JOINT TECHNOLOGY COMMITTEE
COSCA | NCSC | NACM

Cybersecurity Incident Planning and Response for Courts

JTC RESOURCE BULLETIN UPDATED | SEPTEMBER 2025

Abstract

Cybersecurity incidents are no longer hypothetical risks for courts—they are an operational reality. From ransomware to data breaches, today's cyber threats are increasingly sophisticated, widespread, and disruptive. Courts must be prepared to act swiftly and decisively to mitigate damage, protect sensitive data, and maintain public trust.

This bulletin provides judicial leaders, administrators, and technology teams with a practical framework for cybersecurity incident response. It emphasizes the importance of proactive planning, clear roles and responsibilities; internal and external coordination; and continuous improvement. Topics include incident detection and triage, containment strategies, forensic considerations, communication protocols, recovery operations, legal compliance, and post-incident review.

While the bulletin draws on best practices from cybersecurity and emergency management disciplines, it is specifically tailored to the unique governance, operational, and confidentiality requirements of the judicial system. It also highlights collaboration across agencies, courts, vendors, and law enforcement partners to ensure a cohesive and effective response.

The ability to respond confidently and competently to a cyber incident is not only a matter of technical readiness, but also a cornerstone of court resilience. By investing in planning, testing, training, and governance, courts can better protect their data, operations, and reputation in the face of today's digital threats.

Document History and Version Control			
Version	**Date Approved**	**Approved by**	**Brief Description**
3.0	9/2025	JTC	Substantially revised and updated document.
2.0	7/2019	JTC	Substantially revised and updated document.
1.0	2/17/2016	JTC	Released document.

Suggested Citation: *JTC Resource Bulletin: Cybersecurity Incident Planning and Response 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

Abstract ii

Document History and Version Control ii

Acknowledgments iii

Executive Summary 6

Introduction 7

Lay the Groundwork 9

- **Identify Your Court's Important Data Assets** 9
- **Risk Assessment and Analysis** 10
- **Recovery Time Objectives (RTO)** 10
- **Recovery Point Objective (RPO)** 10
- **Document Systems** 11
- **Create Multilevel Redundancy with Data Backups** 11
- **Anticipate the Impact of Data Loss or Compromise** 12
- **Enable Logging and Implement Automated Monitoring** 12
- **Be Familiar With Laws Governing Data Collection and Privacy** 13
- **Anticipate Malicious Intent** 14
- **Map Out the Threat Surface** 14
- **Review Terms and Conditions of Contracts with Vendors** 15

Develop the Plan 16

- **Create a Cybersecurity Incident Response Team** 17
- **Plan Primary and Secondary Communication Channels** 19
- **Identify Tasks and Responsibilities** 19
  - Figure 1 - ABCs of Cyber Incident Response 20
  - Access 21
  - Block 24
  - Collect 25
  - Document Response Efforts 26
  - Coordinating with Vendors and External Partners 27
  - Disseminate 29
- **Notification and Coordination During a Cyber Incident** 31
  - Judges and Court Personnel 31
  - Operational Contingencies and Support 32

Law Enforcement 34
Other Courts and Agencies 34
Potential Victims 35
The Media 36

Test and Update the Plan Regularly 40
Exercises and Training 41

Conduct Cybersecurity Tabletop Exercises in Courts 42

Conclusion 44

Appendix A: About Cyberattacks 45
Targeted and Opportunistic Attacks 45
Targeted Attacks 45
Opportunistic Attacks 47
Cyberattack Tactics 47
Unauthorized Access 47
Malware and Viruses 48
Attacks That Disrupt Service 50
Ransomware 50
Zero-Day Exploits 51

Appendix B: Cybersecurity Tabletop Exercises 52
Cybersecurity Tabletop Exercise Scenario for Courts 52
Objective 52
Exercise Participants 52
Exercise Notes 52
Exercise 53
Scenario Summary 53
Activation 53
Assessment 53
Containment 53
Communication 53
Continuity of Operations 54
Recovery and Lessons Learned 54

Executive Summary

Cybersecurity threats continue to escalate in scope and sophistication, putting courts at increasing risk of disruption, data loss, and reputational harm. As custodians of sensitive information and vital justice services, courts must be equipped to manage and respond to cyber incidents confidently and effectively.

This bulletin provides court leaders with a strategic, practical framework for planning, preparing, and executing an effective response to cybersecurity incidents. Drawing from real-world examples and national best practices, it highlights the critical components of a court-specific incident response strategy, including:

- Formation of a cross-functional incident response team with clearly defined roles and responsibilities.
- Legal, regulatory, and policy considerations that must shape the court's incident response posture.
- Communication strategies for internal stakeholders, the public, and media during an incident.
- Vendor coordination, system isolation, forensic investigation, and recovery planning.
- Exercises, training, and regular testing to ensure readiness and continuous improvement.

Cybersecurity incident planning is not a one-time exercise; it is an evolving, enterprise-wide responsibility. By adopting the recommendations in this bulletin, courts can reduce vulnerability, limit damage from attacks, and maintain public confidence in their ability to administer justice under challenging conditions.

Introduction

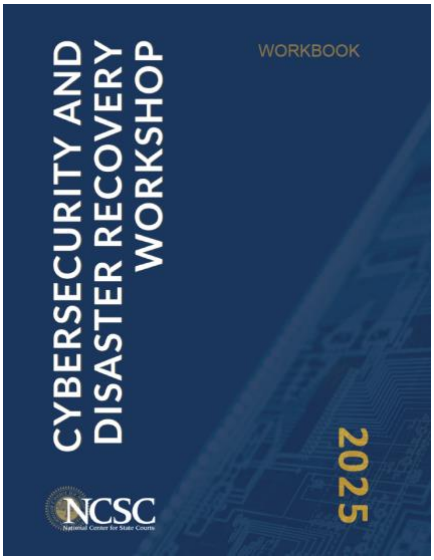
Cyberattacks targeting courts and other public institutions are no longer rare or hypothetical; they are a present and persistent threat. Courts hold highly sensitive information, manage mission-critical operations, and often depend on shared infrastructure and limited resources. These factors make the judicial system a particularly vulnerable and high-value target for cybercriminals and nation-state actors alike.

In this evolving threat landscape, courts must take proactive steps to develop, maintain, and exercise a comprehensive cybersecurity incident response plan. A successful response requires more than just technical tools. It requires clearly defined roles, coordinated communication, tested procedures, and a culture of accountability across the organization. This bulletin provides a roadmap for court leaders and technologists to prepare for and respond to cybersecurity incidents with confidence and clarity.

> *Cybersecurity isn't just about protecting systems; it's about protecting trust. Courts must be ready to act swiftly and strategically when incidents occur, not only to secure data but to maintain public confidence.*
>
> - Adapted from current best practices in public sector cybersecurity planning

This document outlines critical components of incident response planning, including stakeholder coordination, communication protocols, legal and regulatory considerations, and operational continuity. It emphasizes the importance of pre-established relationships with vendors, interagency partners, and IT professionals who may assist during a crisis.

Courts that prepare thoughtfully, exercise their plans regularly, and engage all personnel including judges, clerks, and external partners will be best equipped to withstand a cybersecurity incident and recover effectively.



Valuable Resource:

Hosted by NCSC and funded by the State Justice Institute (SJI), courts are encouraged to incorporate materials from the 2024/2025 Cybersecurity and Disaster Recovery Workshops into their cybersecurity planning efforts. These materials offer practical guidance, planning templates, and real-world examples that can significantly strengthen court preparedness.

Note: Specific highlights and tools from the accompanying NCSC Cybersecurity Planning Workbook and Template are emphasized throughout this paper to support actionable planning and implementation.

Lay the Groundwork

An effective incident response plan requires that several key components be in place before an incident occurs. The plan must be developed with an understanding of the court's essential data assets, potential vulnerabilities, and the legal requirements related to data collection, privacy, and victim notification. Courts also need tools in place to monitor these data assets and detect intrusions.[1]

Identify Your Court's Important Data Assets

Courts must anticipate the potential impact of the loss, theft, or unauthorized alteration of essential data assets. These include, but are not limited to, judges' orders, court records, witness identities and testimony, juror information, digital court recordings, financial transaction data, digital evidence, and personnel records. Creating a comprehensive inventory of these assets is a critical first step in any cybersecurity preparedness plan.

Courts should also account for data held by third-party vendors on their behalf. Key questions include: What data exists? Where is it stored? What is its value, both to court operations and to potential cybercriminals? This assessment must go beyond traditional financial or personally identifiable information (PII), such as credit card numbers, Social Security numbers, and birth dates. In today's digital court environment, judicial decisions, audio/video evidence, and case-related communications represent highly sensitive assets that are equally attractive targets for cyber threats.

An up-to-date asset inventory lays the foundation for further risk analysis and the development of appropriate safeguards.

