JTC Resource Bulletin

Cybersecurity Basics for Courts

Version 2.0
Adopted 4 December 2019

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

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
David Slayton (Co-Chair)
Texas Office of Court Administration

David K. Byers
Arizona Supreme Court

Jeff Shorba
State Court Adminstrator's Office, Minnesota

Rodney Maile
Administrative Office of the Courts, Hawaii

Laurie Dudgeon
Kentucky Administrative Office of the Courts

NCSC Appointments
Justice Constandinos Himonas
Utah Supreme Court

The Honorable Samuel A. Thumma
Arizona Court of Appeals

Ex-officio Appointments
Joseph D.K. Wheeler
IJIS Courts Advisory Committee

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

CITOC Appointments
Jorge Basto
Judicial Council of Georgia

Casey Kennedy
Texas Office of Court Administration

NCSC Staff
Paul Embley
Jim Harris

Table of Contents

Executive Summary

Accepting that courts *will* face cybersecurity incidents is essential. Prevention efforts are still important. However, prevention efforts must now be coupled with preparations to respond when the inevitable occurs.

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. 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.

Preventing incidents

While careful prevention cannot ensure immunity from incident, it can reduce risks dramatically, limit the impact of an attack, and lay the groundwork for 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. Review the threat surface each time a system is implemented or upgraded.

Reduce the threat vector

Reducing geographic access to applications (despite credentials) can help 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. Have the ability to quickly disable lost devices. Ensure file encryption utilities are installed and enabled.

Limit access to systems, processes and data

The Principle of Least Privilege is an IT best practice that reduces risks by giving people and systems only the specific access they need to perform their role.

Use only authorized software

Software on the enterprise network should be licensed and current, and installed and configured by tech staff.

Manage accounts and passwords

Ensure user activities can be attributed as well as audited. Require complex, unique passwords.

Segment the network

Firewalls used to separate various network segments add a layer of complexity that makes it more difficult for malware to access data.

Invest in cybersecurity

Organizations must budget for cybersecurity – software, services, and staff time to include the cost of training all employees.

Own it

Cybersecurity must be viewed as the responsibility of every individual in the organization, not just the IT group.

Assembling a cybersecurity incident response team

A court's cybersecurity team should include representatives from each department that would be involved in handling an incident or notifying others (either the public or court personnel). At a minimum, that team should include the Chief Judge/Justice, Court Administrator/CEO, CIO, IT Security Officer, Public Information Officer, HR, legal, and cybersecurity response vendors.

Identify the spokesperson

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.

Meet regularly

The incident response team should meet on a regular basis, ideally at least quarterly. During an incident, the team should meet frequently to share information, monitor recovery efforts, and adjust to new information.

Establish channels of communication

Collect, protect, and share contact information for individuals and organizations (personnel, IT vendors, security, police, etc.), both daytime and after hours/weekends. Ensure your response plan anticipates interdepartmental and cross-functional communications that will be required to work cohesively

Laying the groundwork for recovery

An effective post-incident response plan requires key components be in place before an incident occurs.

Identify essential data assets

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

Document systems

Documentation may be used to review and address potential security gaps and will become the road map for recovery in the event of an incident.

Create redundancy

Ensure backups are current and network diverse. An offline "island" of redundant data will make it much easier to recover if an incident occurs.

Enable logging and implement automated monitoring

Make full use of monitoring, logging, and diagnostic tools on an ongoing basis. Implement security monitoring and attack detection systems that 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; include provisions allowing the court to audit security procedures.

Be familiar with the laws governing data collection and privacy

Courts must protect the personally identifiable information they collect and are not immune from the legal implications and financial penalties of a data breach. Be familiar with both state and federal laws relating to data protection.

Understand the implications of shared technology infrastructure

Court IT assets may sit on a network the court doesn't control and has little visibility into. Courts should not take it for granted that partner agencies are following best practices and have resources dedicated to cybersecurity.

Anticipate malicious intent

Those who have experienced a cyberattack emphasize the importance of not underestimating malicious intent.

Developing the Plan

Establish and document procedures to follow in the aftermath of a cybersecurity incident. Make sure judges, supervisors, and management staff are all aware of the plan and the expectations. Ensure response procedures are logical within the context of your court's organization and processes, and that they align with existing court policies. Task categories may need to be revisited repeatedly throughout an incident and the sequence of tasks will differ based on how an incident is discovered.

The ABCs of a cyber-incident response plan fall into four basic task categories: assess, block, collect, and disseminate. These are not sequential steps and will likely need to be revisited repeatedly throughout an incident.

