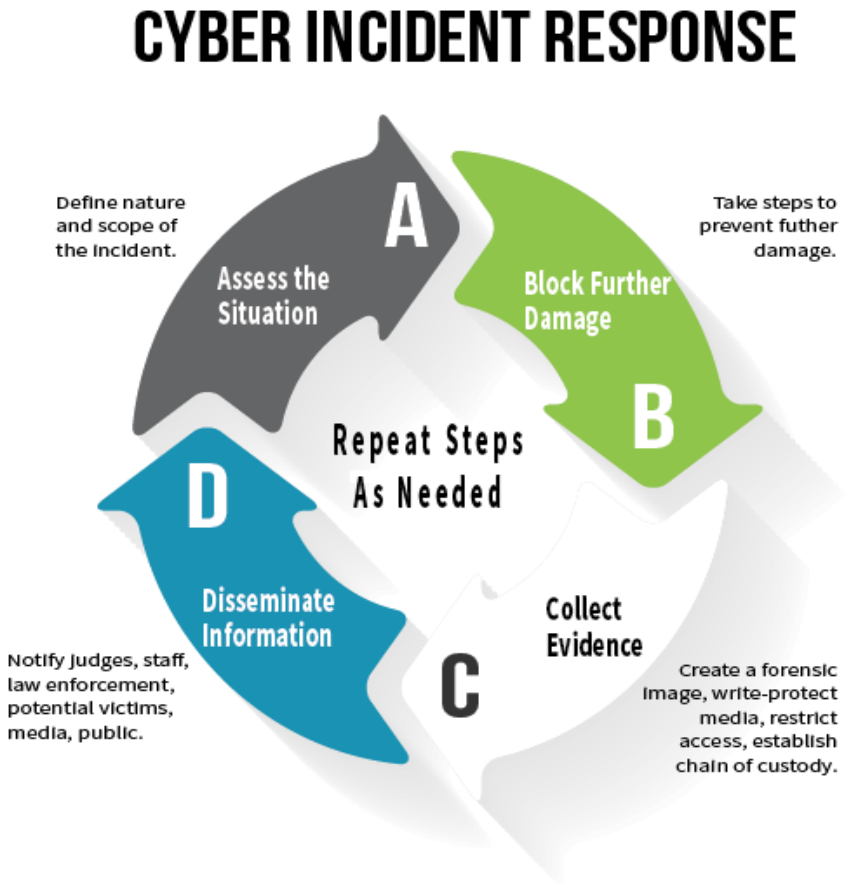


FIGURE 1: ABCS OF A CYBERSECURITY RESPONSE

See Appendix B for Cybersecurity Discussion Guide which provides a list of questions for administrators and managers to use as a guide to have a productive cybersecurity conversation with technology staff and providers (another agency or vendor).

See also JTC's *Cybersecurity Incident Planning and Response for Courts* for more detailed information.

State of Cybersecurity in Courts

Proactive cybersecurity measures are no longer optional, they are essential. While prevention remains important, most organizations will face a cyber incident at some point, requiring a coordinated and timely response. Courts are increasingly targeted as attackers employ more sophisticated methods. This section draws on real-world examples to illustrate the growing threat and underscore the need for preparation.

Figure 2 represents the increasing court threat surface and highlights examples of possible cyber incidents.

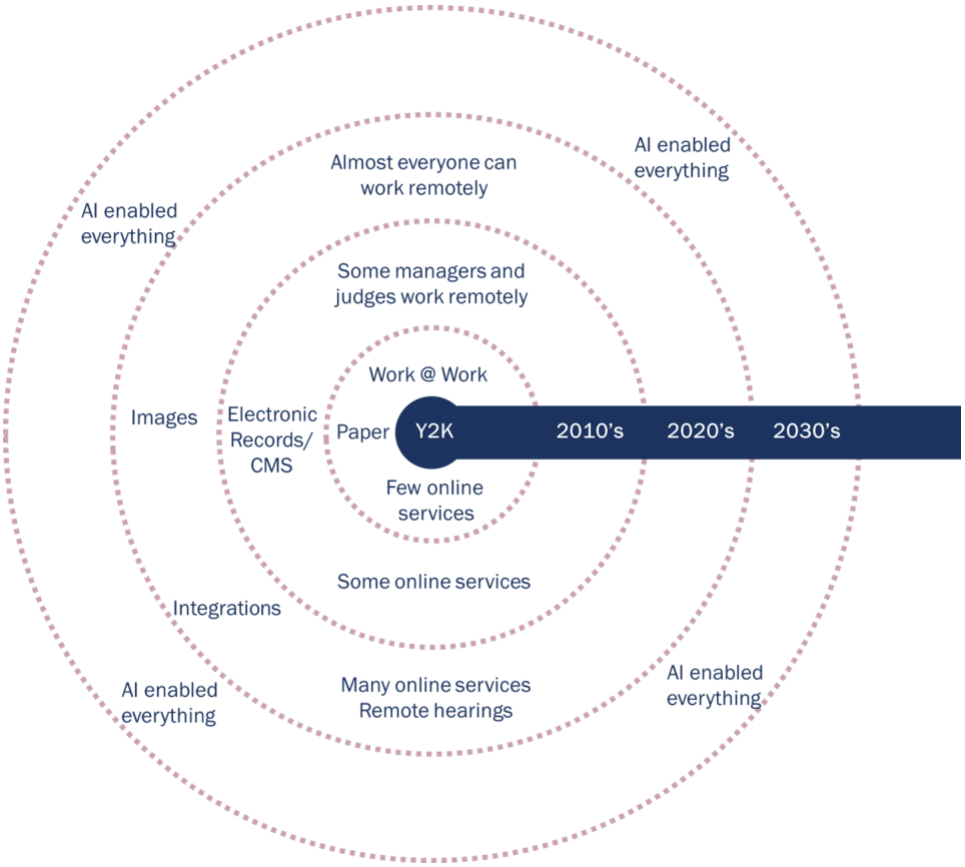


FIGURE 2: INCREASING THREAT SURFACE

Cybersecurity is a universal concern regardless of industry, location, or jurisdiction. The scale and complexity of recent cybersecurity incidents affecting both public and private organizations is sobering. Courts may assume they are unlikely targets due to limited financial data storage, such as credit card information. This assumption is dangerously outdated. Courts store sensitive personal data, including case files, witness information, law enforcement reports, and protected health information. As

a result, they have become increasingly attractive targets for ransomware operators, hacktivists, and nation-state actors.