*See **NCSC Workbook**.*
The Endpoint Inventory tool within the NCSC Workbook supports comprehensive documentation of all network-connected hardware, including but not limited to servers, laptops, desktops, mobile devices, AV equipment, and printers. This inventory is essential during containment and restoration phases to scope the impact of an incident and prevent reinfection.

[1] Joint Technology Committee (2025). *JTC Resource Bulletin: Cybersecurity Basics for Courts Version 4.0*

Conduct Risk Assessment and Analysis

A foundational component of cybersecurity planning is conducting a thorough risk assessment. This involves categorizing data assets, assigning relative value, and evaluating the likelihood of compromise or loss. The process also estimates the potential financial, operational, or reputational impact if assets are disrupted or breached.

The assessment should identify potential vulnerabilities and recommend appropriate countermeasures, along with an analysis of their costs and effectiveness. This enables courts to assign tolerance thresholds for acceptable downtime and data loss for each asset, also known as Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Once these parameters are defined, decision-makers can perform a cost-benefit analysis to prioritize investment in cybersecurity controls.

*See **NCSC Workbook**. Courts should use the Technology Priorities Table within the NCSC Workbook to inventory critical systems, assess interdependencies, and document RTOs and RPOs. This supports deliberate sequencing during system restoration and reduces the likelihood of cascading failures.*

Recovery Time Objectives (RTO)

RTOs refers to the maximum acceptable duration of system downtime following a disruption before it significantly impacts court operations. Courts should evaluate and assign RTOs for each critical system or function. These values guide the level of investment in preventative and recovery countermeasures, helping to ensure essential services can be restored within the defined timeframe.

Recovery Point Objective (RPO)

RPO defines the maximum acceptable amount of data loss measured in time. For example, if backups are performed once nightly up to 24 hours of data could be lost. Courts must determine acceptable data loss thresholds for each data asset and design backup strategies to meet those thresholds.

Document Systems

Thorough documentation of system configurations, services, dependencies, and recovery procedures is essential for an efficient and coordinated recovery. Up-to-date documentation helps identify vulnerabilities, supports disaster recovery planning, and aids in post-incident assessments.

Key documentation practices include:

- Maintaining current documentation for all network and application systems.
- Identifying and tracking interdependencies among systems, especially those that affect recovery sequencing.
- Fully documenting all backup and recovery procedures, storage locations, and recovery sequencing.

Create Multilevel Redundancy with Data Backups

Redundant and diverse backups significantly reduce the risk of permanent data loss. A best practice is to maintain at least one isolated, offline, immutable, and offsite backup. Only store backups on the same network, as production systems exposes them to simultaneous compromise in a cyberattack.

Best practices for data backup and redundancy:

- Test backups regularly by restoring randomly selected files.
- Periodically perform a full system restore to verify recoverability.
- Maintain at least one complete backup offline and offsite. Ideally a complete backup should be "air-gapped" and physically disconnected from the internet.
- Use long-term backup retention schedules, ideally covering several months, to account for latent attacks.
- Audit backup sets to ensure no critical data is excluded.
- Invest frequently in modern backup technology to ensure a comprehensive approach incorporates frequent snapshots and immutable backups.

Configure systems to automatically save to backup locations and train court users to follow backup protocols when prompted.

Anticipate the Impact of Data Loss or Compromise

Anticipate the impact of losing access to this data or having it altered or otherwise compromised. Identify which court functions depend on which data sets and build in redundancies to ensure the quick recovery or restoration of information following an incident.

> *See **NCSC Workbook**. To effectively triage resources during a disruption, courts should complete the Essential Functions Table found in the NCSC Workbook. This allows leadership to focus on statutorily required services, such as arraignments, protective orders, and emergency warrants, and align them with realistic RTOs.*

Enable Logging and Implement Automated Monitoring

Just as monitoring courthouse entrances with closed circuit television does not prevent incidents but aids in response and investigation, system logging and automated monitoring are foundational cybersecurity practices that significantly enhance a court's ability to detect, investigate, and respond to incidents.

To maintain effective oversight, courts should:

- Capture and retain log information from all critical infrastructure components, including switches, routers, proxy servers, firewalls, and authentication systems.
- Store logs in a secure, tamper-resistant location that remains isolated from production networks. Sophisticated attacks often target both logs and backups to obscure detection and hinder recovery.
- Use login banners or warnings to inform court personnel their activities may be monitored and recorded, reinforcing transparency and compliance with privacy policies.
- Utilize the full capabilities of monitoring and diagnostic tools, anticipating their critical role in incident response and forensics.

Implement real-time security monitoring and intrusion detection/prevention systems that analyze network activity and automatically generate alerts when suspicious behavior is detected.

Be Familiar With Laws Governing Data Collection and Privacy

Courts must not only protect the PII they collect but obtain consent from system court personnel to monitor communications as part of their cybersecurity strategy. Monitoring tools and system logging are vital for detecting and responding to intrusions, but they must be supported by appropriate legal consent. This consent can typically be obtained through login banners or user acknowledgment warnings, which must be in place prior to any incident or monitoring activity.[2]

Courts are not immune from the legal and financial consequences of a data breach. Many jurisdictions impose statutory penalties for failure to safeguard personal data or to notify affected individuals in a timely manner. In the event of a breach, courts may be held liable for delayed or incomplete victim notification.

It is especially important for courts to be aware of both federal and state data breach notification requirements.[3] Federal laws such as the Privacy Act of 1974,[4] and state-specific laws such as Virginia's Personal Information Breach Notification Act,[5] may impose strict timelines and conditions for notification. Some laws include compounded penalties for delayed reporting or failure to notify.

Notification obligations often hinge on whether data exfiltration (e.g., unauthorized data removal) has occurred and the type and volume of data affected. This highlights the need for courts to implement effective system monitoring and retain digital forensic tools capable of identifying whether and what data was accessed or exfiltrated.

---

[2] CISA. (2021). *Incident response recommendations*. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov

[3] National Conference of State Legislatures (NCSL). (2023). *Security breach notification laws*. https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

[4] U.S. Department of Justice. (2020). *The Privacy Act of 1974*. https://www.justice.gov/opcl/privacy-act-1974

[5] Virginia Code § 18.2-186.6. (2023). Personal information; notification of breach. Virginia General Assembly. https://law.lis.virginia.gov/vacode/title18.2/chapter6/section18.2-186.6/

Anticipate Malicious Intent

Courts that have experienced a successful and disruptive cyberattack emphasize the importance of not underestimating malicious intent. Cyberattacks may not only target data but also recovery tools, backups, and monitoring systems. In some cases, a secondary attack is launched during the recovery phase to further impair incident response efforts.

Several court managers noted they had not anticipated the level of malicious intent behind cybersecurity incidents. A more realistic understanding of potential motives would have prompted greater caution and faster action.

Understanding potential threat motivations, such as financial gain through ransomware, operational disruption, erosion of public trust, or reputational damage, is essential. By identifying likely threat actors and their intent, courts can effectively prioritize cybersecurity planning, investment, and response strategies.

Recognizing attackers may deliberately sabotage recovery efforts reinforces the need for multi-layered defenses, tested backups, and offline redundancies.

Map Out the Threat Surface

The threat surface (sometimes called the attack surface) includes all points of entry and vulnerabilities, from network interfaces and services to physical devices, through which an unauthorized actor could access or compromise systems and data. This surface extends beyond the internal network and firewall; it now includes remote connections, cloud services, mobile devices, third-party vendors, and even the home networks of court personnel. As courts continue to adopt digital tools and hybrid work environments, the threat surface is constantly expanding and evolving. Identifying and regularly reassessing this surface is a critical step in effective prevention planning.

The threat surface not only includes network and software vulnerabilities, but also human factors and physical infrastructure. Courts should identify all potential points of entry, including open ports, external internet connections, untrained or undertrained staff, and system integrations with other organizations and governmental agencies. Third-party connections, particularly to non-data systems such as HVAC, alarm systems, copiers, door access controls, and other internet-connected devices, should also be assessed for vulnerabilities.

Because technologies and configurations change frequently, new vulnerabilities can be introduced at any time. It is essential to review the threat surface regularly, and at a minimum, conduct a reassessment whenever a new system is implemented, or a significant upgrade occurs.

Review Terms and Conditions of Contracts with Vendors

Courts must carefully review the terms and conditions of contracts with vendors, particularly those that manage court data or host critical applications. A clear understanding of each vendor's cybersecurity responsibilities is essential.

- **Notification Requirements**
  Contracts should require vendors to provide immediate notification of any known or suspected cybersecurity incident, even if the breach was discovered months after it occurred. Notification should not be delayed until the full scope of the incident is confirmed.
- **Security Updates**
  Ensure vendor agreements include obligations to provide timely security patches and updates, not only for the vendor's own software but also for third-party components integrated into their solutions. This is particularly important in hosted or cloud environments where patching timelines can significantly impact risk.
- **Audit Rights**
  Contracts should grant the court the right to audit the vendor's security protocols and practices on a regular basis. This helps ensure ongoing compliance with agreed-upon cybersecurity standards.
- **Inclusion in Incident Response Planning**
  Confirm the court is explicitly included in the vendor's cybersecurity incident response plan and communication protocols are defined in advance.
- **Integration of Continuity of Operations Plan and Disaster Recovery**
  For vendors that host court applications or data, their services and platforms should be formally incorporated into the court's Continuity of Operations Plan (COOP) and Disaster Recovery (DR) planning. Vendor participation in COOP exercises may also be appropriate, depending on the level of service they provide.

