JTC Resource Bulletin

Cybersecurity Basics for Courts

Version 3.0
Adopted September 15, 2021

Abstract

Cybersecurity threats are a reality for all organizations, public and private. In spite of good prevention efforts, every court will almost certainly face a cybersecurity incident including data breach or cyberattack. This paper provides a basic explanation of prevention techniques and the preparations necessary for court managers to respond quickly and effectively in the event of a cybersecurity incident.

Document History and Version Control

Version	Date Approved	Approved by	Brief Description
1.0	2/17/2016	JTC	Release document
2.0	12/4/2019	JTC	Release updated document
3.0	9/15/2021	JTC	Release updated document

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:
To improve the administration of justice through technology

Joint Technology Committee:

COSCA Appointments

Stacey Marz (Co-Chair), Administrative Office of the Courts, Alaska

David K. Byers, Arizona Supreme Court

Laurie Dudgeon, Administrative Office of the Courts, Kentucky

Jeff Shorba, State Court Administrator's Office, Minnesota

Rodney Maile, Administrative Office of the Courts, Hawaii

NACM Appointments

Kevin Bowling (Co-Chair), Michigan 20th Judicial Circuit Court

Paul DeLosh, Supreme Court of Virginia

Roger Rand, Multnomah Circuit Court, Oregon

Kelly C. Steele, Florida Ninth Judicial Circuit Court

Jeffrey Tsunekawa, Texas Office of Court Administration

NCSC Appointments

Judge Jennifer Bailey,

11th Judicial Circuit, Miami, FL

The Honorable Samuel A. Thumma, Arizona Court of Appeals

CITOC Appointments

Winnie Webber, 19th Judicial Circuit, Lake County, IL

Casey Kennedy, Texas Office of Court Administration

Ex-officio Appointments

Joseph D.K. Wheeler, IJIS Courts Advisory Committee

NCSC Staff

Jim Harris

Table of Contents

Executive Summary

Accepting that courts *will* face cybersecurity incidents is essential. In 2020, more than 2,400 American hospitals, schools, and government agencies – including courts – were the victims of ransomware. Court leaders must shift their thinking from "If?" to "When?", and the purpose of this Resource Bulletin is to guide their prevention, preparation, response, and recovery actions.

Section 1 presents cybersecurity Essential Terminology in plain English, and Appendix A contains more detail about a variety of cyberattacks. **Section 2** provides a thumbnail sketch of the State of Cybersecurity in Courts, which might be useful in persuading court leaders, policy makers, and funders to invest time and money in prevention and preparation.

Section 3 offers specific, achievable prevention steps, as well as cost-free resources available to your court. Its companion, **Appendix B**, is a checklist of preventative-maintenance actions, ranked in order of cost and difficulty.

The balance of the Resource Bulletin is dedicated to preparation for planning and responding to a cybersecurity incident: from the creation of a **cybersecurity response team** to **periodic testing of a court's cybersecurity response plan**, the goal is to earn the public's trust and confidence that your court is ready to respond to a cyberattack when it occurs. Mitigating the harm of data loss, continuing essential court operations, complying with notice requirements, and assisting the investigation and prosecution of cybercriminals cannot be achieved amid the chaos of a cyberattack without advance planning. **Appendix C** suggests key questions court leaders should ask their technologists and technology vendors to start the discussion.

Some court leaders might say, "My court is too small to attract the attention of a cybercriminal." Other court leaders might say, "Cybersecurity is evolving too rapidly for us to take meaningful action." Still others might think, "I don't have to worry about cybersecurity because that's my vendor's job." These perspectives are simply excuses that attempt to justify a passive approach that provides a false sense of security. This Resource Bulletin is purposefully designed to be useful to every court, big or small, in-house or out-sourced, with or without a Chief Information Security Officer. Because cybersecurity is everyone's job.

State of Cybersecurity in Courts

The number, scope, and breadth of organizations experiencing cybersecurity incidents in the past few years is vast and unsettling. Attacks against courts are on the rise, and the methods of attack continue to become more sophisticated. The reality is that regardless of preventive measures, most organizations will deal with some form of cybersecurity incident. Accepting that courts *will* face cybersecurity incidents is essential.

Cybersecurity often comes at a cost, not only in terms of dollars, but also convenience and performance. Properly balancing cybersecurity and convenience can be a challenge for management when looking at what security measure to invest and implement. As recent cyber-attacks demonstrate, convenience should not be a reason to circumvent sound security practices and policies.

2020 Data Breach Statistics[1]
Average time to detect a breach: 228 days
Average time for containment: 80 days
Average data breach lifecycle: 315 days
Global average cost of a data breach: $3.86 million
Average cost per lost or stolen record in a data breach: $150

This figure highlights the steps related to a cybersecurity breach after an attack has been confirmed.

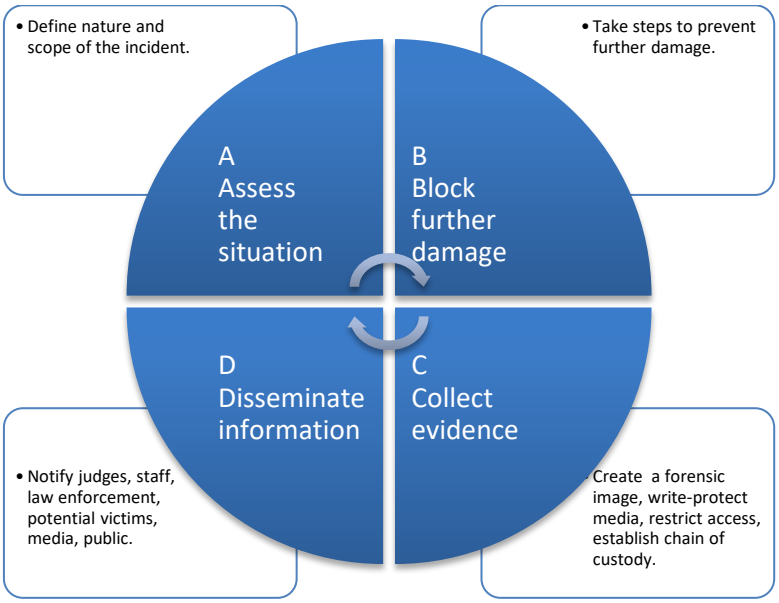

Figure 1 - ABCs of Cyber Incident Response

Cybersecurity is a team effort that requires the diligence of every user of technology resources and the commitment of the court executive team to appropriately plan, prevent and respond properly to incidents. It starts by having good prevention practices and methods in place such as regular training, testing, monitoring, and best practices for the protection and the recovery of data. Cybersecurity planning allows the court to identify, categorize and prioritize the recovery of its mission essential functions and the data systems and services that support those functions. It is important for courts to include cooperation and coordination with other entities when in a shared IT services environment.

[1] Sobers, Rob. "98 Must-Know Data Breach Statistics for 2021.",Varonis, 6 Apr. 2021

Introduction

Cybersecurity is a topic of broad interest and one in which courts should actively engage as the consequences of not doing so can be disruptive and costly. In most respects, courts do not have distinctly different cybersecurity risks and challenges than other public and private entities. While there are many reputable organizations that specialize in cybersecurity, courts should first consider resources provided by two US-agency sponsored organizations:

> **CISA.** The Cybersecurity and Infrastructure Security Agency is a part of the US Department of Homeland Security. Their charter includes incident response services, assessment capabilities, and cybersecurity tools.[2]
> **NIST.** The National Institute of Standards and Technology is a science lab devoted to standards of measurement for industry and science. NIST's Cybersecurity Framework[3] of standards, guidelines, and best practices can be applied to court organizations of any size or sophistication.

This paper explains the basics of cybersecurity in language designed to assist non-technical court personnel in collaborating with the people and organizations that oversee cybersecurity for their court. It is meant to be a conversation starter as well as a forceful nudge toward action.