Notable Recent Cyberattacks on U.S. State Courts

- **Los Angeles County Superior Court (July 19, 2024)**
  A ransomware attack forced the closure of all 36 courthouses, the largest unified trial court in the U.S., on a Monday following detection on Friday. Systems from jury portals to case management were disabled. The court restored basic functionality by Tuesday and full service within about eleven days. There was no evidence that user data had been compromised.[7]
- **Cleveland Municipal Court, Ohio (February–March 2025)**
  On February 23, 2025, the court suspended all internal systems in response to a suspected ransomware incident.[8] The Ohio National Guard's Cyber Reserve Force assisted in the investigation. The Qilin ransomware group later claimed responsibility. Most operations, including online services and hearings, were suspended until reopening on March 12, 2025.[9]

Additional examples:

- In 2021, the **Alaska court system** was targeted by a ransomware attack that temporarily disabled its online services and disrupted court operations statewide.
- In 2023, the **Minnesota Judicial Branch** temporarily shut down access to online court records due to a cybersecurity threat.
- In 2024, the **Kansas court system** suffered a ransomware incident that led to significant case management delays and forced reliance on manual processes, and the **Cook County Circuit Court (Illinois)** experienced a major breach that caused service interruptions and potentially compromised sensitive court data.

---

[7] Reuters Legal. (2024, July 22). *Los Angeles court closed after ransomware attack*. Reuters. https://www.reuters.com/legal/government/los-angeles-court-closed-after-ransomware-attack-2024-07-22/

[8] Reddick, J. (2025, February 26). *'Cyber incident' shuts down Cleveland Municipal Court for third straight day*. *The Record from Recorded Future News*. https://therecord.media/cyber-incident-shuts-down-cleveland-municipal-court

[9] Hoenig, M. (2025, March 7). *Cleveland Municipal Court hit by cyber attack*. The Record from Recorded Future News (KJK). https://kjk.com/2025/03/07/cleveland-municipal-court-hit-by-cyber-attack/cleveland19.com+11

The U.S. Federal Courts were also subject to a cyberattack. In early 2025, the Administrative Office of the U.S. Courts confirmed a cybersecurity breach impacting the Case Management/Electronic Case Files (CM/ECF) system. The breach reportedly compromised sensitive court records, prompting enhanced security protocols and temporary restrictions on external access to certain filings.[10]

These incidents illustrate that courts of all sizes and jurisdictions can become victims, regardless of geographical remoteness or perceived irrelevance. Emerging trends–such as hiring freelance hackers or leveraging insider access–amplify the growing and evolving disruption risks faced by judicial institutions.

The integration of interconnected digital systems, remote access capabilities, and online filing platforms has dramatically increased exposure. Cyber threats now transcend physical borders–attackers can strike from anywhere at any time. Courts must treat cybersecurity as a leadership and governance issue, not merely a technical one.

Accepting that cybersecurity incidents are inevitable is critical. Indeed, an undetected incident may already exist within your systems. Court leaders and IT teams must implement and regularly test a comprehensive incident response and recovery plan before an event occurs. Preparation enables quicker mitigation, minimizes operational interruption, and helps uphold public trust in the judicial system, even when that system is under duress.

[10] Ilascu, I. (2025, February 28). *U.S. judiciary confirms breach of court electronic records service*. BleepingComputer. https://www.bleepingcomputer.com/news/security/us-judiciary-confirms-breach-of-court-electronic-records-service/

Preventing Incidents

Preventing a cybersecurity incident is always preferable to recovering from one, no matter how well the recovery is managed. No prevention strategy can guarantee complete immunity, but intentional and proactive measures can significantly reduce risk, limit the impact of an attack, and lay a solid foundation for effective recovery.

Valuable resources, services, and training opportunities are available at no cost to state and local government entities–including the judicial branch–through:

- The **Cybersecurity and Infrastructure Security Agency** (**CISA**),[11] which offers support in areas such as incident response, cybersecurity training and exercises, penetration testing, risk assessments, governance development, threat detection and prevention, and real-time alerts.
- The **Multi-State Information Sharing & Analysis Center** (**MS-ISAC**),[12] which provides free membership for government agencies. Benefits include access to a 24/7 security operations center, incident response assistance, threat advisories, malicious code analysis, vulnerability management tools, and tabletop exercise templates.

Both organizations place a specific emphasis on threats to government systems and offer practical, actionable resources that every court should be utilizing.

Strengthening the Cybersecurity Foundation

Cybersecurity is more than just firewalls and passwords, it requires a proactive, layered defense strategy. Courts face constant threats from cybercriminals ranging from phishing schemes to sophisticated intrusion attempts. While many courts rely on IT professionals to implement safeguards it is equally important for court leadership, judges, and staff to understand and support essential security measures that help reduce exposure to threats.

The following section outlines key strategies to harden a court's overall cybersecurity posture. These practical steps aim to reduce the "threat vector", the potential pathways through which an attacker can gain access to systems or data and build resilience into the court's operations. Whether managing digital access, securing physical spaces, or controlling the software environment these foundational

---

[11] Cybersecurity and Infrastructure Security Agency. (n.d.). *Cybersecurity services for government partners*. U.S. Department of Homeland Security. Retrieved July 28, 2025, from https://www.cisa.gov/resources-tools/services/cybersecurity-services

[12] Center for Internet Security. (n.d.). *Multi-State Information Sharing and Analysis Center (MS-ISAC)*. Retrieved July 21, 2025, from https://www.cisecurity.org/ms-isac

actions support a culture of security and help courts respond more effectively to the constantly evolving cyber landscape.

Reduce the Threat Vector

Most IT organizations already take steps to block website traffic from known malicious IP addresses. Further narrowing the threat vector can significantly improve system security. One effective approach is restricting geographic access to critical applications, even when valid credentials are used. For example, access to a state's child support filing system should be limited to users within the continental United States to prevent unauthorized foreign access attempts.

Secure Facilities and Digital Devices

Physical security is an essential and often overlooked component of cybersecurity. Server rooms should remain locked and all digital devices must be physically secured when not in use. A stolen laptop, tablet, or phone can become a significant point of exposure for sensitive data and a gateway for cyberattacks.

Courts should have clear policies and procedures for handling lost or stolen equipment, including the ability to quickly disable or remotely wipe affected devices. Full-disk encryption tools–such as BitLocker for Windows and FileVault for macOS–should be installed and enabled on all portable devices to protect stored data in the event of device loss or theft. BitLocker and FileVault offer operating system–native whole-drive encryption that ensures data remains inaccessible without proper credentials, even if the hardware falls into unauthorized hands. This is especially important for laptops and other mobile devices which are highly susceptible to physical loss.[13] [14]

Unfortunately, courts and other non-technical organizations are often lax in safeguarding IT assets. The most common security vulnerabilities are human errors. Ensure all personnel–including judges, staff, contractors, and volunteers–understand that unauthorized individuals must not be granted access to sensitive equipment or restricted areas. Ongoing training and clear accountability protocols can help reinforce this expectation and reduce human-related risks.