Develop the Plan

Establish and document clear procedures to follow when a cybersecurity incident is identified. Start by identifying your court's specific vulnerabilities so you can plan for the most likely scenarios. Ensure the response procedures are practical, reflect your court's organizational structure, and align with existing policies. Update or revise policies and processes to support an effective response as necessary.

> *Pre-planning can help victim organizations limit damage to their computer networks, minimize work stoppages, and maximize the ability of law enforcement to locate and apprehend perpetrators.*[6]

Avoid simply copying a model plan. While such templates are convenient, they often contain assumptions, expectations, or commitments your court may not be able to meet. These gaps may only become apparent when the plan is tested, or worse, during a real incident.

A strong response plan should detail:

- **Who** will be involved
- **What roles** each individual will play
- **How** the team will communicate internally and externally and who will be the primary messenger
- **What steps** are each person's responsibility
- **When** each task must be completed

The plan must be secure to prevent cyberattackers from learning of the response. It must also be accessible to the cybersecurity incident response team, even if members do not have access to the affected systems.

[6] United States Department of Justice (DOJ). Computer Crime and Intellectual Property. Best Practices for Victim Response and Reporting of Cyber Incidents. Version 1.0. Washington, D.C.: Cybersecurity Unit, April 2015. Web.

Create a Cybersecurity Incident Response Team

The court's cybersecurity incident response team should include representatives from all departments or divisions involved in incident management and communications, including both internal and external stakeholders. At a minimum, the team should include the following.

- **Chief/Presiding Judge/Justice**
  As the public face of the court, the chief/presiding judge or justice often serves as the primary spokesperson or point of interest by the press, other branches of government and the public at large.
- **Court Administrator/Chief Executive Officer**
  Coordinates court operations and allocates the resources needed to execute the response plan while ensuring continuity of business.
- **Chief Information Officer**
  Leads the technical aspects of the response and coordinates with IT support staff and vendors.
- **Information Technology (IT) Security Officer**
  Ensures compliance with legal and regulatory mandates. May collect digital forensic evidence and serve as a liaison to law enforcement and external agencies.
- **Public Information Officer (PIO)**
  Assists the chief judge/justice by providing accurate, up-to-date information for communication with the public and media.
- **Human Resources (HR)**
  Participates if the incident affects court employees, supporting communication, employee-related procedures, and employee well-being.
- **Chief Financial Officer (CFO)**
  Coordinates the expenditure of funds to address the response, including forensic consultant, any necessary equipment purchases, subscriptions to protect against future attacks, etc. and how to make such purchases confidential if possible.
- **Legal**
  Advises on the legal implications of the court's response and works to minimize legal risk.

The cybersecurity incident response team should develop a communication plan in advance of any incident. The plan should clearly identify who is authorized to speak on behalf of the court to both external and internal stakeholders. It should also address how messaging will be coordinated if the incident affects multiple parts of the court or other branches of government to ensure a consistent and accurate message is delivered.

> *See **NCSC Workbook**. To support the development of a comprehensive response structure, courts should complete the Crisis Management Team and Cyber Incident Response Team directories provided within the NCSC Cybersecurity and Disaster Recovery Workbook. These templates help designate individuals responsible for executive, legal, communication, and technical functions, facilitating coordinated response across court leadership, IT, and external partners.*

During an active incident, the team should meet regularly to review procedures and have constant access and frequent communication with each other to assess the situation and determine next steps. Each member brings a vital perspective to ensure a comprehensive and coordinated response.

Plan Primary and Secondary Communication Channels

Anticipate traditional communication methods such as email, videoconferencing, and phone systems may be unavailable during a cybersecurity incident. Collect and securely store up-to-date contact information for all key individuals and organizations, including court personnel, IT vendors, security teams, and law enforcement. Be sure to include daytime and after-hours/weekend contact details.

Depending on the court's structure, the designated IT contact may not be a court employee. In some jurisdictions responsibilities may fall under a county or municipal IT department. Your response plan should reflect these realities and account for any interdepartmental and cross-functional communications to ensure a cohesive response.

To make information readily accessible during an incident response plans and contact lists should be available in multiple formats. Digital copies can be stored on team members' smartphones or through a secure app. At least one paper copy should be maintained in a designated location accessible to authorized personnel.

> *See **NCSC Workbook**. Courts should document available communication methods using the Communication Modalities Table found within the NCSC Cybersecurity and Disaster Recovery Workbook. Identifying and validating multiple communication channels, such as SMS alerts, cloud portals, and emergency conferencing, ensures the court can maintain contact with stakeholders when standard tools fail.*

Identify Tasks and Responsibilities

Clearly identify and define the tasks that must be performed in response to an incident and assign responsibility for each task. The plan should also designate backup personnel in case a primary is unavailable.

While the IT team will take the lead in addressing technical issues it should not be the only department involved in the response. Coordination across departments is essential. Identify in advance who will serve as the court's spokesperson—whether it be the chief judge or justice, the PIO, or another designated court leader—and ensure that only the authorized spokesperson communicates publicly about the incident.

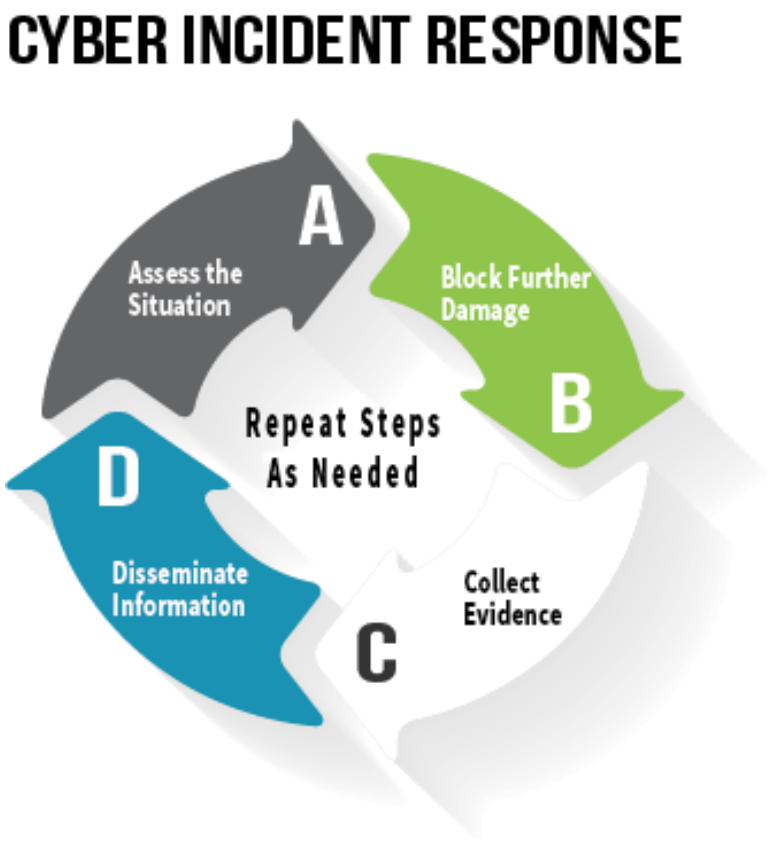
Having conflicting or even multiple messages from different "official" sources can lead to confusion and undermine public confidence. Consistent messaging is key. Regular team meetings during the incident are critical to maintaining

coordination and ensuring information is shared accurately, effectively, and in a timely manner.

Similar to the "ABCs of First Aid," which prioritize life-saving actions, a cybersecurity response plan must address critical elements swiftly and decisively. **Figure 1 – ABCs of Cybersecurity Incident Response** introduces four essential task categories: **Assess, Block**, **Collect**, and **Disseminate**. These categories do not represent a rigid, sequential process. Instead, they are functional groupings of actions that may be revisited multiple times as the incident evolves.

The order in which the tasks are carried out will vary depending on the nature of the cybersecurity event: how it was discovered, when it occurred, and who identified it. Flexibility and responsiveness are key as effective incident management requires adapting these tasks to the unique circumstances of each event.

FIGURE 1 - ABCS OF CYBER INCIDENT RESPONSE



Access

Recognizing a cybersecurity incident is essential. While that may seem obvious, attackers often dwell undetected in systems for extended periods. According to IBM's Cost of a Data Breach Report 2025, the global average breach lifecycle, which is the time to identify and contain a breach, is now 241 days or approximately eight months.[7]

Treat any suspicious event as an intrusion, even before it is confirmed. It is better to act and later determine it was a false alarm than to wait and risk increased damage. In some cases, literally disconnecting from the internet may be the best immediate action while evaluating whether the issue stems from intrusion, malfunction, or user error.