Essential Terminology

A **cybersecurity incident** is 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."[4] Cybersecurity incidents come in several forms. A **cyberattack** is an attempt by hackers to damage or destroy a computer network or system. A **cyberbreach** is an incident of unauthorized access, viewing, use, or retrieval of sensitive, protected, or confidential data. **Exfiltration** is when data has been successfully transferred and stolen.

Cyberattacks include malware, viruses, denial of service (DOS) attacks, ransomware, zero-day exploits, and unauthorized access from within the organization (current and former personnel) or by hostile individuals and organizations halfway around the world.[5] Attacks may be targeted at the court specifically or may simply be opportunistic.

A cyberattack may be used to gain access on an ongoing basis to networks or databases, resulting in a data breach (or cyberbreach). Though no known incidents of cyberattack have resulted in altered court records, it is conceivable that a cyberattack could be used to reverse decisions, fabricate felony convictions to impact voting rolls, reduce sentences to release gang members, etc.

---

[2] See https://www.cisa.gov.

[3] See https://www.nist.gov/cyberframework.

[4] "Law Enforcement Cyber Incident Reporting." *FBI.gov*. Federal Bureau of Investigation, n.d. Web.

[5] For more information about malware, viruses, and other mechanisms of cyberattack, see Appendix A: About Cyberattacks.

State of Cybersecurity in Courts

Taking steps to prevent a cyberattack is clearly worth focused attention. Regardless of preventive measures, most organizations will deal with some form of cybersecurity incident at some point, necessitating a response. Courts are not immune and attacks against courts are on the rise. This paper will incorporate some of the hindsight knowledge gleaned by court managers who have attempted preparation and prevention, experienced an incident, and dealt with the aftermath.

Cybersecurity is an issue no matter the industry, geography, or jurisdiction. The number, scope, and breadth of organizations experiencing cybersecurity incidents in the past few years is vast and unsettling. Courts may believe they are unlikely to be victims of cybersecurity incidents because they don't manage large databases of credit card information. However, threats are real and increasing. From courts and corporations to utilities to universities, public and private entities are finding themselves under attack by individual profiteers, criminal groups, and state-sponsored hackers who are gathering data as well as spreading propaganda, viruses, malware, ransomware, and more. The confluence of complex interrelated systems and the Internet has given criminals entirely new ways of doing harmful things digitally. Cyberspace is borderless, so attacks can come from anywhere at any time. There are new trends such as "hacker for hire" where bad actors can be hired to do harm to an organization creating increased risks for disruption to organizations from disgruntled individuals.

Accepting that courts *will* face cybersecurity incidents is essential. In fact, a cybersecurity incident may already be ongoing within your organization, undetected. Court managers must have an established plan for responding when the inevitable occurs because any organization with data or a public-facing role can be targeted. The time to prepare to deal with an incident is before one occurs. Having a tested recovery plan in place can help courts respond more effectively, mitigating some effects of an attack and/or breach.

Preventing Incidents

Avoiding a cybersecurity incident through intentional prevention efforts will always be more desirable than a well-executed recovery. While careful prevention cannot ensure immunity from incident, it can reduce risks dramatically, limit the impact of an attack, and lay the groundwork for smooth recovery.

Map Out the Threat Surface

The threat (or attack) surface includes all the points where an attacker could gain virtual or physical access to systems and data.[6] The threat surface is continuously expanding from what is inside the firewall, all the way down to the homes of individual personnel.

[6] For more information, see "Attack Surface Analysis Cheat Sheet." *The Free and Open Software Security Community*. The Open Web Application Security Project (OWASP), 2021. Web.

The threat surface includes network and software vulnerabilities, as well as humans and facilities. Identify potential points of entry, open ports, and external Internet connections, as well as connections to other organizations and governmental agencies. Be sure to include third-party connections to non-data systems, such as HVAC, alarm systems, copiers, door access systems, and any other Internet-connected devices.

Because systems and technologies change rapidly, new vulnerabilities may be introduced at any time. Review the threat surface regularly, or at a minimum, each time a system is implemented or upgraded.

There are resources, services and training opportunities at CISA[7] and the Multi-State Information Sharing & Analysis Center (MS-ISAC)[8] for free to state and local governments including the judicial branch. CISA may provide assistance for incidence response, cybersecurity training and exercises, risk assessments including pen (penetration) testing, governance, detection and prevention, and information sharing/alerts. MS-ISAC members (free to government) include access to the security operations center, incident response services, advisories and notifications, malicious code analysis, tabletop exercise template, and vulnerability management. These organizations include some specific focus on threats to government agencies and offer valuable resources every court should be utilizing.

Reduce the Threat Vector

Most IT organizations are already taking steps to block website traffic from known malicious IP addresses. Reducing geographic access to applications (despite credentials) can help to further narrow the threat vector. For example, lawyers filing into state's child support application need to be in the continental US.

Secure Facilities and Digital Devices

Physical security is a key component of cybersecurity. Keep server rooms locked and devices secured. A stolen laptop is an avenue for data exposure and cyberattack. Have policies and procedures for dealing with lost equipment and the ability to quickly disable lost devices. Ensure file encryption utilities are installed and enabled (e.g., BitLocker for Windows devices and FileVault for iOS) on portable user devices. Non-technical organizations, including courts, are notoriously lax in protecting IT assets. The most common security failures are human: ensure personnel (judges, internal/external staff, volunteer, contractors) do not give individuals without proper credentials access to equipment or secured spaces.

[7] For more information about free resources and alerts, see https://www.cisa.gov/cyber-hygiene-services

[8] For more information about MS-ISAC resources and alerts, see https://www.cisecurity.org/ms-isac/

Limit Access to Systems, Processes, and Data

Ensure the keys to the cyber-kingdom have limited access. Courts should implement the Principle of Least Privilege, an IT best practice that reduces risks by giving people and systems only the specific access they need to perform their role.[9]

It is also important to secure and monitor physical access to critical on-premises systems and infrastructure. Often, there are door access logs that are tracked for access to secure areas, along with video monitoring.

Segment the Network

Closely related to the concept of Principle of Least Privilege is the practice of segmenting networks so that data and applications are grouped in some way that separates unrelated data and applications. For example, financial applications should be housed in a different part of the network than the case management system. The firewalls and communications equipment that separate various network segments add a layer of complexity that makes it more difficult for malware to access data. If one part of the network is breached, data in another segment may not be impacted.

Authorized Software and Patch Management

User-installed software is a common and preventable source of cyberattack. Software installed in the enterprise network environment should be licensed, current, and installed and configured by tech staff. Have policies and processes in place to remove unauthorized software.

Ensure software patches, modifications made between release cycles are applied as they become available. Patches are often created specifically to address security vulnerabilities discovered after software is released, as well as to correct other bugs/defects. However, patches that fix one issue may also "break" other features/connections. Test patches first to ensure they won't introduce other issues. Have systems within your organization configured to update software on a regularly scheduled basis. As a general rule, efforts are made to apply updates during non-working hours, but some patches must be pushed out during working hours if they are critical. Educating and reinforcing the need to have computers and devices in a state that can accept the patches, such as ensuring they are powered on with an internet connection every evening should be done regularly. Usually, scheduled updates that are missed due to some technical reason will load at the next available opportunity, which may conflict with other operations. This highlights the importance for end users to maintain the proper equipment status to receive updates and to accept possible delays if updates are installed outside of normal schedules.

[9] For more information, see https://csrc.nist.gov/projects/role-based-access-control/faqs

Ensure vendor contracts have a clause to specify timely updates to third party components and libraries (such as integrated web browsers or database software) when vulnerabilities are published, or the security components of such software becomes obsolete. Software is often composed of multiple third-party systems that may discover a vulnerability that can be exploited after the vendor's software is installed.

Now that more systems are available 24/7/365, it is important to have a process to plan scheduled maintenance and software updates. Some systems have standing maintenance schedules in place. It is recommended to have notification alert method(s) of planned outages.