---

[13] University of Oxford Information Security. (n.d.). *Encryption*. Retrieved July 22, 2025, from https://www.infosec.ox.ac.uk/encryption

[14] CISA. (n.d.). *How to protect the data that is stored on your devices*. U.S. Department of Homeland Security. Retrieved July 28, 2025, from https://www.cisa.gov/resources-tools/training/how-protect-data-stored-your-devices

Limit Access to Systems, Processes, and Data

Access to critical systems should be tightly controlled. The "keys to the cyber-kingdom" must be limited to only those who truly need them. Courts should implement the Principle of Least Privilege (PoLP), a well-established IT best practice that reduces risk by granting users, applications, and systems only the minimum access necessary to perform their functions.[15]

In addition to digital access controls courts must also secure and monitor physical access to on-premises infrastructure. Include maintaining door access logs for secured areas, implementing multi-factor authentication for physical entry points, and using video surveillance to monitor access to sensitive locations such as server rooms and network closets.

Segment the Network

Closely aligned with the PoLP is the practice of network segmentation, the division of the network into smaller, isolated zones based on function or sensitivity. For example, financial applications should reside in a separate network segment from case management systems or public-facing services.

This type of segmentation is typically enforced using firewalls, Virtual Local Area Networks, and access control rules which add layers of complexity that hinder unauthorized lateral movement by attackers. In the event of a breach segmentation can help contain the impact ensuring that a compromise in one area does not automatically expose the entire network.

Network segmentation also supports compliance and auditing efforts by allowing more precise tracking and logging of system interactions and is a key component of zero trust architecture, which is rapidly becoming the cybersecurity standard in both public and private sectors.

Authorized Software and Patch Management

Unauthorized or user-installed software is a common and preventable source of cybersecurity risk. All software installed on a court's enterprise network should be licensed, up to date, and installed and configured by authorized IT personnel. Courts should maintain clear policies and procedures for detecting and removing unauthorized software.

---

[15] NIST. (n.d.). *Principle of least privilege*. In *Glossary of Key Information Security Terms*. NIST Computer Security Resource Center. Retrieved July 28, 2025, from https://csrc.nist.gov/glossary/term/least_privilege

Patch management is equally essential.[16] Software patches–updates issued between major release cycles–are frequently developed to address newly discovered security vulnerabilities and correct other bugs or performance issues. However, applying a patch without testing can unintentionally disrupt other systems or break integrations.

To manage this risk, courts should:

- **Test patches** in a controlled environment before deploying them broadly.
- **Schedule updates** during non-working hours, when possible. Critical patches may need to be deployed during active business hours.
- **Configure systems** to update on a consistent, automated schedule.
- **Educate court personnel** on the importance of leaving devices powered on and connected to the internet, particularly overnight, to receive scheduled updates.

Missed or delayed updates can result in updates being installed during active use, potentially interfering with court operations. This reinforces the need for both IT staff and end court personnel to maintain systems in a state that supports timely and secure patching. Clear communication, regular training, and documented procedures will improve patch compliance and reduce the risk of system vulnerabilities.

Vendor contracts should include clear language requiring timely updates to third-party components and libraries–such as embedded web browsers, database engines, or authentication modules–when known vulnerabilities are disclosed or when security support for those components becomes obsolete. Modern software is often built on numerous third-party dependencies and vulnerabilities in these components can be exploited even after the primary vendor's software is installed.[17]

Given that many court systems now operate round-the-clock, it is essential to have a defined process for scheduling system maintenance and updates. Some systems may already have standing maintenance windows in place. If not, courts should establish them as part of routine operations.

---

[16] NIST. (2022). *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology* (Special Publication 800-40 Rev. 4). NIST. https://doi.org/10.6028/NIST.SP.800-40r4

[17] NIST. (2024). *Secure Software Development Framework (SSDF), version 1.1: Recommendations for mitigating the risk of software vulnerabilities* (NIST Special Publication 800-218). NIST. Retrieved July 28, 2025, from https://www.nist.gov/resources-tools/nist-sp-800-218-secure-software-development-framework-v11-recommendations-mitigating-risk-soft

To minimize disruptions, courts should also implement effective notification procedures to alert stakeholders of upcoming planned outages or system updates. Depending on the system and its user base this may include email notifications, system banners, website alerts, or other communication channels.

Manage Accounts and Passwords

To ensure user activities are traceable and auditable each individual must have a unique user account. Systems should be configured to automatically lock workstations or log off court personnel after periods of inactivity to prevent unauthorized access through unattended devices.

Implement network monitoring tools that can:

- Inventory all connected devices
- Audit user activities
- Detect anomalies
- Trigger automated alerts when unusual behavior occurs

When personnel separate from the organization, whether through routine departure or termination for cause, all associated accounts must be disabled or removed immediately. Maintain an inventory of internal and external systems accessed by each user to ensure comprehensive deactivation when needed.

Password management should emphasize both security and usability:

- Require strong, unique passwords for each account.
- Encourage the use of passphrases (e.g., 1twillb3Fr!day$00n) that are both long and easier to remember.
- Enforce periodic password changes through automated prompts and system policies.

Authentication

Implement multi-factor authentication (MFA), which enhances security by requiring court personnel to provide two or more independent forms of verification.[18] [19]

These may include:

- Something you know (e.g., a password or PIN)
- Something you have (e.g., a smart card or authentication app)

---

[18] NIST, *supra*.

[19] CISA. (n.d.). *Multifactor Authentication*. U.S. Department of Homeland Security. Retrieved July 28, 2025, from https://www.cisa.gov/resources-tools/resources/multi-factor-authentication-mfa

- Something you are (e.g., a fingerprint, facial scan, or other biometric data)

A common form of MFA is two-factor authentication, such as a password plus:

- A text message with a verification code
- A code generated by an authentication app (e.g., Microsoft Authenticator or Google Authenticator)
- A biometric identifier

Biometric authentication offers convenience and strong identity assurance, but it also raises privacy and data protection concerns as it involves the collection and storage of sensitive personal information. Courts should carefully evaluate legal and ethical considerations before implementing biometric technologies.

Note: Basic single-factor authentication such as username and password alone is no longer sufficient to protect court systems given the increasing sophistication of cyberattacks.

Invest in Cybersecurity

Organizations must allocate dedicated funding for cybersecurity including software, services, and staff time as part of their regular budget cycle. This includes not only technical safeguards but also training for all personnel, as human behavior remains one of the most exploitable vulnerabilities.

According to Accenture's State of Cybersecurity Resilience 2023 report, cybercriminals are increasingly targeting indirect pathways, including third-party vendors and supply chain partners.[20] High-profile breaches such as the SolarWinds attack where a compromised software update from a trusted vendor led to widespread infiltration across government and private networks underscores the urgent need for supply chain security.[21]

While there have been significant innovations in cybersecurity–including AI-driven threat detection, faster breach response, and improved patch management–attackers continue to evolve. Sophisticated phishing, social engineering, and vendor compromise remain among the most common attack vectors. Organizations must invest both in foundational security practices and in emerging technologies to improve their overall cyber resilience.