IDENTIFY THE INTRUSION

Detection can occur through multiple channels:

- **Automated security alarms** (e.g., from intrusion detection systems or endpoint protection tools) may notify IT of a suspected intrusion.
- **Public-facing indicators** such as a defaced court website or unexpected redirects may be identified by the public before staff are aware.
- **Individual victims** such as court personnel, litigants, or jurors, may report compromised personal information traced back to the court.
- **External parties** in some cases may be the first to notify a court of a breech. These external parties can be the media or federal agencies like the FBI.

Unfortunately, courts may not be the first to identify a breach: in 2020, only 59% of incidents were detected internally by the affected organizations.[8] There have been situations where individuals discover their private information has been exposed and trace the exposure back to the court.

[7] IBM. (2025). *Cost of a data breach report 2025*. IBM Security. Retrieved August 2025, from https://www.ibm.com/reports/data-breach

[8] Verizon. (2020). *2020 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/

UNDERSTAND THE NATURE OF THE INTRUSION

The signs of a cyberattack vary depending on the type of attack. Some are obvious, while others may go unnoticed without proper monitoring. The following are common indicators of an intrusion.

- **Phishing Messages**

  Phishing is a form of social engineering in which an attacker impersonates a trusted source, such as a supervisor, colleague, judge, or external stakeholder, to trick recipients into revealing sensitive information or clicking malicious links.

  Sophisticated phishing messages may come from spoofed email addresses that closely mimic real addresses within the court, law firms, prosecutors' offices, or vendors. Unlike obvious scams promising lottery winnings, these messages are carefully crafted to look authentic and invoke urgency.[9]

- **Slow Connections**

  In a Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack, attackers flood systems with an overwhelming volume of malicious requests. This exhausts system resources, causing slow performance, errors, and potential service outages. Unexplained performance degradation, such as slow page loads, delayed file access, or widespread connectivity issues, can be among the first indicators that a DoS-related attack is underway.

  - The United States Cybersecurity and Infrastructure Security Agency (CISA) lists unusually slow network performance such as delays opening files or accessing websites as a key symptom of a possible DoS/DDoS.[10]
  - Security analysts also highlight slow loading times, unexplained timeouts, and increased memory or CPU usage as common signs that a DDoS attack may be occurring.[11]

- **Malicious Pop-ups**

  Pop-ups that claim to alert court personnel to a cybersecurity threat may, in fact, be the threat itself. These often disguise links to malicious websites,

[9] CISA. (2023). *Phishing guidance*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/news/phishing-guidance

[10] CISA. (n.d.). *Understanding denial of service attacks*. https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

[11] eSecurity Planet. (2023). *How to tell if you've been DDoSed: 5 signs of a DDoS attack.* https://www.esecurityplanet.com/networks/how-can-you-tell-if-youve-been-ddosed/

advertisements, or fraudulent downloads. Clicking on these pop-ups may trigger malware installation or redirect court personnel to phishing pages.[12]

- **Ransomware**

  Ransomware is designed to be immediately noticeable. This form of malware encrypts data or locks court personnel out of systems and demands payment, often in cryptocurrency, to restore access. Courts experiencing ransomware attacks may face halted operations, inaccessible case files, and data exfiltration.[13]

ASSESS THE SCOPE AND IMPACT

Use automated logging and monitoring systems to determine the scope of the intrusion. Log data can help identify which IT assets have been compromised, when the intrusion occurred, and how the incident unfolded.

SYSTEMATICALLY ASSESS IMPACT

Begin by systematically evaluating the extent of the breach across networks, hardware, applications, and data files. Where feasible document:

- When the incident began and how long it remained undetected
- The methods used by the attacker (e.g., phishing, malware, credential theft)
- The specific assets impacted and the nature of the compromise
- The potential for lateral movement to other IT assets or systems
- The operational and reputational impact on court personnel, judicial officers, and justice partners

> ***Keeping log files intact is a key requirement in investigation.*** *Often, an attacker will delete log files to hide their tracks. Have an alert sent to you if a log file is suddenly deleted—this is not normal activity and is often a sign an attacker is on the system. Store logs offsite where the attacker can't gain access and erase the evidence.*[14]

[12] Federal Trade Commission (FTC). (2023). *How to spot, avoid, and report tech support scams.* https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

[13] National Institute of Standards and Technology (NIST. (2022). *Guide for cyber incident handling for federal agencies* (Special Publication 800-61 Revision 2). https://doi.org/10.6028/NIST.SP.800-61r2

[14] SANS Institute. (2023). *Logging and monitoring best practices: Cyber defense essentials*. https://www.sans.org/white-papers/logging-monitoring-cyber-defense/

A thorough and accurate assessment is essential to guide an effective and proportional response. Although no organization can respond flawlessly under pressure, assembling and analyzing the best available information will support timely decisions and minimize disruption.

COMMUNICATIONS CONSIDERATIONS

Consider whether initial response steps should be made public. In some cases, it may be strategic to maintain the appearance of normal operations, at least temporarily, to prevent tipping off bad actors that their presence has been detected or to avoid disclosing vulnerabilities. If the issue is publicly visible (e.g., your website is down), you may need to issue a brief public statement acknowledging the disruption.

Consider whether judges and staff beyond the incident response team need to be informed immediately. While limiting internal awareness can help control the spread of sensitive information, certain employees may need to take urgent action to mitigate further harm. Additionally, the incident may impact business operations or court proceedings in ways that require timely internal communication.

Block

Preventing further damage is the highest priority. Disruptive but necessary actions such as removing infected devices, disabling network access, or temporarily taking the court's website offline may be required to contain the incident. In some cases, restoring data from clean backups or even replacing infected machines may be the most efficient route to recovery.[15]

When working to block further damage, take the following steps:

- Maintain a detailed log of all containment and recovery actions, including timestamps, personnel involved, and tools used. This will assist with later forensics and internal reviews.
- Apply available software patches promptly to address known vulnerabilities exploited in the attack.[16]
- Reset user credentials and create new, complex passwords. Multifactor authentication (MFA) should be enabled wherever possible to prevent reentry.
- Expand system monitoring and intrusion detection tools to detect persistent threats or attempted reentry by attackers.

---

[15] CISA, *supra*.

[16] NIST, (2023). *Computer security incident handling guide* (NIST Special Publication 800-61 Revision 3). https://doi.org/10.6028/NIST.SP.800-61r3

- Reinforce physical security protocols. Cyber incidents may lead to on-site confusion, making physical areas (like server rooms) more vulnerable. Keep sensitive areas locked and limit access to authorized personnel only.

> ***Important Legal Consideration:*** *Do not attempt to retaliate against an attacker by "hacking back" or accessing external systems believed to be the source of the intrusion. Under U.S. law, unauthorized access to other systems, even if retaliatory, is illegal and may result in civil or criminal liability.*[17] *Additionally, attackers often use compromised systems as proxies, so such action may harm innocent third parties.*

COMMUTATIONS CONSIDERATIONS

Your court may not have full control over the systems targeted by the incident. Understand in advance who owns and manages your IT infrastructure and how decisions are made in the event of an emergency. Key questions include:

- Can another agency or department restrict your access to critical networks or systems?
- Can a vendor, legally or practically, restrict your access to critical networks or systems?
- Do you have established communication protocols and working relationships with those entities?

If your court depends on external agencies for IT infrastructure identify those dependencies ahead of time and to securely store contact information in both digital and physical formats in case internal systems are inaccessible during a cyber event.

Collect

No court has unlimited resources, and some courts may be tempted to limit their response to simply blocking the attack and resuming normal operations. However, it is essential courts gather comprehensive data about the incident and conduct a thorough investigation. Understanding what occurred is crucial—not only for identifying the intruder but also for preventing further intrusion and strengthening long-term cyber resilience.[18]

Thorough data collection and analysis refine the initial assessment of the damage and guide additional efforts and decisions. Essential details to capture include:

---

[17] DOJ, *supra*.

[18] NIST. (2018). *Computer Security Incident Handling Guide* (Special Publication 800-61 Revision 2). https://doi.org/10.6028/NIST.SP.800-61r2

- Machines affected
- Type, origin, and duration of the incident
- Malware used
- Identity of the victims

Do not modify or delete files that may be necessary to investigate the incident. If the court's IT department lacks the resources or expertise to manage the investigation, a cybersecurity firm should be retained. This relationship should be established before an incident occurs.