Manage Accounts and Passwords

To ensure user activities can be attributed as well as audited, establish a unique account for each user. Configure systems to automatically lock the user workstations or log them off after a certain period of inactivity to prevent unauthorized access through an unattended device. Implement monitoring software to scan the network, inventory connected devices, audit user activities, and automatically trigger notifications if activity is unusual. Disable or remove accounts immediately when someone is terminated, whether the termination is routine or for cause. Inventory which systems, internal and external, that each user has access to so all related accounts can be deactivated or removed.

Require complex, unique passwords. Automate periodic user password reset requirements. Use phrases that are longer and therefore harder to guess, but can be easier to remember, e.g., 1twillb3Fr!day$00n.

Authentication

Utilize multi-factor authentication, which requires two or more categories of credentials, e.g., password or pin plus a smart card, authentication mobile app, or biometric identifier (fingerprint, iris scan, facial recognition, etc.). One form of multi-factor authentication is "two-factor authentication". The first factor is a password, and the second could include a text with a code sent to your smartphone an authenticator mobile app or biometrics. Biometrics are unique physical characteristics, such as fingerprints, that can be used for automated recognition. While readily available, usage of biometrics requires storing personal data, and privacy concerns should be considered before implementing this type of method. Basic authentication using account and password as security is now too easily compromised.

Invest in Cybersecurity

Organizations must budget for cybersecurity – software, services, and staff time to include the cost of training all personnel. According to the Accenture 2020 report on the State of Cyber Resilience, "…most organizations are getting better at preventing direct cyberattacks. But in the shape-shifting world of cybersecurity, attackers have already moved on to indirect targets, such as vendors and other third parties in the supply chain".[10] This report also highlights the fact that there have been significant innovations in cybersecurity. These innovations are better at stopping attacks, finding breaches, and fixing breaches faster which reduce impact. Although user behavior is a primary weak link, now we see attacks through the supply chain such a compromised patch update coming from a vendor. The most notable recent attack was through the network monitoring software SolarWinds through a compromised update.[11] Given the increasing ways that a cyber-attack can come in through the front and back door, continuous investment into the basics as well as new innovative technology is something that should be planned for as a regular part of the budget cycle.

Continuous security awareness training for users is of foundational importance because the threat landscape keeps changing. Having the entire organization trained on fundamentals such as 1) good cybersecurity practices, 2) knowing what to look for, as well as 3) the procedures to apply (for common and new threats) are critical factors to improving cyber resilience.

Phishing campaigns are still a major source of intrusion, but are one of the easiest kinds of attacks to prevent. Antivirus software can screen out a large percentage of phishing attempts. Training, frequent reminders, and "phishing tests" can help users recognize and respond appropriately to threats.

Ongoing IT training is another important investment. Ensure staff who will assist in prevention and/or recovery efforts have adequate, current training and certifications. Untrained staff may unintentionally do more harm than good in attempting to re-route a network or stand-up clean workstations.

See Appendix B for actionable cybersecurity guidance.

[10] Bissell, Kelly, Lasalle, Ryan, and Dal Cin, Paolo. "Third Annual State of Cyber Resilience". Accenture, 2020.

[11] "Highly Evasive Attacker Leverages SolarWInds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor". *Fireeye*, 2020.

Segment the Network: Firewalls and network infrastructure devices used to separate various network segments add a layer of complexity that makes it more difficult for malware to access data.

IT Risk Analysis: Organizations should conduct an IT Risk Analysis to identify the risks, and to determine the cost benefit of countermeasure investment, interpret the results, and create a remediation and mitigation plan.

Conduct routine penetration testing: Organizations should invest in a third-party company to exploit weaknesses and vulnerabilities. The resulting report should be used to provide direction and guidance for reducing exposure to risk while also providing actionable steps towards a resolution.

Own It

Cybersecurity must be viewed as the responsibility of every individual in the organization, not just the IT group. Accountability is a difficult yet vital consideration, because anyone can fall victim to a cybersecurity attack. But organizations must find ways to raise awareness and hold individuals accountable for preventable cybersecurity incidents.

Cybersecurity Governance, Policy, and Planning

Cybersecurity often comes at a cost, not only in terms of dollars, but also convenience and performance. Properly balancing cybersecurity and convenience can be a challenge for management. As recent cyberattacks demonstrate, convenience should not be a reason to circumvent sound security practices and policies. The painful and expensive process of recovery from a successful cybersecurity incident is why the minor inconveniences of security processes, policy, and training should be accepted and tolerated by court users and others that utilize court data and systems. Good cybersecurity practices require commitment from the entire enterprise environment.

It is important to establish a governance body that represents a team approach. The work of this governance group is to review and update cybersecurity policy and practices, receive regular communication about threats and attack attempts, and to provide oversight on recommendations about needed cybersecurity protection investments. A governance body can bring several perspectives to the table and provide a method to truly evaluate relevant factors of what constitutes a good cybersecurity posture.

It is important to educate court decision makers about what downtimes to expect when a successful cybersecurity incident had taken place. Cybersecurity incident outages are the most painful inconvenience. Such outages last several months depending on the scope of the attack, depth of the attack, and whether or not data has been exfiltrated. This is not like a normal technology disruption, and this is a primary reason to include cybersecurity incidence response in Continuity of Operations Planning (COOP).

Internally the number one question throughout this process will be "When will operations be restored?", which is difficult to answer because of the complex factors related to assessment and forensics as each type of successful cyber-attack incident can vary widely.

2020 Data Breach Statistics[12]

- **Average time to detect a breach:** 228 days
- **Average time for containment:** 80 days
- **Average data breach lifecycle:** 315 days
- **Global average cost of a data breach:** $3.86 million
- **Average cost per lost or stolen record in a data breach:** $150

Assembling a Cybersecurity Incident Response Team

While IT will clearly lead efforts to address the technology ramifications of a cybersecurity incident, IT cannot be the only department involved in incident prevention and recovery planning. A court's cybersecurity incident response team should include representatives from each department that would be involved in handling an incident or notifying others (either the public or court personnel). Consider carefully how you will "staff the threat." Identify alternates for each role in the event a designated individual is unavailable.

At a minimum, that team should include the following:

- **Chief Judge/Justice**
  As the "face" of the court, the Chief Judge/Justice should likely be the spokesperson.

- **Court Administrator/CEO**
  Musters the resources necessary to carry out the plan while orchestrating ongoing business. If the court does not have a Chief Information Security Officer on staff, the CIO will be responsible for coordinating the responsibilities included below.

- **CIO**
  Takes the lead in the technical portions of the action plan.

- **Chief Information Security Officer**
  Ensures the team's responses meet legal mandates for protecting data and preventing data loss by implementing industry standards and providing focused cybersecurity oversight.

---

[12] Sobers, Rob. "98 Must-Know Data Breach Statistics for 2021.",Varonis, 6 Apr. 2021

The CISO may collect digital forensic evidence and/or act as liaison to law enforcement and other agencies in the event of a breach.

- **Public Information Officer**
  Ensures Chief Judge/Justice has accurate and complete information and assists with communications to press and public.

- **Human Resources**
  If personnel are affected, HR participates in efforts to address the impact.

- **Chief Financial Officer**
  Ensures appropriate funding source is used to respond to the incident, including navigating procurement rules to contract with vendors during the emergency.

- **Legal**
  Works to protect the court from making legal missteps in response efforts.

- **Vendors**
  Fills gaps in staff skillsets and organizational resources to meet immediate, short-term needs. Having agreements in place for recovery services prior to an incident will save critical time locating, negotiating, and contracting those services.

Each team member represents unique organizational perspective that will be important in preparing to address the breadth of implications of a cybersecurity incident. Court managers may need to handle some less technical recovery efforts as IT personnel focus on urgent, technical tasks.

Identify the Spokesperson

Multiple, divergent accounts of the incident going out to the public and the press from more than one "official" source will add confusion and complexity. Determine who will act as spokesperson and ensure the spokesperson is the only one speaking publicly about the incident.