---

[20] Accenture Security. (2023). *The state of cybersecurity resilience 2023* (Accenture Research). Accenture. Retrieved July 28, 2025, from https://www.accenture.com/us-en/insights/security/state-cybersecurity

[21] Belfer Center, Harvard Kennedy School. (2021). *SolarWinds attack: Turning a routine update into a global espionage campaign*. Belfer Center for Science and International Affairs. Retrieved July 28, 2025, from https://www.belfercenter.org/publication/solarwinds-attack

Training: A Foundational Element of Cyber Defense

Continuous cybersecurity awareness training for all personnel is critical. The threat landscape evolves constantly and without regular reinforcement court personnel may inadvertently fall for preventable attacks.

Training should cover:

- Core cybersecurity best practices
- How to recognize suspicious behavior or messages
- How to respond appropriately, including reporting incidents

Phishing remains one of the most common and preventable intrusion methods. While antivirus and email filtering tools can block many phishing attempts user education remains the most effective defense. Organizations should incorporate:

- Ongoing training sessions
- Periodic simulated phishing tests
- Clear reporting channels for suspected phishing emails

Technical Staff Training and Certification

In addition to end-user awareness technical staff should be equipped with current knowledge and tools. Personnel involved in incident response, system recovery, or network reconfiguration should maintain up-to-date certifications and specialized training. Inadequately trained staff may unintentionally compound the damage during a response.

Investing in training and certifications such as CompTIA Security+, Certified Information Systems Security Professional, [22] or Certified Ethical Hacker ensures technical teams are prepared to act decisively and effectively in both prevention and response roles.

Cybersecurity is not a one-time investment, it is a strategic, ongoing commitment. With threats evolving and attackers increasingly exploiting both technical and human vulnerabilities, a well-rounded, well-funded, and continuously updated cybersecurity program is essential.

See Appendix C for actionable cybersecurity guidance.

[22] *Certified Information Systems Security Professional (CISSP)*. In *Wikipedia*. Retrieved July 28, 2025, from https://en.wikipedia.org/wiki/Certified_Information_Systems_Security_Professional

IT Risk Analysis

Organizations should conduct a comprehensive IT risk analysis to:

- Identify potential threats and vulnerabilities
- Assess the likelihood and impact of various risks
- Evaluate the cost-benefit of countermeasures
- Develop a remediation and mitigation plan

Risk analysis should be updated regularly and conducted following major system changes, policy updates, or incidents. The results inform security investment decisions and help prioritize action.[23]

Conduct Routine Penetration Testing

Courts and other government entities should regularly engage qualified third-party vendors to perform penetration testing, simulating real-world attack scenarios to uncover vulnerabilities in systems, applications, and configurations. These ethical hacking engagements provide:

- Detailed reports on exploitable weaknesses
- Actionable recommendations for remediation
- Validation of existing security controls

Penetration testing complements internal vulnerability assessments and helps organizations improve their overall security posture.[24]

Own It: Accountability and Awareness

Cybersecurity is not just the responsibility of the IT department, it is the shared responsibility of every employee. While accountability can be challenging it is essential to creating a resilient organization. Anyone can fall victim to a phishing email, social engineering, or poor cyber hygiene. However, courts must:

- Foster a culture of cybersecurity awareness
- Train all personnel regularly
- Implement fair and clear accountability policies for preventable incidents

Creating a sense of ownership empowers staff to be proactive, attentive, and aligned with the organization's security objectives.

---

[23] NIST. (2008). *Guide to Information Security Testing and Assessment* (NIST Special Publication 800-115). NIST. Retrieved July 28, 2025, from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-115.pdf

[24] NIST. (2020). *Zero Trust Architecture* (NIST Special Publication 800-207). https://doi.org/10.6028/NIST.SP.800-207

Cybersecurity Governance, Policy, and Planning

Cybersecurity inevitably comes at a cost, not only in terms of financial investment but also in convenience and performance. Striking the right balance between security and usability can be challenging for management. As recent cyberattacks have demonstrated, convenience must never be an excuse to bypass or weaken security protocols. The cost and disruption of recovering from a successful cybersecurity incident far outweigh the minor inconveniences of security processes, policies, and training. Effective cybersecurity requires organization-wide commitment from executive leadership to frontline court personnel.

Establishing Cybersecurity Governance

Courts should establish a cybersecurity governance body that adopts a collaborative, enterprise-wide approach. This group should:

- Regularly review and update policies and procedures
- Receive updates on current threats, attempted intrusions, and response efforts
- Oversee cybersecurity investments ensuring they align with operational priorities and risk levels

A well-structured governance group provides diverse perspectives enabling more informed and strategic decision-making. It also fosters shared responsibility and helps define what constitutes an effective cybersecurity posture for the court environment.

See Appendix D for the Cybersecurity Governance Checklist for Courts.

Planning for the Inevitable: Outages and Recovery

Judicial leaders must be educated on the operational realities of cyber incidents, including what levels of downtime to expect following a successful attack. Cybersecurity-related outages are not typical system disruptions. Outages can last weeks or even months depending on:

- The scope and severity of the attack
- The systems affected
- Whether data was exfiltrated or encrypted

These extended outages can halt critical court operations and compromise public trust. This is far more than a typical IT outage. Cybersecurity incident response planning must be integrated into the court's Continuity of Operations Plan (COOP). Courts should use specialized guidance and templates designed for judicial systems to integrate these scenarios effectively.[25]

When Will Operations be Restored?

Internally the top question during a cyber incident is inevitably: "When will operations resume?" The answer is difficult because the timeframe depends on multiple variables including the scope of the breach, time required for assessment and forensic analysis, and whether data exfiltration occurred. Attack types and impacts vary widely meaning recovery timelines do too.

2025 DATA BREACH METRICS

Breach response is often measured in months, not days, and can result in multimillion-dollar losses. The figures to the right and below, drawn from IBM's Cost of a Data Breach Report 2025,[26] highlight current trends in duration and incurred losses due to data breaches:

Average time to identify a breach
181 days

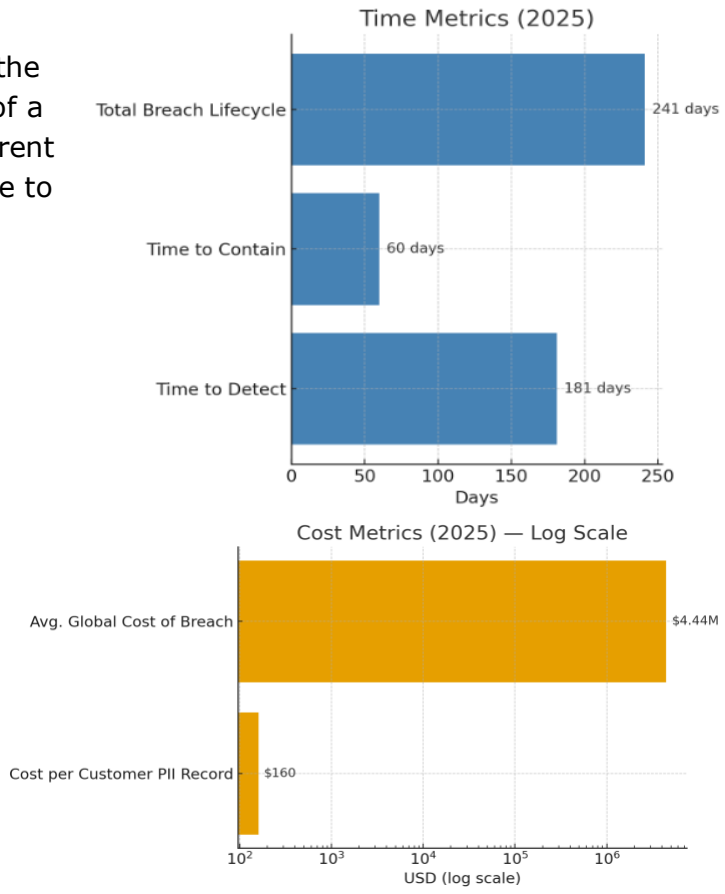
Average time to contain a breach
60 days