CAPTURE FORENSIC INFORMATION

Using new or sanitized media creates a "forensic image" of affected computers. According to the U.S. Department of Justice, forensic imaging is a critical first step in preserving a digital record of a system at the time of compromise which may later be used for legal proceedings or analysis. The image must be created using forensically sound procedures including write-protection and strict chain-of-custody documentation to preserve evidentiary value.[19]

There may be digital "breadcrumbs" that trace back to the perpetrators. These can reveal motives, such as data theft, operational disruption, ransomware deployment, or reputational damage. Digital evidence can also indicate attacker skill level, such as whether the code used is unique or adapted from known hacking tools.[20]

Examples of Forensic Details To Collect

- *Logs and file creation/ modification data*
- *Unauthorized changes to system settings*
- *Creation or modification of user accounts or permissions*
- *Existence of unauthorized hidden files*
- *"Hacker tools" or remnants of other unauthorized activity*

Document Response Efforts

Maintaining a comprehensive record of the response process is vital for legal, operational, and improvement purposes. The cybersecurity incident response plan should designate who is responsible for documentation and what they are expected to record.

[19] DOJ, *supra*.
[20] CISA, *supra*.

Essential documentation elements include:

- Timeline of events and activities
- Phone calls
- Emails
- Other contacts
- Inventory of systems and software (including version)
- System names and configurations
- Accounts and access levels
- Active services
- Stored data
- Personnel and vendors involved
- Roles and responsibilities
- Contact information
- Tasks performed

Thorough documentation not only supports post-incident analysis but can also serve as a roadmap for future response improvements and evidence in legal proceedings.

Coordinating with Vendors and External Partners

Vendors:

Use available private procurement processes or waive procurement processes, if possible, when contracting with cybersecurity vendors or services to ensure your court's system architecture and response plans are not publicly disclosed.

> ***Important!***
> *If your court carries cybersecurity insurance, the policy may require that you work with specific incident response or forensic service providers. Be sure to review your policy in advance to understand both the available options and any contractual requirements. Failure to comply with your insurer's terms could affect coverage eligibility during a breach response.*

If you contract with a vendor for incident response or forensic services, consider how the vendor will support you if it becomes necessary to disconnect your court from the internet. Many vendors rely on internet connectivity to remotely access and perform diagnostics. Be aware of the trade-offs involved:

- Can an initial assessment be completed before disconnection?
- Are there time zone differences that might impact response time?
- If the vendor collects physical equipment (e.g., computers or hard drives), is there a documented chain of custody process in place to track each item and ensure proper return?
- How will the vendor store and secure your data and devices during the investigation?

Also consider whether any portion of the forensic report will be shared publicly. In most cases these reports are kept confidential to avoid exposing system vulnerabilities to potential attackers. While you may implement changes based on the report's findings, the specifics should remain protected.

Partners:

Proactively build relationships with other agencies and key stakeholders to establish "bridge connections," prearranged, secure communication channels and operational protocols. These networks can be crucial during a crisis, enabling access to alternative systems and resources.

Such partnerships may be vital for continuing essential administrative functions, like payroll, procurement, and billing, during a disruption. Leveraging the systems of trusted partners helps ensure continuity of operations and minimizes downtime, ultimately protecting both the court and its employees.

To support an effective digital forensic response courts should develop a clear operational plan that includes:

- **Internal Capacity Assessment**
  Determine whether your court has staff with the necessary forensic expertise to conduct timely investigations and preserve digital evidence.
- **External Support**
  If internal resources are lacking, secure agreements with cybersecurity vendors or utilize existing contracts through state or local government entities for immediate support.

- **Collaborative Support**
  Consider formal partnerships with other courts or agencies to allow their forensic experts to provide on-site or embedded assistance during emergencies. This can enable rapid deployment of skilled personnel when needed.
- **Defined Protocols**
  Ensure protocols for information sharing, data access, and confidentiality are clearly established in advance of any incident.

By proactively identifying, formalizing, and documenting these relationships and resources, your court will be better positioned to respond quickly and effectively to cyber incidents, minimizing operational disruption and preserving critical evidence for legal or investigative purposes.

Disseminate

Effective communication is a vital component of any cybersecurity incident response. Timely and accurate dissemination of information is essential for limiting confusion, preserving public trust, and guiding recovery efforts. Courts must ensure communication channels remain operational and secure. Never use systems suspected to be compromised to communicate sensitive or urgent information.[21]

SPEED AND TRANSPARENCY MATTER

The speed of informal communication channels, including word of mouth and social media, can easily outpace formal court messaging. Therefore, early and proactive messaging is critical, even if all details are not yet known.[22]

Courts should avoid the temptation to delay communication until a full understanding of the event has been established. Early communication can include:

- Acknowledgment an incident has occurred
- Known impacts on operations or data
- Contact information for further questions
- Timeline for follow-up updates

Additionally, courts should establish communication protocols with key stakeholders in advance, including:

- Judges and court staff
- Law enforcement and emergency management

[21] NIST, *supra*.

[22] CISA, *supra.*

- Partner agencies (e.g., prosecutors, public defenders)
- The local bar association

This ensures vital information is disseminated quickly and accurately.

USE PRE-APPROVED TEMPLATES

As part of cybersecurity incident response planning, courts should develop and vet communication templates that meet legal and regulatory standards. These can be adapted quickly for use during an incident and reviewed by legal counsel, public affairs, and IT in advance. Examples may include press release outlines, email alerts, and website/social media messages.

DESIGNATED SPOKESPERSON ROLE

A single designated spokesperson, such as the chief judge, trial court administrator, or PIO, should be responsible for public-facing communication. This avoids mixed messages and promotes confidence in the court's leadership and control of the situation.[23]

The spokesperson's key message elements may include:

- Confirmation the court continues to operate (in whatever capacity that may be) and all emergency and essential functions are available, including any temporary process changes implemented in response to the incident.
- A general description of how the attacker gained access (if known), provided the entry point is no longer vulnerable.
- Identification of any data that was potentially compromised or confirmation that no known data was compromised.
- A summary of containment steps that have been taken.
- Guidance on steps individuals should take to protect themselves.
- Actions the court is taking to safeguard affected individuals and systems.
- Instructions on how to obtain additional information.
- The date and time when the next update will be provided.

Where necessary, coordination with law enforcement or partner agencies should occur prior to public release to ensure no investigatory efforts are compromised.

[23] DOJ, *supra*.

Notification and Coordination During a Cyber Incident

Judges and Court Personnel

Court managers, judges, IT staff, facilities personnel, and communication officers should be informed of the incident, its potential impact on court operations, and the steps being taken to respond. The plan should outline when and how court personnel will be notified, based on the court's organizational structure. Information should be shared strategically and controlled carefully.

Identify and document alternative communication methods, including:

- Microsoft Teams or Zoom
- Mass text messaging platforms
- Phone trees
- Cloud-based email or messaging services

Recognize email access may be partially or fully disrupted (e.g., internal access only or external access only). To mitigate this consider using off-premises or cloud-hosted email services as part of your preparedness strategy.

Hold daily briefings with senior managers and administrative judges separate from general staff updates when appropriate. Use teleconference or video conferencing to provide:

- Situation updates
- Response progress
- Upcoming actions and priorities
- Realistic timelines for recovery and restoration

Ensure key personnel are present to answer questions and allow time for discussion. Make clear all official communication will come from the court. Instruct staff and judges—as they should not speak directly to the media—to direct media inquiries to the designated point of contact (POC). Release general high-level public statements initially and ensure internal staff are informed before those statements are made public. Share copies of press releases with all court staff.

Provide clear instructions to staff and judges on how to maintain security during the incident including:

- Do not connect personal or unauthorized devices to the network
- Turn in equipment as directed
- Promptly report suspicious emails or communications

Also, communicate any upcoming security hardening measures, expected disruptions, and required training sessions.

Operational Contingencies and Support

Develop contingency plans for continuing operations if digital systems become unavailable. This may include reverting to manual methods such as paper, fax, and phone-based workflows. The following are key points for courts to consider.

- **Maintain Secure Offline Backups**
  - **Paper-Based Forms:**
    Keep hard copies of critical court forms (e.g., warrants, orders, docket sheets, payment receipts, continuance forms) organized by case type and function.
  - **Procedural Manuals:**
    Print essential operating procedures, emergency response guides, and chain-of-custody documentation. Store these in designated, clearly labeled binders.
- **Use Air-Gapped Digital Storage**
  - Store updated digital copies of court forms, manuals, and contact lists on an encrypted, non-networked device (e.g., a USB drive or external hard drive).
  - Devices should be kept in a secure, easily accessible location (e.g., a locked drawer in the clerk's office or judge's chambers).
- **Train Staff in Manual Operations**
  - Regularly train court personnel on reverting to manual processes for case intake, docketing, filings, and scheduling.
  - Include exercises in tabletop cybersecurity incident simulations to reinforce how staff should document, route, and protect sensitive case information without access to digital systems.
- **Establish Paper Tracking Protocols**
  - Create a logbook system for manually tracking all case filings, orders issued, and case activities during a system outage.
  - Assign a designated staff member to later reconcile paper-based actions with the electronic case management system once restored.
- **Identify Alternate Communication Channels**
  If email or court communication tools are compromised courts should have:
  - Pre-designated landlines or backup phones
  - Pre-drafted notification templates
  - A call tree or group text chain for internal communication

- **Keep a Printed Emergency Contact Directory**
  Include contact information for:
  - Judges and key court staff
  - Law enforcement and public safety officials
  - Local IT/security contacts
  - Partner agencies (e.g., probation, victim services, legal aid)
- **Create a "Go Manual" Binder**
  Include:
  - A printed copy of your cyber incident response plan
  - Key case processing instructions (e.g., intake, calendaring)
  - Emergency orders templates
  - Local rules or directives needed to continue operations offline

Ensure all paper forms and backups are version controlled and reviewed quarterly to reflect current policies and legal requirements. This layered preparedness allows courts to continue critical operations, protect data integrity, and uphold due process, even during severe cybersecurity events.