Assign Responsibilities

Identify essential tasks and who is responsible for each. Be specific. Tasks that can be addressed with limited IT involvement can reduce recovery bottlenecks. Ensure court managers have the flexibility to address situations within their skillset and authority.

Meet Regularly

The incident response team should meet on a regular basis, ideally at least quarterly. In the event of an incident, the team should meet frequently to share information, monitor recovery efforts, and adjust to new information as it becomes available. Meeting regularly throughout the incident is critical to ensuring the team is unified in their

response efforts and that information is being communicated accurately, effectively, and in a timely way.

Establish Channels of Communication

Collect and protect contact information for individuals and organizations (personnel, IT vendors, security, police, etc.), both daytime and after hours/weekends. Anticipate that organizational contact mechanisms like email and phone systems may not be functioning. Use emergency notification systems (e.g., Everbridge) as part of the business continuity plan. Time is of the essence; it is important to communicate quickly especially if there is an ongoing threat.

To ensure the information is immediately available in the event of an incident, the response plan and contact information could be made available to team members to retain on their individual smart phones or via an app. A copy should be stored in paper form in a specific place accessible to those who will need it.

For many courts, city or county IT departments manage court networks, so the IT point of contact may not be a direct employee of the court. Ensure your response plan anticipates interdepartmental and cross-functional communications that will be required to work cohesively.

Plan the Message

While it is impossible to plan exactly the content of your internal and external messaging in advance of a cybersecurity incident, it is helpful to have your messaging template set up. This includes formatting the message, drafting language that reassures that the court will continue to operate to the best of its ability and handle at least essential priority proceedings, and that as more information becomes known, the court will continue to provide updates. It is also helpful to have your external plan include all communication channels such as press releases, website updates, and social media posts. For internal communications, assure personnel (judges, internal staff, volunteers, contractors) of the system's capabilities to continue operating in a modified fashion, appreciating their flexibility and efforts as the response occurs.

Laying the Groundwork

An effective post-incident response plan requires that key components be in place before an incident occurs. It is essential that the plan be designed with recognition of the court's data assets and potential vulnerabilities, as well as the applicable laws governing data collection, privacy, and victim notification. Courts also need tools to monitor essential data assets and detect intrusion.

Identify Essential Data Assets

Anticipate the potential impact of the loss of or unauthorized changes to essential data assets including judges' orders, court records, the identity and testimony of witnesses, juror identities, digital court recordings, financial transaction information, digital evidence, and personnel information. This inventory of assets is a critical first step.

Courts must know what data they hold, or that vendors hold on their behalf. What data exists, where is it stored, and what is its value, both to the court and to a potential intruder? Think beyond credit card numbers and personally identifiable information like social security numbers and birth dates. Today, courts hold essential data assets that have nothing to do with financial transactions. A judge's orders, the identity and testimony of witnesses, digital evidence, juror identities, and anything stored digitally are all vulnerable to a cybersecurity incident. An inventory of these assets must be compiled for further planning and determination of the risk profile for each asset.

Risk Assessment and Analysis

Proper planning includes conducting a risk analysis, which is a process to categorize data assets and assigns a value to each data asset or category. This process also assesses exposure risk, and estimate costs associated if the asset(s) were lost or compromised. Further, the risk assessment will assist in identifying potential countermeasures, cost of the countermeasure, and rate their related effectiveness. After this analysis, decision makers then assign tolerance thresholds for downtime and amount of acceptable data loss for each asset. Then a cost benefit analysis of potential countermeasures to safeguard each asset can be conducted once these elements are determined.

Recovery Time Objectives (RTO)

Recovery Time Objectives relates to downtime tolerance thresholds. The RTO is an indication of how long a system may be down before experiencing measurable loss of business operations. Decision makers need to evaluate and assign expected recovery times objectives for systems, which will guide what level of investment in security and recovery countermeasures should be made to maximize successfully meeting the RTO.

Recovery Point Objective (RPO)

Recovery Point Objective indicates the maximum amount of data loss that can be tolerated before it impacts business operations. Some data backups are scheduled processes done after hours, so there may be some amount of data loss between backup operations and the disruptive event. Decision makers need to assign how much data loss may be tolerated for each data asset, so that proper data backup and recovery methods can be put into place to meet the set RPO threshold.

Document Systems

Documentation of system configurations, dependencies, connections, and services are critical resources used in a recovery effort. The maintenance of system documentation especially for the most critical assets should be checked and reviewed on a regular basis. Documentation may also be used to review and address potential security gaps.

- Keep network and application documentation up to date.
- Understand dependencies between systems. If a critical system is dependent on a function of a lower system's function, it might change how recovery is prioritized.
- Fully document backup and recovery processes and locations.

Create Multi-Level Redundancy with Data Backups

Ensure backups are current and network diverse. If the backup is on the same network as primary data, it will likely also be infected. A disconnected/offline "island" of redundant data will make it much easier to recover if an incident occurs.

When creating multi-level redundancy with data backups, be sure to consider the following:

- Regularly test backups by attempting to restore randomly selected files.
- Periodically attempt a full restore.
- At least one complete backup should be stored disconnected/offline and off premise.
- Make sure backup overwrite schedules are long enough to cover potentially several months of a major cyber incident recovery period.
- Audit backups to make sure there that no critical data is being missed or overlooked.
- Configure systems to automatically save to proper backup locations and train users to save critical court files in the proper location if prompted to ensure data is being captured in the backup process.

Enable Logging and Implement Automated Monitoring

In the same way that monitoring the court's entrances via CCTV is not an incident prevention effort, per se, monitoring systems and logging activities are essential security

measures that will dramatically improve the court's ability to detect, investigate, and respond to a cybersecurity incident. On an ongoing basis:

- Capture and store log information from switches, routers, proxy servers, firewalls, etc.
- Store logs and in a manner where they will not be compromised in the event of an attack. Some attacks go after both logs and data backups to impede recovery efforts.
- Implement user consent login banners/warnings to ensure users understand that their activities will be monitored.
- Make full use of monitoring, logging, and diagnostic tools, anticipating that they will, in fact, be called in to use.
- Implement security monitoring and attack detection systems to continuously monitor systems and trigger alarms when patterns of network activity indicate intrusion.

Review Terms and Conditions of Contracts with Vendors

Understand what is contractually required of vendors if they have a cybersecurity incident. Recognize that an incident may not be discovered for months. Even so, vendor agreements should require immediate notification when a breach is discovered, not after the source and extent are investigated. Check vendor contracts to make sure vendor supplied components or software that the vendor maintains require the vendor to provide timely security updates when a vulnerability is disclosed. This should include security updates for third-party components within a vendor solution. Where appropriate, have vendors involved in your COOP and disaster planning efforts especially if the vendor is hosting the data as well as the application.

- Ensure contracts include provisions allowing the court to regularly audit the vendor's security procedures.
- Confirm you are part of your vendor's cybersecurity incident response plan.
- Depending on the level of services the vendor provides, vendor services and platforms should be addressed in the court's COOP/DR plan.

Understand the Implications of Shared Technology Infrastructure

Court IT assets may sit on a network in which the court does not control or have visibility. It can be easy to simply assume the Executive Branch, city or county has

controls in place to guard against intrusion. As these other government agencies providing support may have to deal with a multi-level cybersecurity incident impacting several agencies, the court may find itself entangled in the incident reaction process without a clear understanding of how the court's ongoing operational activities fit into the recovery schedule. The court must work to ensure other entities understand the implications to the courts' data and business operations if there is an incident on "shared technology infrastructure". There are legal requirements and time standards that should be considered in planning and coordinating a response for all entities in the shared environment. Through coordinated planning, the court can work be a good steward and user of shared resources and also have its priorities met in the event of an incident.