Breach lifecycle (detection + containment)
Approximately 241 days

Global average cost of a breach
$4.44 million—an increase of 10% from the previous year

Average cost per lost or stolen record
$160

FIGURE 3: 2025 DATA BREACH TIME & COST METRICS



[25] National Center for State Courts (NCSC). (2021). *Courts Continuity of Operations (COOP) Planning Guide and Template*. Retrieved July 28, 2025, from https://ncsc.contentdm.oclc.org/digital/collection/facilities/id/256/rec/3

[26] IBM Security & Ponemon Institute. (2025). *Cost of a Data Breach Report 2025*. IBM. Retrieved July 28, 2025, from https://www.ibm.com/reports/data-breach

Assembling a Cybersecurity Incident Response Team (CIRT)

While the IT department will naturally lead the technology response to a cybersecurity incident it cannot act alone. Effective incident prevention, response, and recovery require a multidisciplinary team that includes representatives from departments involved in operations, communications, legal compliance, and resource management.

Courts should assemble CIRT reflective of the full scope of court operations. Consider how to "staff the threat", ensuring each role has at least one alternate if a primary team member is unavailable.

At a minimum that team should include the following roles:

- **Chief Judge/Justice**
  Serves as the public-facing leader and likely spokesperson for the court during an incident.
- **Court Administrator/Chief Executive Officer (CEO)**
  Oversees day-to-day court operations and mobilizes internal resources to execute the response plan. If a Chief Information Security Officer (CISO) is not on staff, the Chief Information Officer (CIO) may assume responsibility for cybersecurity coordination.
- **Chief Information Officer (CIO)**
  Leads the technical execution of the cybersecurity incident response plan, including restoration efforts and coordination with vendors.
- **Chief Information Security Officer (CISO)**
  Provides focused cybersecurity oversight, ensuring responses align with legal mandates, protect sensitive data, and meet industry standards. The CISO may also manage digital forensics and act as a liaison to law enforcement and other external agencies.
- **Public Information Officer (PIO)**
  Supports the Chief Judge/Justice by preparing accurate and timely communications for court personnel, the public, and the media.
- **Human Resources**
  Participates if court personnel are affected, such as through payroll system disruptions, identity theft, or disciplinary concerns related to the breach.
- **Chief Financial Officer (CFO)**
  Ensures appropriate funding channels and emergency procurement procedures are followed, including the contracting of third-party services when necessary.

- **Legal Counsel**
  Provides guidance to avoid legal missteps during the court's response and recovery efforts, particularly in areas such as data privacy, mandatory breach notification, and liability.
- **Vendors / Third-Party**
  Support Fills gaps in expertise or staffing capacity. Pre-negotiated agreements with cybersecurity firms, forensic experts, and recovery service providers can significantly reduce response time and administrative delays during an emergency.

Each team member brings a unique organizational perspective which is essential for addressing the full range of implications that may arise during a cybersecurity incident. While IT personnel focus on urgent technical tasks, court managers may need to lead or support non-technical recovery efforts, including operational coordination, internal communication, and stakeholder engagement.

Identify the Spokesperson

In the aftermath of a cybersecurity incident conflicting public statements from multiple sources can lead to confusion, misinformation, and damage to the court's credibility. Designate a single spokesperson–typically the Chief Judge, Court Administrator, or PIO–to serve as the sole official voice of the court. Ensure all internal personnel understand that no one else is authorized to speak publicly about the incident.

Assign Responsibilities

Clearly identify essential tasks and assign responsibility for each. Be specific. Non-technical tasks that can be handled by court managers and other staff such as coordinating logistics, communicating with stakeholders, or supporting personnel, can alleviate pressure on IT teams. Court leaders should have the authority and flexibility to address recovery needs within their skillset, minimizing operational bottlenecks.

Meet Regularly

The CIRT should convene regularly–at least quarterly–to review roles, assess readiness, and refine procedures. During an actual incident the team should meet frequently and consistently to:

- Share new information
- Monitor progress on recovery efforts
- Adjust response plans as needed

Regular communication is critical to ensure a coordinated, timely, and unified response.

Establish Channels of Communication

Maintain a comprehensive, secured contact list for key personnel and external partners–e.g., IT vendors, court security, law enforcement)–including after-hours contact information. Anticipate that standard communication systems–email, Voice over Internet Protocol (VoIP), internal phones–may be compromised. As part of your continuity plan, implement an emergency notification system (e.g., Everbridge) to quickly relay information during disruptions.

To ensure rapid access provide team members with a digital copy of the cybersecurity incident response plan and contact list, ideally on secured mobile devices or via an app. Also maintain a paper copy in a designated, accessible location in case digital systems are unavailable.

> ***Tip:*** *To help validate an incident notification is genuine and not a hoax or social engineering attempt, consider establishing a pre-arranged code word or phrase known only to the CIRT. This confidential keyword can be included in the initial alert to confirm the legitimacy of the message and trigger immediate action.*

For courts that rely on city or county-managed IT infrastructure anticipate interdepartmental communication challenges. Your response plan should clearly define who your IT contacts are, even if they are external to the court, and outline protocols for cross-agency coordination.

Communication Planning

Courts must maintain robust, redundant communication systems ensuring multiple contingency paths are available, particularly when primary systems–such as email or VoIP–may be compromised during an incident.[27] These systems should be regularly tested and include after-hours contacts.

It is also essential to embed cybersecurity incident response planning within the COOP ensuring critical operations and communication channels remain intact even during severe outages.[28]

---

[27] CISA & Federal Emergency Management Agency (FEMA). (2018). *Communications continuity and resiliency primer*. U.S. Department of Homeland Security. Retrieved July 28, 2025, from https://www.cisa.gov/sites/default/files/publications/Communications%20Continuity%20and%20Resiliency%20Primer_December%202018_508c.pdf

[28] FEMA. (2023). *Planning considerations for cyber incidents*. U.S. Department of Homeland Security. Retrieved July 28, 2025, from

While the exact content of your communications will vary based on the incident preparing messaging templates in advance can save critical time. Templates should:

- Provide a structure and tone that reassures the public and internal stakeholders.
- Emphasize the court's commitment to continuing essential operations.
- Convey that updates will be shared as more information becomes available.