Ensure you maintain open and effective communication channels with intergovernmental partners and know your court's priority level for IT system restoration. Be prepared to advocate for your needs if multiple entities are affected. Monitor the wellbeing of IT and other critical personnel. During extended incidents, ensure they have opportunities for rest, food, and support.

Set expectations for communication frequency, ideally daily or more often when new information emerges. Be transparent about:

- What is known
- What actions are being taken
- What is expected next

Avoid over-promising. Instead, offer honest, accurate, and timely updates to maintain trust and promote coordinated response efforts.

Law Enforcement

Depending on the nature of the breach, incidents should be reported to one or more law enforcement entities. Preserve all forensic data to support investigation and potential prosecution. For streamlined coordination report all incidents including unsuccessful intrusion attempts to the U.S. Computer Emergency Readiness Team (US-CERT) operated through CISA.[24] Cybercrimes involving intrusion, financial fraud, or suspected criminal activity should also be reported promptly to the FBI via your local FBI field office and the FBI Internet Crime Complaint Center.[25]

Other Courts and Agencies

A cyber event in one court may signal or lead to an attack in another. Even in states with high levels of local autonomy, courts often operate within interconnected networks. As a precaution:

- Notify the State Administrative Office of the Courts (AOC).
- In some jurisdictions, the AOC may have resources or expertise available to assist in the response.

Maintain regular, confidential briefings with funding bodies throughout the event. Doing so builds trust and lays the groundwork for future funding requests related to system hardening and cybersecurity enhancements.

Best practices include:

- Identifying and prioritizing cybersecurity needs.
- Raising those needs at each funding opportunity.
- Referring to the incident as a justification for investment.
- Conducting an internal or external assessment to confirm system vulnerabilities and validate funding requests.

[24] CISA. (n.d.). *Reporting a cyber incident*. U.S. Department of Homeland Security. https://www.cisa.gov/reporting-cyber-incident

[25] U.S. Department of Justice, Criminal Division. (2023). *Reporting computer, internet-related, or intellectual property crime*. https://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime

Potential Victims

When a court's systems are breached, potential victims may include:

- Court personnel
- Partner agencies
- Members of the public, including juvenile and adult defendants, families, jurors, and witnesses

A breach may expose sensitive information such as:

- Personal Identifying Information (PII)
- Case data
- Personnel records
- Information related to witnesses or individuals under protective orders

Most or all states have enacted data breach notification laws requiring courts to notify affected individuals when their PII is compromised. While all 50 states now have such laws, each one differs in scope, timing, and specific requirements, especially regarding government or public entities. Courts must monitor applicable state statutes and any legislative changes and incorporate these obligations into their incident response plans.[26]

In many jurisdictions courts are expected to treat the public as "customers" and act accordingly if PII is compromised. In certain cases, notification requirements may be waived if law enforcement determines that notifying victims would impede an investigation.[27]

Key Questions to Consider

What are your court's specific legal responsibilities for notifying individuals if their PII is compromised?

Are your notification procedures clearly documented in your cybersecurity response plan?

Do you have protocols for coordinating with law enforcement and funders before initiating public or individual notifications?

[26] National Conference of State Legislatures (NCSL). (2022). *Security breach notification laws*. https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

[27] DOJ, supra.

The Media

Preserving public trust depends on transparent and coordinated communication. Communications should come through official channels and be consistent, avoiding rumors or misinformation.

- Share timely, factual information about the breach and response.
- Establish a cadence and format for follow-up updates, as uncertainty and vagueness can erode public confidence.

BEST PRACTICES FOR MEDIA COMMUNICATION

- **Avoid informal channels**
  All updates should be provided through official, secured channels.
- **Expect to release a statement early**
  You may need to make a public statement before all details are known, even while the breach is ongoing.
- **Set expectations**
  Clarify how and when future updates will be provided and stick to that schedule. Inconsistent or vague communication can create confusion and erode public trust.

PREPARE MESSAGING TEMPLATES IN ADVANCE

While you cannot anticipate the exact content of messaging ahead of an incident, having a framework in place is essential. Your external communication plan should include the following.

- Templates for press releases, website notices, and social media posts.
- Sample language to reassure the public that court operations will continue for priority matters.
- Procedures for launching a temporary website if the main site is compromised.
- Clear designation of a spokesperson who understands the information release authorization process.

INTERNAL MESSAGING CONSIDERATIONS

Assure court personnel, including judges, staff, volunteers, and contractors, of the court's ability to continue operations in modified form. Acknowledge their efforts, reinforce their role in the response, and keep them updated on changes and expectations. Internal communications must align with external messaging but may include additional operational detail.

MEDIA SPOKESPERSON COORDINATION

Designate a single spokesperson for external communications. Typically, the PIO, trial court administrator, chief or presiding judge or justice acts as the public facing spokesperson. This person should:

- Coordinate closely with internal communications staff.
- Be well-versed in messaging protocols and authorization.
- Provide consistent and transparent information.
- Redirect all media inquiries to the designated POC.

TIMING AND CONTENT OF PUBLIC STATEMENTS

Once initial intelligence is gathered (usually within a few days), issue a well-crafted press release. The release should:

- Provide as much detail as possible without compromising the investigation.
- Offer enough substance to satisfy the media and reduce follow-up questions.
- Use general descriptions of systems (e.g., e-filing, case management) for clarity.

PREPARE FOR KEY QUESTIONS

Be ready to address the following:

- What type of attack occurred (e.g., malware, ransomware, denial of service)?
- Was any sensitive data or PII compromised? If not, repeat this message consistently in communications.
- Was a ransom request made?
- What services are affected, and what are the alternative processes?

When describing the situation, be transparent but cautious. The following language may be helpful in doing so:

- "We have disconnected from the internet."
- "Law enforcement is investigating."
- "We are working with cybersecurity professionals."
- "Staff have recently completed or are undergoing cybersecurity training."
- "We are working around the clock to resolve the issue."

Avoid disclosing specific restoration timelines. Instead, communicate recovery is ongoing and complex and that updates will be provided as new information becomes available.

Close initial statements with:

- "This is all we are able to share at this time as the matter is under active investigation."

COMMUNICATE WINS AND UPDATES

As systems are restored communicate these milestones internally and externally. Transparency builds confidence.

CONTEXT FOR MANAGING EXPECTATIONS

it is not reasonable to expect the court to know details during the first week, let alone in a month. Be prepared to explain typical incident timelines:

- **Average Time to Detect:**
  181 days
- **Average Time to Contain:**
  60 days,

This helps set realistic expectations and underscores why early responses may lack detail.

DISCUSSING IMPACT AND COSTS

Funding bodies and the media may ask about the financial impact of the breach. In the early stages:

- Avoid disclosing exact cost figures which may signal the court's willingness to pay or the perceived value of systems.
- Point to the ongoing investigation, law enforcement involvement, and lack of full information as reasons for withholding details.

Later, once the situation stabilizes, be transparent as appropriate.

Also, prepare to explain the broader impact on operations and the community, including:

- Potential delays in issuing protective orders.
- Real estate transactions or title searches.
- Disruption in sharing dispositions with law enforcement.

UPDATE FREQUENCY AND TRANSPARENCY

Set a clear cadence for updates, ideally daily or as new facts emerge. Each update should explain:

- What is known
- What actions have been taken
- Next steps
- When the next update will be

Avoid overpromising. The goal is to be honest, consistent, and credible in the early stages of an incident, not necessarily definitive.

Test and Update the Plan Regularly

Once the cybersecurity incident response plan is in place, courts should test it at least annually to ensure it remains current, effective, and actionable.

Regular testing verifies:

- All systems across the enterprise are included.
- Personnel roles and contact information are accurate.
- Response procedures can be executed efficiently under pressure.

*See **NCSC Workbook**.*
To guide this prioritization, courts are encouraged to use the Essential Functions Table within the NCSC Workbook. This tool helps identify services, such as arraignments, protective orders, and emergency warrants, and align them with appropriate RTOs, ensuring operationa continuity even under duress.