The Executive Branch, city and county networks may support municipal government, state infrastructure, law enforcement and other resources such as transportation (airport, bus and train) and emergency health services. Courts that are not involved in active monitoring and response can be taken down by another agency's breach. Conversely, an incident that originates with the court could spread through other agencies dependent on the same network, potentially impacting public health and safety systems. Courts should not assume their partner agencies are secure.

When considering the implications of shared technology infrastructure, be sure to acknowledge the following:

- Understand the court's liability and responsibility in protecting both themselves and other agencies that share the network.
- Have a contingency plan to move to a secondary location with its own external network access or to obtain emergency network services.
- Have proper governance in place between the court and the providing agency that outlines responsibilities, participation in the comprehensive COOP/DR plans that impact court operations, and a clear understanding of the priorities within the court for protection and recovery. This can take the form of a Memorandum of Understanding (MOU) or other agreement.
- Make sure that critical contacts and a proper communication channels are in place to troubleshoot any suspected events and to coordinate efforts to address an active incident.

Be Familiar with the Laws Governing Data Collection and Privacy

Courts must not only protect the personally identifiable information (PII) they collect, but must also obtain consent of system users to monitor communications in order to detect

and respond to an intrusion.[13] User consent can be easily obtained through log-in banners or warnings, but those mechanisms must be in place before an intrusion occurs.

Courts are not immune to the legal implications of a data breach. Many jurisdictions have financial penalties tied to data collection, privacy, and victim notification. It is particularly important for courts to know the applicable laws governing victim notification because there are compounded penalties that could be costly. In addition to federal requirements, make sure to research state breach notification requirements and plan accordingly.[14] Often notification requirements depend on data exfiltration thresholds, which is why having proper monitoring, as well as tools to conduct proper forensics, will be important.

Anticipate Malicious Intent

Those who 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 and backups. A secondary attack may hamper recovery efforts. One court manager noted that he simply had not anticipated the level of evil intent behind cybersecurity incidents. Understanding that would have prompted much greater caution and swifter action.[15] Determine the greatest threat motivators such a financial gain from ransomware, disruption, weaking public trust and confidence. By identifying potential threats and intent, the court can better prioritize their cybersecurity plans, investments, and responses.

Anticipating malicious intent can help prioritize planning and additional cybersecurity investment.

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

Establish and document procedures to follow in the aftermath of a cybersecurity incident. This should be an integral part of broader disaster and continuity of operations planning (COOP) for other potentially disruptive incidents including pandemics, natural disasters, weather emergencies, and terrorist attacks. Make sure judges, supervisors, and management staff are all aware of the plan and the expectations. Be careful not to overcommit managers. Don't assign staff to handle multiple aspects of the plan simultaneously.

Ensure response procedures are logical within the context of your court's organization and processes, and that they align with existing court policies. If necessary, modify policies and

---

[13] See *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, a publication by the Computer Crime and Intellectual Property Section, Criminal Division, Office of Legal Education, Executive Office for United States Attorneys. N.D. Web.

[14] See Security Breach Notification Chart at perkinscoie.com.

[15] Email correspondence between P.L. Embley and unnamed court manager, 27 September 2019.

processes. Consider the logistical implications of having to move to a secondary location during recovery.

> …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.[16]

Make sure procedures are not simply "cut and paste" from a model plan. Such plans are convenient to adopt but may include expectations and commitments that a court cannot meet. Gaps may not be clear until the plan is executed in a real situation. Plans must be tested regularly and rigorously. They should fail periodically in the test situation to expose vulnerabilities. If the plan never fails in testing, that doesn't mean it's a particularly effective recovery plan. It may actually reflect a lack of imagination.

One court manager who spent months recovering from an incident ruefully explained the difference between making theoretical plans for "IF an incident occurs" and making tactical, urgent preparation for "WHEN an incident occurs."

> It's a different urgency, priority and scale when you say, "we are getting hacked this weekend" versus "What if we get hacked?" We … had … plans [to isolate cloud services and create disparate "environments" to mitigate risk and increase the complexity and effort needed to cause damage] for years but they never get done when you plan for "If." Planning for "when" presents a completely different urgency… Set a date. [Get it done.] Like many emergencies, [cybersecurity] is only prioritized when there is no choice.[17]

Prioritization is complex, but critical. Every system can't be viewed as equally important. The plan should take into account system interdependencies, court resources, and essential business process priorities. Recovery efforts will be constrained by resources, so priorities should be clear and the plan flexible.

It may make sense to focus early on systems that are easiest to bring up, so that some aspects of the business can resume while recovery continues. For example, communication systems like phones may not be essential to dispensing justice but could make recovery efforts easier.

A response plan should include all the details necessary to act: who will be involved, the roles each will play, how the team will communicate, what steps each team member will take, and the timeframe for completing each task.

Similar to the "ABCs of First Aid" that help protect life, the response plan must attend to vital details quickly. Figure 1 – ABCs of Cybersecurity Incident Response introduces four basic task categories: assess, block, collect, and disseminate. These are not distinctly sequential steps, but

---

[16] United States Department of Justice. Computer Crime and Intellectual Property. *Best Practices for Victim Response and Reporting of Cyber Incidents*. Version 2.0. Washington, D.C.: Cybersecurity Unit, April 2018. Web.

[17] Email correspondence between P.L. Embley and unnamed court manager, 27 September 2019.

rather task categories that may need to be revisited repeatedly throughout an incident. The sequence of tasks in a court's response will also differ based on when, how, and by whom an incident is discovered.

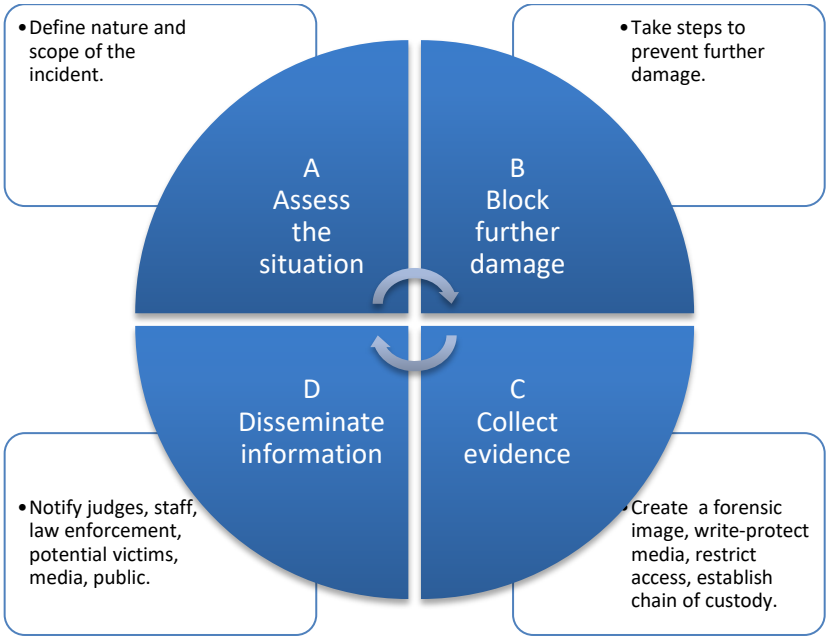

Figure 2 - ABCs of Cybersecurity Incident Response

Assess

Recognizing a cybersecurity incident is essential. While that may seem obvious, the reality is that the median number of days before an incident is discovered was 228, more than 7 months in 2020.[18] Cyberattackers often have access to systems and data for months (or years) before being detected.

Treat any suspicious event as an intrusion, even before you confirm it. It is better to take action that ultimately proves to be unnecessary than to risk additional harm. Pulling the network plug may be the best and most immediate action to take while you analyze whether or not the issue is a real intrusion or just equipment malfunction.