Your external communication plan should include:

- Press releases
- Website updates
- Social media posts

For internal communications, provide consistent updates to judges, staff, contractors, and volunteers. Acknowledge their contributions, emphasize transparency, and reassure them about the steps being taken to restore normal operations.

Court-specific COOP guidance underscores the value of maintaining up-to-date contact lists, defined communication roles, and accessible plans. COOP guidance should also be available in mobile and paper formats–to ensure accessibility–for team members to reference during emergencies.[29]

Cybersecurity as Part of a Continuity of Operations (COOP)/Disaster Recovery Plans

Courts must establish and document clear procedures to follow in the aftermath of a cybersecurity incident. These procedures should be an integral part of the broader COOP and disaster recovery planning, which also cover other potentially disruptive events, such as pandemics, natural disasters, weather emergencies, and terrorist attacks.[30]

It is essential that judges, supervisors, and court management staff are familiar with the plan and clearly understand their roles and responsibilities. Avoid overcommitting key personnel—assign roles and responsibilities thoughtfully,

---

https://www.fema.gov/sites/default/files/documents/fema_planning-considerations-cyber-incidents_2023.pdf

[29] NCSC. (2021). *Court continuity of operations (COOP) planning guide and template*. Retrieved July 28, 2025, from https://www.tmcec.com/wp-content/uploads/2025/05/210218-NCSC-COOP-Planning-Guide-and-Template-2021.pdf

[30] NCSC. (2023). *Emergency preparedness resources for courts*. https://www.ncsc.org/services-and-experts/technology-tools/emergency-preparedness

ensuring no single individual is burdened with managing multiple aspects of the plan during a crisis.

Response procedures should be logical, actionable, and court specific. They must align with existing court policies, and, if inconsistencies exist, relevant court policies and business processes should be revised. Consider the logistical implications of recovery such as relocating to an alternate site and ensuring access to necessary technology and communication systems.

Pre-planning significantly reduces the impact of cybersecurity incidents by limiting damage to computer systems, minimizing operational disruptions, and maximizing the ability of law enforcement to investigate and respond effectively.[31]

Test and Tailor the Plan: Preparing for When, Not If

Avoid solely relying on "cut and paste" model plans. While such templates offer a convenient starting point they may include assumptions, responsibilities, or commitments your court cannot realistically meet. These gaps may only become apparent when the plan is executed during a real incident. Effective recovery planning requires customization to reflect your court's actual resources, operations, and constraints.

Regular and rigorous testing is critical. Plans should be exercised under realistic conditions and intentionally pushed to failure to reveal vulnerabilities. If testing never exposes shortcomings it may indicate insufficient rigor or a lack of imagination, not an airtight plan.

Set Clear Priorities

Prioritization is both complex and critical. Not all systems are equally important, and not all can be recovered simultaneously. Your plan should:

- Account for interdependencies between systems.
- Identify essential business processes that must be restored first.
- Acknowledge staffing and technical constraints.
- Remain flexible to adapt to emerging conditions during the recovery effort.

It may be advantageous to prioritize systems that are easiest to bring back online enabling partial operations to resume. For example, restoring communication systems (phones, email, messaging) may not directly deliver justice but they greatly facilitate the coordination of recovery tasks.

---

[31] CISA. (2021). *Ransomware Guide*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/CISA_MSISAC_Ransomware%20Guide_S508C.pdf

Include Tactical Details

An effective cybersecurity incident response plan must go beyond abstract strategy. It should clearly define:

- Who is on the response team and their specific roles.
- How team members will communicate if usual channels are unavailable.
- The detailed steps each participant must follow.
- Timelines and escalation protocols.

By planning in detail and rehearsing regularly courts will be better positioned to respond with confidence, agility, and effectiveness when–not if–a cybersecurity incident occurs.

Conclusion

Cybersecurity is no longer just an IT issue; it is a court-wide concern that affects every facet of judicial operations from case management to public trust. Courts must acknowledge cyber incidents are not hypothetical, they are inevitable. As threats grow in sophistication and impact preparedness becomes not only prudent but essential.

A well-developed and regularly tested cybersecurity incident response plan is a cornerstone of that preparedness. This plan should include clearly defined roles and responsibilities, communication and escalation protocols, and prioritized recovery objectives. Tabletop exercises and full-scale simulations are vital to ensuring that court personnel, vendors, and interagency partners can execute the plan effectively when an incident occurs.

Cybersecurity investments, including budgeting for tools, training, testing, and external support, should be institutionalized rather than treated as discretionary. Courts must also maintain strong vendor oversight and ensure all service providers meet defined security standards.

Just as important is cultivating a culture of cyber awareness. Every judge, employee, contractor, and volunteer must understand their role in protecting court systems and data. Ongoing training in areas such as phishing prevention, password hygiene, and secure device use helps reduce human vulnerabilities–the most common entry point for cyberattacks.

By planning ahead, practicing regularly, and fostering a shared commitment to security, courts can strengthen their resilience, maintain operational continuity, and protect the sensitive data entrusted to them by the public.

For more information, visit:

https://www.ncsc.org/resources-courts/technology

Appendix A: About Cyberattacks

To create an effective cybersecurity response plan court administrators must understand the wide variety of threats they may face. These include both *opportunistic* and *targeted* attacks, as well as various tactics like ransomware, denial-of-service, and social engineering.

Opportunistic Attacks

Opportunistic attacks are broad, non-targeted cyberattacks designed to find any system vulnerability. Automated tools scan the internet for weaknesses such as outdated software or unpatched systems. Many email-based Trojan horse and worm attacks fall into this category. Courts, as recipients of online payments and custodians of personally identifiable information (PII), are especially vulnerable to opportunistic breaches that seek to harvest sensitive data like social security numbers or payment credentials.[32]

Targeted Attacks

Targeted attacks are deliberate and focused on a specific organization or individual, often to exfiltrate or alter sensitive information. For courts this could involve tampering with digital evidence, witness information, or sentencing records, posing serious threats to public safety.[33] These attacks may be motivated by revenge, political activism, or espionage. In 2013, all the cell doors in a Florida prison's maximum-security wing were opened simultaneously in what was suspected to be a targeted cyberattack.

Another common method for targeted attacks is "spear-phishing" in which deceptive emails trick recipients, often judges, administrators, or elected officials, into downloading malware or revealing credentials.[34]

---

[32] NIST. (2023). *Cybersecurity Framework*. https://www.nist.gov/cyberframework

[33] U.S. DOJ. (2022). *Cybersecurity Unit Best Practices for Victim Response and Reporting*. https://www.justice.gov

[34] CISA. (2024). *Phishing Guidance*. https://www.cisa.gov

Cyberattack Tactics

Regardless of whether a cyberattack is targeted or opportunistic the following tactics are frequently used.