Practicing these procedures helps courts respond with confidence and agility, minimizing the impact of a real cyberattack. Ongoing updates to the plan should include:

- Verification of internal and external contact information.
- Review and testing of monitoring and alert systems.
- Adjustments based on legislative or regulatory changes.
- Updated prioritization of mission-critical systems and data assets.[28]

Key areas to revisit during plan testing include:

- **Monitoring and Logging:**
  Confirm all monitoring systems and logging mechanisms are working as intended.
- **Data Asset Prioritization:**
  Reevaluate and, if needed, reprioritize essential data assets.
- **Legal Compliance:**
  Periodically review applicable federal and state laws related to data collection, privacy, and breach notification.

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

The United States currently operates under a patchwork of federal and state privacy and security laws, many of which overlap, diverge, or even contradict one another. As states continue enacting new privacy legislation, often without preemption from federal law, the legal landscape becomes increasingly complex, especially regarding data breach notification, consumer rights, and confidentiality obligations.[29] Because this landscape evolves rapidly, courts should incorporate annual legal compliance assessments into their cybersecurity response planning to ensure alignment with current regulations.

Exercises and Training

Conduct different types of exercises to build readiness across your team:

- **Walkthroughs and Tabletop Exercises:**
  Help team members understand their roles and allow for discussion of how the plan would play out during an actual incident.
- **Functional and Full-Scale Exercises:**
  Simulate real-world scenarios to test the plan in action.
- **Phishing Simulations and Security Drills:**
  Educate and assess court personnel on identifying threats and following proper procedures.
- **Cybersecurity Training:**
  Keep staff updated on protocols and hardening efforts.

[29] Klaber, A. B., & Attig, C. J. (2025, July 10). *As data centers grow, so do their legal challenges* [Blog post]. Morgan Lewis. https://www.morganlewis.com/blogs/sourcingatmorganlewis/2025/07/as-data-centers-grow-so-do-their-legal-challenges

Conduct Cybersecurity Tabletop Exercises in Courts

Tabletop exercises are a vital tool in court cybersecurity preparedness. These facilitated, discussion-based simulations allow judicial leadership, IT professionals, and operational staff to walk through potential cyber incidents in a controlled environment. The goal is not only to evaluate current plans but also to improve organizational readiness, communication, and resilience. See Appendix B for Court-Focused Tabletop Exercises and Checklists.

Why Tabletop Exercises Matter for Courts

- **Enhance Preparedness and Response Capabilities**

  By simulating real-world threats, such as ransomware attacks, phishing campaigns, or data exfiltration, courts can test their incident response protocols and coordination among internal stakeholders. These exercises reveal practical gaps in decision-making, communication, and technical response that may not be obvious in written plans. As highlighted by the Joint Technology Committee (JTC), regular testing is essential to validate court-specific cybersecurity plans and build institutional muscle memory.

- **Protect Access to Justice**

  Cyberattacks can disrupt critical court services, including hearings, e-filing systems, and case access. Exercises help ensure courts are ready to maintain core functions and due process protections, even when systems are impaired. Protecting these services reinforces both operational integrity and public confidence in the judicial system.

- **Improve Communication and Decision-Making**

  Exercises clarify roles and responsibilities, such as who declares an emergency, who engages law enforcement, and who serves as the public spokesperson. Courts must coordinate across judicial leadership, administrative staff, and IT, as well as with external partners. These scenarios help reduce uncertainty and improve the speed and effectiveness of real-time decision-making.

- **Build Confidence in Cyber Resilience**

  Engaging in cybersecurity preparedness demonstrates to internal and external stakeholders, including judges, staff, policymakers, and the public, that courts take these threats seriously. This cultivates a culture of accountability, vigilance, and strategic investment in risk mitigation.

- **Meet Compliance and Funding Requirements**

  Many federal and state grants, such as Byrne Justice Assistance Grant (JAG), currently encourage or mandate cybersecurity exercises as part of program compliance. Exercises also support alignment with best practices from National Institute of Standards and Technology (NIST), CISA, and JTC guidance, contributing to overall cybersecurity maturity and risk posture.

- **Foster Collaboration with External Stakeholders**

  Courts rarely act alone in a cyber crisis. Tabletop exercises provide opportunities to strengthen relationships and protocols with external entities such as local or state cybersecurity teams, law enforcement, emergency management, and third-party vendors. These collaborations support more coherent response strategies and effective coordination during real-world events.

  > *See **NCSC Workbook**. Courts should pre-identify vendors and service providers using the Critical IT Vendors Table within the NCSC Workbook. This proactive step enables rapid engagement during an incident, clarifies points of contact, and supports courts that rely on third-party providers for hosting, cloud services, or managed infrastructure.*

- **Identify and Prioritize Cybersecurity Investments**

  Tabletop exercises help justify budget allocations by revealing unmet needs such as gaps in secure backups, inadequate MFA, or training deficits. The insights gained can inform strategic investment and risk prioritization, offering evidence-based support for technology and training requests.

Conclusion

Cybersecurity readiness is no longer optional. It is fundamental to ensuring uninterrupted court operations and safeguarding the integrity of judicial systems. As threats evolve courts must plan proactively, prepare thoroughly, and respond decisively.

An effective incident response strategy begins with governance and planning, but must be sustained through regular testing, collaboration with key stakeholders, and continuous improvement. Clear communication, strong leadership, and well-rehearsed procedures are essential to limiting the impact of a cyber incident.

Courts must foster a culture of cybersecurity awareness at every level, from IT teams and administrators to judges and frontline staff. Everyone plays a role in defending against digital threats.

By embracing the principles and practices outlined in this bulletin courts will be better positioned to navigate a cybersecurity crisis, protect critical systems and data, and uphold public trust in the justice system, even in the face of adversity.

Appendix A: About Cyberattacks

To create an effective plan for responding to a cyberattack, a court must first understand the types of threats it may face. These threats vary in sophistication, motivation, and potential impact.

Targeted and Opportunistic Attacks

Cyberattacks generally fall into two categories: targeted and opportunistic.

- **Targeted attacks** are focused on a specific individual, organization, or industry. These attacks are more deliberate and often more dangerous than others, as they are tailored to exploit specific systems or personnel.
- **Opportunistic attacks** occur when a hacker broadly probes systems for any vulnerability, often using automated tools. These are the most common types of attacks and may affect any organization that happens to be vulnerable.

Targeted Attacks

In a targeted cyberattack, the adversary has a specific objective and spends considerable time and resources to compromise the intended victim. For courts, such attacks can be especially damaging, with attackers possibly seeking to:

- Gather or alter information about witnesses or jurors
- Access or manipulate case data, documents, or digital evidence
- Modify sentencing details or judicial rulings

These targeted intrusions pose significant public safety and legal risks—particularly when sensitive information is altered, suppressed, or publicly leaked. Both nation-state groups and organized cybercriminal networks now operate with tools and capabilities that enable highly stealthy and sophisticated attacks against judicial institutions.[30]

Threat actors targeting courts may be driven by a range of motives, including:

- Financial gain through identity theft, extortion, or sale of compromised data.
- Revenge, such as from disgruntled former employees seeking retaliation.
- Espionage, whether corporate or state sponsored, aimed at gathering sensitive or strategically valuable information.
- Sabotage, intended to disrupt judicial processes or erode public trust in court institutions.

[30] U.S. Department of Homeland Security. (2024). *Homeland threat assessment 2025*. https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf

These motivations illustrate why targeted attacks against courts can pose serious public safety and institutional integrity risks.

> *In 2013 at the Turner Guilford Knight Correctional Center in Miami, all cell doors in a maximum-security wing opened simultaneously amid what was reported as a system "glitch." Though initially attributed to technical malfunction, surveillance footage and investigation raised serious concerns the event may have involved human intervention or sabotage, potentially exposing the facility to violent inmate attacks.*[31]

More recent analyses confirm motivations such as financial gain, ideological objectives, espionage, and revenge, remain central drivers of targeted cyberattacks. According to industry experts, while financial profit remains the predominant motive—often representing over 60 percent of cases—many incidents also arise from political, ideological, or revenge-based motivations, particularly in insider threat scenarios.

SPEAR-PHISHING

Spear phishing is a highly targeted form of phishing where attackers craft deceptive emails with malicious links or attachments tailored to a specific person or organization, often using personal information for legitimacy. The primary goal is to gain access to internal systems or sensitive information.

In 2024, CISA warned of large-scale spear phishing campaigns targeting government and IT organizations where attackers impersonated trusted entities and delivered malware via remote desktop protocol files.[32]

Every organization is at risk of being the target of a spear phishing attack. In courts likely targets may include:

- Judges and justices
- Court administrators
- Elected officials
- Personnel with access to sensitive systems or case data

[31] Kim Zetter, *Prison computer 'glitch' blamed for opening cell doors in maximum-security wing*, *Wired*, August 16, 2013, https://www.wired.com/2013/08/computer-prison-door-mishap/

[32] CISA. (2024, October 31). *Foreign threat actor conducting large-scale spear-phishing campaign with RDP attachments*. https://www.cisa.gov/news-events/alerts/2024/10/31/foreign-threat-actor-conducting-large-scale-spearphishing-campaign-rdp-attachments

Opportunistic Attacks

Modern attackers increasingly rely on automated tools and compromised networks, often referred to as "zombie networks," which scan the internet en masse to identify vulnerabilities in unpatched systems, exposed backdoors, or misconfigured software. Attackers even embed vulnerabilities intentionally in software, enabling future exploitation. These opportunistic intrusions typically do not target a specific court or institution but exploit widespread systemic weaknesses.