Identify the Intrusion

Automated alarms may alert IT to an intrusion attempt. If a court's website is defaced or redirects users inappropriately, the public may be aware of a breach before the court. Individuals may discover their personal information has been compromised and may recognize the source of the breach as the court. Worse still, the court's first notification

[18] Sobers, Rob. "98 Must-Know Data Breach Statistics for 2021.",Varonis, 6 Apr. 2021

may occur through a news story or contact from the FBI. In 2020, only 59% of security incidents were detected by the organizations themselves.[19]

Understand the Nature of the Intrusion

Obvious signs of a cyberattack might include suspicious emails or pop-up messages warning that a system has been compromised and instructing the user to click on a particular button or link to stop the attack. Less obvious signs may simply be a slower than usual connection or difficulty getting logged in to a system. Symptoms of a cyberattack differ according to the type of attack.

Some of the more common attack types may include:

Phishing Messages

A phishing message, or phishing email, is a type of online scam that involves a criminal falsely impersonating an employee, supervisor, other person or business who possess organizational authority or is considered a trusted source. Sophisticated phishing emails may come from "spoofed" work email addresses, making them appear legitimate. Unlike the fantastic claims of lottery winnings in foreign banks, spoofed phishing messages are meant to look like they come from trusted colleagues, law firms, district attorney/prosecutor's office, managers, or judges.

Slow Connections

In denial of service (DoS) and distributed denial of service (DDoS) attacks, systems are overloaded with irrelevant data requests. Resources for legitimate data requests are stretched and system response slows noticeably. Often, systems may crash as they are overwhelmed by attempting to process relevant and irrelevant data requests simultaneously.

Pop-Ups

Pop-ups that appear to be a legitimate mechanism for blocking a cyberattack may actually be malicious software. Pop-ups might include disguised links to malicious websites, fake coupons, or digital ads.

Ransomware

Ransomware attacks are meant to be noticed. Ransomware restricts a user's access to their system or data and often includes a demand for payment.

---

[19] "M-Trends 2021 Fireeye Mandiant Services, Special Report" *Mandiant*. A Fireeye Company, 2020.

Assess the Scope and Impact

Use automated logs to assess the scope of the intrusion. Logs should reveal which IT assets have been compromised and when events occurred.

> "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 (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."[20]

Systematically assess which networks, hardware, applications, and data files have been compromised. Where possible, identify the following:

- when the incident occurred;
- what methods were used in the cyberattack;
- how assets have been impacted;
- implications for other IT assets; and
- implications for court customers and justice partners.

Accurately assessing the event's scope and impact is essential to responding appropriately. The effort will be difficult and require resources. No organization will be able to respond perfectly. However, it is important to gather and analyze available information to gauge the severity of the incident.

Block

Preventing further damage is the highest priority. It may be necessary to take disruptive and costly steps such as removing infected computers and temporarily shutting down the court's website to limit damage. Consider reformatting hacked computers and restoring data with clean backups, or simply buying new computers.

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

- Maintain a log of steps taken to block the intrusion.
- Apply any relevant patches from software makers.

[20] Bradley Susan. "Tips to prep for digital forensics on Windows Networks". *CSO*, 30 Sept. 2020. Web.

- Secure user accounts; create new, complex passwords.
- Expand system monitoring and intrusion detection to ensure intruders do not regain access.
- Pay attention to physical security. Chaos can make physical pathways more accessible. Server rooms should always be locked, regardless of the inconvenience to incident response personnel. The theft of hardware because of lax security could compound the impacts of a cyber-intrusion.

Do not try to "defend" against an incident by attempting to access or damage a network thought to be the cause of a cyberattack. Under US law, "hacking back" could result in civil and/or criminal liability.[21] Because many cyberattacks are launched from compromised systems, "hacking back" could easily damage another victim's system, not the hackers.

Collect

No court has unlimited resources, and some courts may be tempted to limit their response to simply blocking the attack and getting on with day-to-day court business. However, it is essential that courts gather as much data as possible about the attack and do a thorough analysis and investigation. Understanding what happened is key to identifying the intruder, but more important, to preventing further intrusion.

Thorough data collection and analysis will help refine the initial assessment of the scope of the damage, and further inform other efforts and decisions. Details that are essential to capture include the following:

- machines affected;
- type, origin, and duration of the incident;
- malware used; and
- identity of the victims.

Do not modify or delete files that may be necessary to investigate the incident.

[21] Cybersecurity Unit, Computer Crime & Intellectual Property Section. *Best Practices for Victim Response and Reporting of Cyber Incidents Version 2.0*. Washington, D.C.: Cybersecurity Unit, Computer Crime & Intellectual Property Section, 2018. *Justice.gov*. Department of Justice, Sept. 2018. Web.

If the court's IT organization does not have the resources or skillsets necessary to investigate a cyberattack, retain a cybersecurity firm. Again, that agreement should be in place before an incident is suspected or discovered.

Capture Forensic Information

Using new or sanitized media, create a "forensic image" of affected computers.

> "A victim organization, or the incidence response firm it hires, may make a "forensic image" of the affected computers to preserve a record of a server at the time of the incident for later analysis and potentially for use as evidence at trial…It is important to create an image use forensically sound procedures; otherwise, there is a risk of altering the system in a manner that compromises its analytic or evidentiary value...it should write-protect the media to help ensure that it is not altered…and should also restrict access to the preserved media while documenting who has maintained possession of the media (chain of custody)."[22]

There may be digital "crumbs" that mark a path back to the perpetrators. Finding those clues can help reveal who is attacking and why. Collect evidence of the intrusion, including log or file creation data indicating that someone without proper authority "accessed, created, modified, deleted, or copied files or logs; changed system settings; or added or altered user accounts or permissions." [23]

Digital evidence may reveal the attacker's intention such as data transfer, disruption, ransom, or loss of public confidence. It can also reveal skill level to such as whether or not the malicious code is unique or a recycled updated of publicly available hacking tools.

Whether or not the intruder scanned the network before the intrusion may help identify the kind of intrusion. Someone with knowledge of internal systems (a targeted attack) may scan only for perimeter vulnerabilities while someone with no knowledge of the network would likely need to go looking for valuable data after successfully breaching the network.

- Preserve logs and file creation data indicating that someone improperly accessed, created, modified, deleted, or copied files or logs.

---

[22] Cybersecurity Unit, Computer Crime & Intellectual Property Section. *Best Practices for Victim Response and Reporting of Cyber Incidents Version 2.0*. Washington, D.C.: Cybersecurity Unit, Computer Crime & Intellectual Property Section, 2018. *Justice.gov*. Department of Justice, Sept. 2018. Web.

[23] McAndrew, Ed, and Anthony Di Bello. "How to Prepare for and Respond to a Cyberattack." *Network World*. Network World, Inc., 8 July 2015.

- Note when system settings changed.
- Identify new or altered user accounts or permissions.
- Determine if there are unauthorized "hidden" files and data stored on systems.
- Look for "hacker tools" or data stored from another intrusion on your network.[24]

Document Response Efforts

Create an ongoing record, documenting all steps taken to respond to the breach. Your plan should designate the person responsible and what information he/she should collect:

- Timeline of events and activities
  - Phone calls
  - Emails
  - Other contacts
- Inventory of all hardware and software on the network (including version)
  - Systems
  - Accounts
  - Services
  - Data
- Names of personnel and vendors working on tasks related to the intrusion

Disseminate

Providing timely and accurate information to all who need to know is essential in responding to a cyberattack. However, do not use compromised systems to communicate that information. Since most communication mechanisms rely on some form of technology, courts should have more than one method for disseminating urgent information to personnel, internal/external users, partner agencies, and the public. The

[24] Cybersecurity Unit, Computer Crime & Intellectual Property Section. *Best Practices for Victim Response and Reporting of Cyber Incidents Version 2.0*. Washington, D.C.: Cybersecurity Unit, Computer Crime & Intellectual Property Section, 2018. *Justice.gov*. Department of Justice, Sept. 2018. Web.

plan should identify the preferred communication method and scenarios when an alternate method should be utilized.

The designated spokesperson takes the lead in communicating key information to potential victims and the public.