Unauthorized Access

Unauthorized access occurs when individuals or software gain entry to networks or data without permission. Such breaches may come from court personnel, former employees, or external actors globally.[35]

Malware and Viruses

Malware includes a wide range of malicious software such as viruses, worms, spyware, and ransomware. Common variants include:

- **Spyware**
  Covertly collects user data
- **Adware**
  Displays intrusive ads
- **Scareware**
  Tricks court personnel with fake warnings
- **Worms**
  Self-replicate and spread across networks
- **Cryptojacking**
  Uses court computing resources to mine cryptocurrency.[36]

Attacks That Disrupt Service

Denial of service (DoS) and Distributed Denial-of-Service (DDoS) attacks overwhelm a network with traffic to make systems unavailable. These attacks have previously disrupted major financial and government operations.[37] The increasing use of internet of things (IoT) devices has also raised the risk of large-scale DDoS attacks. The *IoT Cybersecurity Improvement Act of 2020* was passed to improve security standards for connected devices.[38]

---

[35] IBM Security. (2025). *Cost of a Data Breach Report*. https://www.ibm.com/reports/data-breach

[36] Norton. (2023). *What is Cryptojacking?*. https://us.norton.com

[37] FireEye Mandiant. (2023). *Threat Intelligence Report: DDoS Trends*.

[38] U.S. Congress. (2020). *IoT Cybersecurity Improvement Act of 2020*. https://www.congress.gov

Ransomware

Ransomware encrypts systems and demands payment to restore access. Courts are frequent targets due to their sensitive data and perceived inability to afford downtime. While some municipalities have chosen to pay ransoms to expedite recovery, U.S. policy advises against payment to avoid funding future attacks and to comply with federal sanctions.[39] Organizations like No More Ransom offer free decryption tools and guidance on ransomware prevention and response.[40]

Formjacking

Formjacking involves injecting malicious code into legitimate websites to capture payment information. Courts accepting online payments are potential targets, especially if basic web security protocols like penetration testing and code validation are lacking.[41]

Zero-Day Exploits

Zero-day attacks exploit vulnerabilities in hardware or software before the vendor becomes aware. These attacks are difficult to detect and mitigate until patches are released. Courts should regularly update systems and employ proactive vulnerability scanning.[42]

Social Engineering

Human error remains one of the most common cybersecurity vulnerabilities. Staff can be manipulated into giving out credentials or bypassing physical security. In one court a spoofed email resulted in an employee nearly redirecting a paycheck to a fraudulent account. Organizations can mitigate these risks with email warnings and staff training.[43]

Supply Chain Attack

Supply chain attacks exploit third-party vendors or open-source software integrated into court systems. Notable attacks like SolarWinds illustrate how compromising a trusted vendor can result in wide-reaching breaches. Courts should assess vendor

---

[39] U.S. Treasury Department. (2020). *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*. https://home.treasury.gov

[40] No More Ransom. (2024). *Free Ransomware Decryption Tools*. https://www.nomoreransom.org

[41] Symantec. (2023). *Formjacking: The new silent threat*. https://symantec-enterprise-blogs.security.com

[42] Microsoft Security Response Center. (2021). *Exchange Server Vulnerability Alert*. https://msrc.microsoft.com

[43] Federal Trade Commission (FTC). (2023). *Recognizing and Avoiding Phishing Scams*. https://www.consumer.ftc.gov

cybersecurity posture and ensure contractual obligations for security and notification practices.[44]

[44] National Cybersecurity Center of Excellence (NCCoE). (2024). *Software Supply Chain Risk Management*. https://www.nccoe.nist.gov

Appendix B: Cybersecurity Discussion Guide

Below is a list of questions for administrators and managers to use as a guide to have a productive cybersecurity conversation with technology staff and providers (another agency or vendor).

Suggested Court IT Service Provider Discussion Points
☐ How would we initiate immediate deployment of cybersecurity experts when an attack occurs?
☐ Are current password requirements sufficient?
☐ Are current backup systems secure, immutable, and is at least one physically disconnected from the network?
☐ Are network backups tested, and are you sure that all critical data assets are backed up regularly?
☐ Do we have built-in replication in the cloud? If yes, how do we access it?
☐ What are the weak links in our system, and how can we strengthen them?
☐ How can we work together to improve our Continuity of Operations and Disaster Recovery plans?
☐ Is the network segmented to reduce potential attack exposure?
☐ Do we have the right data governance approach to minimize cybersecurity risk?
☐ How can we work together to inventory, catalog, and assign risk point objectives and risk time objectives?
☐ Are there cybersecurity policies and practices that should be implemented?
☐ Who do we call if there are suspected intrusions or issues, and what type of security support is available?
☐ How often is cybersecurity audited?
☐ What are my security responsibilities and what are yours?
☐ How is sensitive information handled or stored by third-party providers being protected?

Appendix C: Taking Action

Ready to do more about cybersecurity in your court? Use the following possible actions as a checklist to guide discussion.

Suggested Court Actions	Action Level
☐ Verify that **data is backed up** frequently, fully as well as incrementally, and stored in multiple, secure locations.	Basic
☐ Frequently **test restore procedures** on randomly selected files to ensure that backups are usable. Periodically **attempt a full restore**.	Basic
☐ Review the **threat surface** regularly, or, at a minimum, each time a system is implemented or upgraded.	Basic
☐ **Require strong, complex passwords** and change them as necessary (when compromised, leaked, or suspicious activity). Do not use the same password on more than one system.	Basic
☐ Use only **authorized software** on the enterprise network environment and limit installation and configuration privileges to tech staff.	Basic
☐ Ensure **network and application documentation** is up to date.	Basic
☐ Implement **software patch management** procedures to ensure all software components are updated as patches become available.	Basic
☐ Use PoLP approach to user accounts and data access.	Basic
☐ **Restrict physical access** to servers and network equipment.	Basic
☐ Establish **controlled entry points** for remote network or data access.	Intermediate
☐ Implement **network monitoring**. Establish benchmarks for "normal" activity, then configure to alert key personnel of any activity outside of set thresholds.	Intermediate
☐ Conduct regular **walkthroughs and tabletop exercises** to test cybersecurity response plans.	Intermediate
☐ Ensure **agreements with technology service providers** clearly identify roles, responsibilities, service levels, and response expectations. This applies to both vendors and **government entities that provide services** to the court.	Intermediate
☐ Ensure user **screens lock** after a certain period of inactivity.	Intermediate

☐ Establish policies and procedures for dealing with **lost equipment**; have the ability to quickly disable lost devices.	Intermediate
☐ Implement **multifactor authentication**, e.g., password or pin plus a smart card or biometric identifier.	Intermediate
☐ Ensure **file encryption utilities** are installed and enabled (e.g., BitLocker for Windows devices and FileVault for iOS) on portable user devices.	Intermediate
☐ Establish an **offline off-premises backup** to facilitate recovery if online backups are compromised.	Advanced
☐ **Segment the network.**	Advanced

Appendix D: Cybersecurity Governance Checklist for Courts

This checklist provides a practical guide for courts to assess and strengthen cybersecurity governance, particularly in environments involving shared infrastructure with external agencies, such as state or local government IT.