Email-based malware threats, such as Trojans, worms, and malicious attachments, continue to be distributed broadly, relying on user errors rather than precision targeting. Courts remain vulnerable because they store or transmit PII such as social security numbers, driver's license information, or payment data for fines and fees. This exposure creates risk profiles similar to those of private-sector businesses making courts attractive targets.

A prominent case occurred in 2013, when the Washington State Court system suffered a breach that exposed up to 160,000 social security numbers and one million driver's license numbers. Initially attributed to a software vulnerability, the incident underscored the vulnerability of legacy systems and delayed patching practices.[33]

Cyberattack Tactics

Whether an attack is targeted or opportunistic, cybercriminals tend to use a common set of tactics. These tactics can include:

- Gaining unauthorized access to systems or data
- Deploying malware or viruses to compromise or steal information
- Disrupting service through denial-of-service
- Demanding payment through ransomware attacks

Unauthorized Access

Any access to a system, network, or data without proper authorization compromises its integrity. Unauthorized access can originate from:

- Internal actors, such as current and former employees.
- External actors, including cybercriminals or nation-state actors, sometimes operating halfway around the world.

[33] Reuters. (2013, May 10). *Washington State courts hacked; data of thousands at risk*. https://www.reuters.com/article/world/us/washington-state-system-hacked-data-of-thousands-at-risk-idUSBRE9480YZ

- Automated systems, such as infected devices or bots acting on behalf of hackers.

Access may be obtained manually or via compromised systems. Regardless of the method, unauthorized access poses serious risks to data confidentiality, system availability, and operational trust.

Malware and Viruses

Malware, short for malicious software, is designed to disrupt computer operations, gather sensitive data, or gain unauthorized access to systems. Malware comes in many forms, including:

- **Viruses:**
  Attach to legitimate files or software and spread when those files are opened
- **Worms:**
  Self-replicate and spread across networks without user interaction
- **Trojan Horses:**
  Disguise themselves as legitimate software but contain harmful code
- **Spyware:**
  Secretly collects user data and monitors activity
- **Adware:**
  Bombards users with unwanted advertisements
- **Scareware:**
  Mimics security alerts to trick users into downloading fake (and often harmful) software
- **Keyloggers:**
  Record users' keystrokes to capture passwords and sensitive data

Malware can be delivered through:

- USB drives
- Email or text message attachments
- Embedded links in websites or social media
- Software downloads from untrusted sources

Some malware is designed to capture PII, such as Social Security numbers, birthdates, or credit card data, especially from point-of-sale systems. Others may covertly monitor web activity, track physical location, or degrade system performance. One of the most common forms of malware today is the document-based virus, which is embedded in files such as PDFs or Word documents.

In some jurisdictions, "computer contaminant" is the legal term used in state statutes to describe malware and related threats.

Attacks That Disrupt Service

Denial of Service (DoS) attacks aim to render system resources unavailable to legitimate users, either by crashing a service or overwhelming it with irrelevant or malicious requests. When launched from multiple sources using compromised devices (often a botnet), these become Distributed Denial of Service (DDoS) attacks.

In early 2025, Cloudflare reported stopping more than 20 million DDoS attacks which was a 358% increase compared to the same time in 2024. During that quarter alone, there were 700 extremely large-scale attacks, each blasting over one terabit of data per second, with about eight such massive attacks occurring every day.[34]

Today's DDoS attacks are not only more frequent but also more powerful and harder to detect. In one recent case attackers sent 7.3 terabits of data per second, totaling more than 37 terabytes, in just 45 seconds to a single system. The sheer speed and volume made it nearly impossible to stop the attack before it disrupted essential services.[35]

Some of the largest DoS attacks have temporarily crippled:

- Online payment providers
- Banks and financial institutions
- Social media platforms
- Even segments of the U.S. stock market

In some cases individuals or groups who carry out DDoS attacks view them as a form of digital protest, akin to picketing a business. These actors, often referred to as "hacktivists" use DoS attacks to disrupt day-to-day operations and draw attention to political or ideological causes.

Ransomware

Ransomware is a form of malicious software that functions as a cyber hostage-taker blocking access to data or disabling computer systems until a ransom is paid. Once activated, ransomware can encrypt files, lock users out of systems, or display threatening messages.

In some cases, ransomware may display explicit or disturbing content, such as pornographic images, in an attempt to embarrass or intimidate the user into paying

[34] Cloudflare. (2025, April 1). *DDoS threat report for 2025 Q1: 20.5 million attacks blocked* [Blog post]. https://blog.cloudflare.com/ddos-threat-report-for-2025-q1/

[35] Tom's Hardware. (2025, June 15). *Massive DDoS attack delivered 37.4 TB in 45 seconds—Cloudflare blocks record assault*. https://www.tomshardware.com/tech-industry/cyber-security/massive-ddos-attack-delivered-37-4tb-in-45-seconds-equivalent-to-10-000-hd-movies-to-one-victim-ip-address-cloudflare-blocks-largest-cyber-assault-ever-recorded

the ransom. These tactics may be used to exploit fear and pressure individuals into quick action, particularly in professional environments like courts.

Court personnel should be trained to recognize the signs of a ransomware attack. If ransomware is suspected:

- Immediately disconnect the affected computer to prevent external data transmission.
- Disconnect from the internal network to contain the spread of the ransomware across systems.

Early recognition and rapid isolation are key to limiting damage and preserving critical court operations and data integrity.

Zero-Day Exploits

Zero-day exploits occur when attackers take advantage of an unintentional flaw or vulnerability in a vendor's hardware or software before the vendor becomes aware of and corrects the issue. Because the vendor has had "zero days" to respond, there is no immediate patch or fix available at the time of the attack. These types of vulnerabilities may go undetected for months or even years. In some cases the public may be the first to notice the effects, especially if the flaw is used to steal personal information and commit identity theft. Even when the vendor discovers the vulnerability the term "zero-day" remains highlighting the urgency with which they must act to develop a patch or provide users with a workaround.

Appendix B: Cybersecurity Tabletop Exercises

Cybersecurity Tabletop Exercise Scenario for Courts

Objective

To evaluate the court's ability to respond to a ransomware attack affecting the case management system (CMS), e-filing, and email platforms, while maintaining access to justice, internal communication, and public trust.

Exercise Participants

- Chief Judge or Presiding Justice
- Court Administrator/CEO
- CIO and/or Chief Information Security Officer
- Court IT Staff
- Public Information Officer
- HR Representative
- Legal Counsel
- Court Clerks
- Local/State IT Agency Representative
- Law Enforcement Liaison
- Key Vendors (if applicable)

Exercise Notes

- The exercise should take between one and three hours depending on the size and complexity of your court and network.
- Existing incident response plans should be used and referenced during the exercise. (If you do not have an existing response plan, see the **NCSC Workbook**.
- A parking lot or list should be kept of any gaps, updates or issues identified during the exercise and they should be assigned to individuals for follow-up.

Exercise

Scenario Summary

On a Monday morning, court staff arrive to find they cannot log into the CMS. A pop-up message on multiple systems indicates files are encrypted and a ransom is demanded in cryptocurrency. Simultaneously, the court's website redirects to a malicious domain, and social media reports suggest widespread confusion among the public. Email servers are down.

Activation

- Who detects the incident?
- Who is notified first?
- How is the response team activated?
- Where/how does the response team meet?
- What systems are impacted?
- Is this an IT issue or a cybersecurity incident (what do the logs say)?

Assessment

- What data is affected (e.g., CMS, filings, partner integrations, personal information)?
- Are backups available and accessible?
- What legal or ethical duties are triggered?
- Does an insurance policy need to be activated?
- Is there a cybersecurity firm on retainer to be contacted?

Containment

- What systems should be isolated?
- How is external access restricted?
- How are judges and staff informed of the issue?

Communication

- Who is the spokesperson?
- What internal messaging is sent to staff and judges?
- How do you communicate with attorneys, litigants, justice partners and the public?
- How is the media handled?

Continuity of Operations

- Can essential court functions continue?
- Are alternate filing or docketing procedures available?
- Is a judicial or administrative order necessary to do business in a different way?
- What backup documentation/manual processes are in place?

Recovery and Lessons Learned

- How will you coordinate restoration of data and systems?
- How do you verify data integrity?
- What post-incident review and policy revisions are necessary?

NCSC

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