- How the attacker gained access;
- Data compromised;
- Steps taken to contain the incident;
- What steps victims should take, if any, to protect themselves or their organizations;
- Actions taken to protect victims;
- Who to contact for more information; and
- When the next update will be provided.

Because information (and misinformation) flows quickly through informal channels including word of mouth and social media, it is important to communicate quickly to judges, court personnel, other courts, law enforcement, and where appropriate, the public. It will likely be necessary to make an initial public statement about a cybersecurity incident before all the facts are known, potentially even while a breach is ongoing. Share essential information as soon as it is known that an incident has occurred, to include appropriate contact information to address questions. Have a way to communicate with the local bar association so they can provide this information to local members. As part of the planning process, developing some vetted communication templates will allow for faster response that will also meet legal requirements.

Judges and Court Personnel

Court managers, judges, IT staff, facilities, and public relations personnel should be notified of the incident, any potential impact to their workflow, and steps being taken to respond. The response plan should define when and how all court personnel should be informed taking into account the structure of the court.

Law Enforcement

- Depending on the nature of the breach, it should be reported to one or more law enforcement entities. Ensure forensic data is preserved for incident investigation.

- Report incidents (including unsuccessful cyber intrusion attempts) to the US Computer Emergency Readiness Team (US-CERT).[25]

- Report computer crimes, intrusion episodes, and any attack on financial systems that involves fraud to the FBI.[26]

Bear in mind that law enforcement will involve themselves only to the extent they believe useful to finding and punishing perpetrators. Their interests and efforts may run counter to recovery efforts.

Other Courts and Agencies

A cybersecurity event in one court may convey an attack to another court. Even in local autonomy states, there is much interconnectivity. Notify the state AOC. In some instances, a state AOC may have resources to assist in responding to a cybersecurity incident. Notify the local bar association and agencies that regularly interact with the court. There may be a state cybersecurity agency that should also be alerted of an attack on the court.

Potential Victims

When a court's system is breached, potential victims include court personnel, other agencies, and the public, including juvenile and adult defendants, families, jurors, and victims/witnesses. Intrusion into a court's data could potentially compromise sensitive personnel information or reveal personally identifiable information that could make it possible to steal an individual's identity or threaten the safety of witnesses or those under protective orders. If court personnel have used their work email for personal business (i.e., applying for a home loan, preparing a tax return, making travel reservations, coordinating volunteer activities, etc.), the incident could impact the individual or others outside the court in unexpected ways.

All US states now have victim notification laws that proscribe minimum response requirements in the event of a cyberattack. Each state's legislation specifies the obligation and defines any provisions unique to government entities.[27] Be knowledgeable about your state's unique notification laws and incorporate those requirements into your response plan.

In most states, courts must consider the public as their "customer" and respond accordingly if personally identifiable information is compromised. In some instances, the

---

[25] "US-CERT Federal Incident Notification Guidelines." Cybersecurity and Infrastructure Security Agency, Apr. 2017. Web.

[26] "Cyber Incident Reporting." *FBI*. n.d. Web.

[27] See Security Breach Notification Chart at perkinscoie.com.

notification requirement is waived if law enforcement believe that notifying victims would "impede an investigation."[28]

The Media

Continued public trust and confidence in the court is dependent on a proactive approach to containing the breach and protecting sensitive data, as well as how information about those efforts is communicated. The organization whose systems were breached is a victim, as are all the individuals whose personal information was compromised.

Information should not be communicated through informal channels; provide regular official updates. It may take months or years to complete an investigation into the full extent of an intrusion.

- Share information as it becomes available. Explain what occurred and what steps are being taken to respond.
- Set expectations for when and how updated information will be communicated, then be consistent in providing the updates. Vague explanations and unpredictable follow-up give the public an impression of incompetence, or worse.

Testing the Plan

Once the plan is in place, ***test it frequently*** to ensure all systems across the enterprise are included, key personnel and contact details are still valid, and team members are trained and prepared to act. Practicing response procedures on a regular basis will help courts respond more efficiently and effectively, reducing the damage and resulting costs from an actual cyberattack. Walkthroughs and tabletop exercises can help team members understand their roles and provide an opportunity to discuss how the plan would work in the event of a real cyberattack. Functional and full-scale exercises simulate an actual attack.[29] There may be opportunities to partner with another agency to set up walk throughs and tabletop exercises. Plan testing involves a cross section of administrators, IT, internal users, vendors and even connected agencies and possibly provider organizations.

- Revisit monitoring and logging mechanisms to ensure they are functioning as intended.
- Reevaluate and, if necessary, reprioritize essential data assets.

---

[28] Cybersecurity Unit, Computer Crime & Intellectual Property Section. *Best Practices for Victim Response and Reporting of Cyber Incidents Version 2.0*. Washington, D.C.: Cybersecurity Unit, Computer Crime & Intellectual Property Section, 2018. *Justice.gov*. Department of Justice, Sept. 2018. Web.

[29] For more information, see "CISA Tabletop Exercise Package." *CISA.gov*. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, n.d. Web.

- Periodically review laws relating to data collection and privacy.

Federal and state laws and reporting requirements may overlap. Cybersecurity is a rapidly changing landscape; new threats, as well as new laws and rulings could impact the court's response plan.

Conclusion

Cyberattacks are a reality in today's data-driven world. As threat actors become more sophisticated and attacks are more frequent and publicized, courts must be prepared to confront incidents in full view of the public. Anticipating risks and preparing to effectively respond can help courts act with greater confidence when a cybersecurity incident unfolds. Creating and continually practicing and testing a cybersecurity response plan is essential. This should highlight the importance of educating users to be aware of what to look for, how to avoid risks, and how to respond to and notify the correct resources about suspicious activity. Responding confidently to an attack can reduce the negative implications of a breach, as well as help maintain the confidence of the public.

For more information, contact NCSC at technology@ncsc.org.

Appendix A: About Cyberattacks

To create an effective plan for responding to a cyberattack, court administrators must understand the variety of threats they must work to prevent, and to which they may one day have to respond.

Opportunistic Attacks

When a hacker attacks broadly hoping to discover vulnerability, the attack is considered "opportunistic." These are the most common kind of attacks. Looking for vulnerabilities is now highly automated. Attackers may intentionally code in a vulnerability and use "zombie networks" to crawl the Internet looking for "backdoors" into systems. Many email-based Trojan horse and worm attacks are primarily opportunistic.

Cybercriminals may be looking for social security numbers, credit card and banking information. Because courts accept payments for a variety of reasons, personally identifiable information (PII) is one form of cyberattack that may be more likely. As a payment recipient, courts align with private sector businesses in terms of risks in this area.

Targeted Attacks

If the attack is focused on a specific individual, organization or industry, it is a "targeted" attack: the attacker has a specific goal and more effort is expended to compromise the target. Examples of court-specific targeted attacks that could pose a serious risk for public safety might include attacks designed to gather (and/or potentially modify) witness or jury member information, case information, digital evidence, or sentencing details. Targeted attacks are generally considered more dangerous.

Motivations for a targeted attack may include revenge on a current or former employer, identity theft, or spying. For courts, it is not out of the realm of possibility that a hacker might attempt to destroy evidence, modify judgments, fabricate charges, or generally wreak havoc.

Cybercriminals may be looking for ways to disrupt automated security measures. In a suspicious incident at a correctional center in Florida in 2013, all of the cell doors at a maximum-security wing opened simultaneously, setting prisoners free.[30]

"Spear-phishing" is a clever and graphic term that describes a targeted attack using email with malicious files attached. Information is the target. The most likely targets of spear-phishing attacks in the courts are judges, administrators, and elected officials. Often these

[30] Zetter, Kim. "Prison Computer 'Glitch' Blamed for Opening Cell Doors in Maximum-Security Wing." *Wired.com*. Conde Nast Digital, 16 Aug. 2013. Web.

attacks are executed by having someone click on something in an email or website that looks legitimate.