Note: This checklist is not exhaustive but offers a starting point for improving court cybersecurity posture.

1. **Governance Structure**
   - Establish a formal cybersecurity governance body with cross-functional representation (e.g., judiciary, administration, IT, security).
   - Define roles and responsibilities for cybersecurity decision-making and oversight.
   - In courts without a designated Chief Information Security Officer (CISO), designate a cybersecurity liaison responsible for overseeing implementation and reporting regularly to leadership.
   - Schedule regular meetings to review incidents, assess risks, and align on cybersecurity priorities.
2. **Policy and Compliance**
   - Review and maintain up-to-date cybersecurity policies and procedures.
   - Align with NIST Cybersecurity Framework or CIS controls and CISA best practices.
   - Ensure compliance with legal, regulatory, and judicial mandates for data privacy and security.
3. **Interagency Coordination**
   - Establish Memoranda of Understanding with shared infrastructure providers.
   - Define roles and responsibilities in joint COOP and disaster recovery plans.
   - Actively participate in interagency cybersecurity exercises and joint incident response planning.

4. **Communication and Incident Response**
   - Identify points of contact for emergency communication across agencies.
   - Develop protocols for incident reporting, escalation, and external notification.
   - Ensure inclusion in partner agencies' cybersecurity incident response plans.
5. **Asset and Risk Management**
   - Maintain a current inventory of essential data assets and IT systems.
   - Conduct routine risk assessments and update risk mitigation strategies.
   - Define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for all critical systems.
6. **Budget and Resource Planning**
   - Allocate dedicated budget for cybersecurity tools, staffing, and training.
   - Identify funding sources (e.g., grants) that support cybersecurity improvements.
   - Evaluate cost-benefit for ongoing investment in preventive and recovery measures.
7. **Cybersecurity Awareness and Workforce Training**

   Cybersecurity is everyone's responsibility. All court personnel, including judges, staff, contractors, and volunteers, should complete role-based cybersecurity awareness training. Training should include phishing prevention, secure handling of sensitive data, and regular simulated attack scenarios to test awareness and build a culture of vigilance.
8. **Zero Trust Architecture**

   Courts should consider adopting a zero trust architecture, a model built on the principle of never trusting any request by default, regardless of its origin. This includes strict identity verification, least-privilege access controls, and continuous monitoring of users, devices, and applications to detect and prevent threats inside and outside the network perimeter. Zero trust models should be implemented gradually and integrated into overall IT modernization plans.
9. **Mobile Device and BYOD Policy Considerations**

   Mobile devices introduce unique cybersecurity challenges. Courts should establish policies governing the use of personal devices (Bring Your Own Device or BYOD), including mandatory encryption, mobile device management (MDM), and remote wipe capabilities. Access to court data from mobile devices should be limited based on role and risk exposure.

10. **Cloud Security and SaaS Governance**

    As courts increasingly adopt cloud services, they must evaluate the risks and responsibilities associated with cloud platforms and Software-as-a-Service (SaaS) solutions. Courts should understand the shared responsibility model and ensure that vendor agreements clearly define security roles, encryption standards, and incident response procedures. Courts should also ensure data residency, encryption, and access management are addressed in cloud agreements.

11. **Data Classification and Handling**

    Courts should develop a data classification policy that categorizes data based on sensitivity and defines appropriate handling procedures. Categories might include public, internal, confidential, and restricted data. Policies should dictate storage, transmission, access, and destruction protocols for each category.

12. **Incident Postmortem and Lessons Learned**

    Following any cybersecurity incident, courts should conduct a formal postmortem analysis to identify root causes and gaps in their incident response plan. This process should result in a documented improvement plan and be shared with all relevant stakeholders to ensure continual learning and system resilience.

13. **Cybersecurity Metrics and Reporting**

    Courts should adopt a basic set of cybersecurity metrics to monitor security posture over time. Examples include patch compliance rates, number of security incidents, endpoint protection coverage, phishing simulation outcomes, and user training completion rates. These metrics should be summarized regularly in reports to leadership.

14. **Interagency and Judicial Collaboration**

    Cybersecurity requires collaboration across agencies, jurisdictions, and branches of government. Courts should participate in statewide and national efforts, such as incident response exercises and information-sharing forums–to strengthen collective preparedness and response.

15. **Privacy-by-Design and Data Minimization**

    Courts should adopt privacy-by-design principles in all technology initiatives and strive to collect only the minimum data necessary to fulfill judicial functions. Regular audits of data collection, retention, and access practices should be conducted to reduce risk and support legal compliance.

Checklist Area	Recommended Actions
☐ **1. Governance Structure**	• Establish a formal cybersecurity governance body • Define roles and responsibilities • Ensure regular incident and strategy review meetings
☐ **2. Policy and Compliance**	• Maintain up-to-date cybersecurity policies • Align with NIST and CISA standards • Ensure compliance with data security mandates
☐ **3. Interagency Coordination**	• Establish MOUs with IT providers • Define roles in COOP and DR plans • Participate in joint exercises
☐ **4. Communication and Incident Response**	• Identify emergency contacts • Develop incident protocols • Ensure inclusion in partner response plans
☐ **5. Asset and Risk Management**	• Maintain inventory of IT assets • Conduct risk assessments • Define RTO and RPO
☐ **6. Budget and Resource Planning**	• Allocate budget for tools and training • Identify grant opportunities • Evaluate cost-benefit of investments
☐ **7. Cybersecurity Awareness and Workforce Training**	• Provide role-based training • Include phishing and data handling • Simulate attack scenarios
☐ **8. Zero Trust Architecture**	• Implement least-privilege access • Enforce strict identity verification • Monitor continuously
☐ **9. Mobile Device and BYOD Policy**	• Define encryption and MDM policies • Allow access by role and risk • Enable remote wipe

Checklist Area	Recommended Actions
☐ **10. Cloud Security and SaaS Governance**	• Understand shared responsibility model • Define vendor security roles • Ensure encryption and response procedures
☐ **11. Data Classification and Handling**	• Define data sensitivity levels • Establish storage and transmission rules • Outline destruction protocols
☐ **12. Incident Postmortem and Lessons Learned**	• Conduct root cause analysis • Document improvement plans • Share findings with stakeholders
☐ **13. Cybersecurity Metrics and Reporting**	• Track patch compliance, incidents • Monitor phishing test results • Report regularly to leadership
☐ **14. Interagency and Judicial Collaboration**	• Join incident response efforts • Participate in info-sharing forums
☐ **15. Privacy-by-Design and Data Minimization**	• Apply privacy-by-design to all tech • Collect only essential data • Audit regularly for compliance

NCSC

National Center for State Courts
300 Newport Avenue | Williamsburg, VA 23185
(800) 616-6164 | **ncsc.org**