Cyberspies collect proprietary or classified information that may be either profitable or advantageous. For example, in January 2021, Microsoft experienced a major vulnerability in its on-premises Exchange product, which supports email and calendaring. Up to four zero-day exploits took advantage of this vulnerability. This attack is suspected to originate from China and allows bad actors to siphon off emails from targeted organizations. "If used in an attack chain, all of these vulnerabilities can lead to Remote Code Execution (RCE), server hijacking, backdoors, data theft, and potentially further malware deployment."[31]

Cyberattack Tactics

Whether the attack is targeted or opportunistic, tactics commonly used in a cyberattack include unauthorized access to a computer system or data, viruses or malware that compromise systems, attacks that disrupt service on a website, and so-called "ransomware."

Unauthorized Access

Any access to a system, network, or information without authorization has compromised that system. Unauthorized access may come from within the organization, current and former personnel, or hostile individuals and organizations half-way around the world. The access may be by an individual or by another computer.

Malware and Viruses

Malware, short for MALicious softWARE, is software used to disrupt computer operations, gather sensitive information, gain unauthorized access, or encrypt data. Viruses, worms, and Trojan horses are all forms of malware. Using scripts, executable code, or other software spread through USB drives, or via text or email attachments, malware may be used to gather sensitive information including personally identifiable information (things such as social security numbers, birthdates), or to capture credit card information at Point of Sale (POS) terminals or on websites. Malware (or "computer contaminant" in state statutes) may be used to covertly track an individual's system or web use, or physical location.

Malware can take many forms and be used for a variety of purposes. Document-based viruses are the most common form of Malware. Spyware gathers user information covertly. Irritating adware displays advertisements continuously. Scareware produces

[31] Osborne, Charlie. "Everything you need to know about the Microsoft Exchange Server Hack". 16 March 2021. Web.

legitimate-looking warning messages, tricking victims into purchasing software that either has no benefit or that contains a malicious payload. A worm actively transmits itself over a network to infect other computers, and often contains functionality that interferes with the normal use of the systems infected. Cryptojacking, where hackers hijack computing power to mine cryptocurrency, is a new malware-like threat.[32]

Attacks That Disrupt Service

Denial of service (DoS) attacks make system resources unavailable for their intended users by either crashing the system, or by overwhelming it with irrelevant requests. A Distributed Denial of Service (DDoS) attack comes from more than one computer IP address. Some of the largest DoS attacks have temporarily crippled operations for online payment providers, banks, social media websites, and even the US stock market.

The increasing prevalence of Internet of Things (IOT) devices in homes and businesses and lack of security standards has prompted Congress to pass the IoT Cybersecurity Improvement Act of 2020 directing NIST and OMB to increase cybersecurity of IoT devices.[33]

Some who perpetrate DDoS attacks see them as a legitimate form of protest, similar to picketing a business. So-called "Hacktivists" use such attacks to disrupt day-to-day operations.

Ransomware

A cyberattack form of hostage-taking, ransomware is malicious software designed to block data or computer system functionality until a sum of money is paid. Some forms of ransomware may splash pornographic images across the user's screen. Users may be tempted to pay the ransom to avoid the embarrassment or the implicit suggestion that the user may have been viewing pornography while on the job.

Court personnel should be trained to recognize signs of ransomware and to respond promptly if ransomware is even suspected. Disconnecting from the Internet immediately can prevent data from being transmitted and limit the spread of the ransomware.

Municipalities are increasingly falling victim to ransomware attacks. Some are choosing to pay the ransom in a calculated attempt to reduce the cost to taxpayers and shorten the recovery timeline. An insurance policy may cover much of the ransom; the policy deductible may be significantly less than the cost of trying to reconstruct encrypted data.

---

[32] "Cryptojacking, Cybercriminals can unknowingly use your computer to generate cryptocurrency". Interpol. n.d. Web.

[33] See H.R. 1688 Public Law: 116-207. 4 Dec. 2020, Internet of Things Cybersecurity Improvement Act of 2020.

However, even a cyberbreach insurance policy will not ensure that attackers will actually release the data after the ransom is paid.

The United States is increasingly taking a pay no ransom posture. It recommends not paying ransoms because it funds the next attack. The US Treasury Department has an advisory that warns organizations not to pay ransoms as these payments may also violate economic sanctions imposed by the government on cybercriminal groups/organizations or state-sponsored hackers.[34] It would be good to read over the advisory since it states "OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to US jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC".[35] Consideration on ransomware payment or nonpayment should include a review of pertinent legal requirements and also weigh in potential additional penalties or sanctions.

Several European law enforcement agencies and a number of private internet security companies have joined forces to fight ransomware attacks through The No More Ransom project. The organization offers prevention advice and decryption tools. Victims of an attack can upload an encrypted file and/or the ransom note to hopefully diagnose the strain of ransomware and reverse the effects without paying the ransom.[36] US agencies have not yet signed on to the effort, but the resources are available to anyone, anywhere in the world. Courts may wish to leverage the resources of this well-respected organization.

Formjacking

Individuals making online payments can fall victim to formjacking, where malicious code added to a legitimate website captures credit card payment information. The victim's card information is then sold on the "cyber underground."

Any organization that accepts payments online can experience a formjacking attack. Smaller, less-sophisticated organizations are often the target. Regular pen (penetration) testing and vulnerability scans (ethical, controlled "hacking") can help identify and address formjacking.

---

[34] Constantin, Lucian. "US Treasury Department ban on ransomware payments puts victims in a tough position". CSO Magazine. 22 Oct. 2020.

[35] "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. Department of the Treasury. 1 Oct. 2020.

[36] See What can be done to fight against ransomware attacks?, Interview with Professor Josephine Wolff. *All Things Considered*. NPR.org. August 21, 2019.

Zero-Day Exploits

Attackers use unintentional flaws or vulnerabilities in a vendor's hardware or software, exploiting the flaw before the vendor realizes it exists. Often these attacks are not discovered for months or even years.

If the vulnerability exposes personal information that is used in identity theft, the public may be first to discover the problem. Even if the vendor discovers its own issue, these vulnerabilities are called "Zero-Day Exploits" because the application author has zero days after the flaw is uncovered to create and issue a patch or warn users of the issue and provide a workaround. One way to avoid Zero-Day Exploits is to keep system and browser software updated.

Social Engineering

The failure that compromises data and/or systems may be highly technical or not very technical at all. Humans trying to be helpful can be tricked into disclosing sensitive information or taking actions that facilitate access. For example, assisting a staff may assist a "tech support rep" by providing login information or holding a secured door open for the next person to enter. In a recent incident, a court payroll clerk received what appeared to be a legitimate email from the state court administrator requesting that his paycheck be deposited into a new checking account and providing the banking details. The clerk, trying to be responsive, redirected the deposit, even though the request had not come through the court's payroll deposit authorization process. The scam was discovered accidently, just a day or two before paycheck funds were misdirected. On closer scrutiny, it was obvious that the email had come from an external email account spoofing the court's email addresses. Many organizations are adding a banner to highlight that an email is outside of the organization to help users better identify potential phishing attempts using spoofed emails.

Supply Chain Attack

An emerging attack type uses the supply chain or value chain to infiltrate a network. It takes advantage of less secure elements by attacking third party vendor supported products or open-source code used by the organization to gain entry. Recently, software supply chain attacks have been on the rise where hackers manipulate code in the third-party software to compromise downstream applications. "This has dramatically changed the attack surface of the typical enterprise in the past few years, with more suppliers and service providers touching sensitive data than ever before."[37] This is why it is important

[37] Korolov, Maria. "Supply chain attacks shows why you should be wary of third-party providers". 4 Feb, 2021. CSO Online. Web.

to engage more purposefully with vendors about their cybersecurity posture, planning, notification and recovery operations.

Appendix B: 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 at regular intervals. Don't 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 "Principle of Least Privilege" 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 multi-factor 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 C: 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 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?