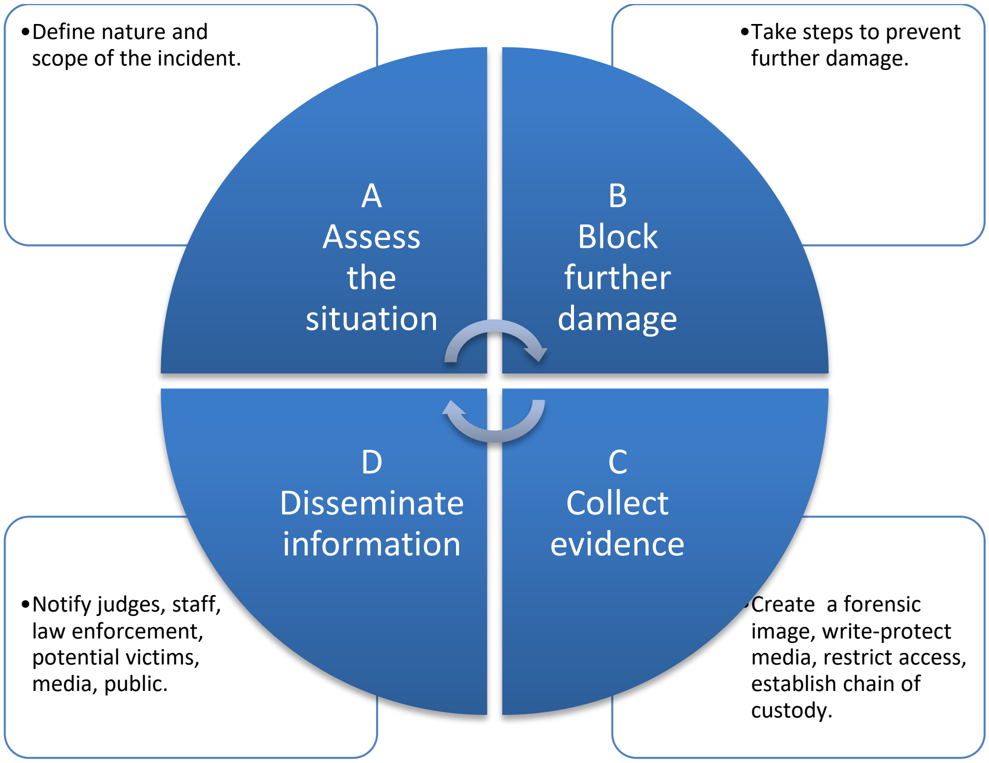
•Define nature and scope of the incident.
•Take steps to prevent further damage.
A
Assess the situation
B
Block further damage
D
Disseminate information
C
Collect evidence
•Notify judges, staff, law enforcement, potential victims, media, public.
•Create a forensic image, write-protect media, restrict access, establish chain of custody.

Figure 1 - ABCs of Cyber Incident Response

Testing the Plan

Test the plan frequently to ensure all systems across the enterprise are included, personnel and contact details are still valid, and staff are trained and prepared to act. Practicing response procedures will help courts respond more efficiently and effectively, reducing the damage and resulting costs from an actual cyberattack.

Introduction

Cybersecurity is a topic of broad interest. 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.[1]
>
> 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[2] 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."[3] 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.

Cyberattacks include malware, viruses, denial of service (DOS) attacks, ransomware, zero-day exploits, and unauthorized access from within the organization (current and former employees) or by hostile individuals and organizations halfway around the world.[4] Attacks may be targeted at the court specifically or may simply be opportunistic.

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

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

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

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

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.

State of cybersecurity in courts

The number, scope, and breadth of organizations experiencing cybersecurity incidents in the past few years is vast and unsettling. Courts that have experienced a cybersecurity incident are in good company. Utilities to universities 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. Attacks against courts are on the rise.

Taking steps to prevent a cyberattack is clearly worth focused attention. However, the reality is that regardless of preventive measures, most organizations will deal with some form of cybersecurity incident at some point. In fact, a cybersecurity incident may already be ongoing. Because any organization with data or a public-facing role can be targeted, court managers must have an established plan for responding. 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.

Unlike the threats organizations and individuals faced fifty years ago, cybersecurity is an issue no matter the industry, geography, or jurisdiction. 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. James D. Comey, former FBI Director, compared the “vector change” of cybercrime to the changes that came in the 1920s and 1930s when “…the confluence of the automobile and asphalt… gave birth to an entirely new way of doing bad things.” The confluence of complex interrelated systems and the Internet has had a similar impact, giving criminals entirely new ways of doing bad things digitally.

Comey went on to say that cybercriminals today are like outlaws Dillinger or Bonnie and Clyde doing “…a thousand robberies in all 50 states in the same day from their pajamas from Belarus.”

> The traditional notions of space and time and venue and border and my jurisdiction and your jurisdiction are blown away by a threat that moves not at 40

> miles an hour or 50 downhill, but at 186,000 miles per second. The speed of light.[5]

Accepting that courts *will* face cybersecurity incidents is essential. Prevention efforts are still important. However, prevention efforts must now be coupled with preparations to respond when the inevitable occurs. 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] It 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, and any other internet-connected devices.[7]

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.

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,

[5] Comey, James B. "Addressing the Cybersecurity Threat." International Conference on Cybersecurity. Fordham University, NY, NY. 7 Jan. 2015. Address.

[6] For more information, see "Attack Surface Analysis Cheat Sheet." *The Free and Open Software Security Community*. The Open Web Application Security Project (OWASP), 18 July 2015. Web.

[7] Stolen vendor credentials were used in the cyberbreach of Target stores in late 2013. See Wallace, Gregory. "Stolen Credentials Blamed in Target Breach." *CNNMoney*. Cable News Network, 29 Jan. 2014. Web.

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 staff do not give individuals without proper credentials access to equipment or secured spaces.

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,[8] an IT best practice that reduces risks by giving people and systems only the specific access they need to perform their role.

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 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 be unimpacted.

Use only authorized software

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. 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

[8] For more information, see https://csrc.nist.gov/glossary/term/least-privilege.

issues. Ensure systems within your organization are configured to update software regularly. Have policies and processes in place to remove unauthorized software.

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 log users 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.

Require complex, unique passwords. Automate periodic user password reset requirements. Don't use the same password on multiple systems. Phrases are longer and therefore harder to guess, but can be easier to remember, e.g., 1twillb3Fr!day$00n. Train staff not to use the same passwords at home and at work. Where possible, utilize multi-factor authentication, which requires two or more categories of credentials, e.g., password or pin plus a smart card or biometric identifier (fingerprint, iris scan, facial recognition, etc.).

Invest in cybersecurity

Organizations must budget for cybersecurity – software, services, and staff time to include the cost of training all employees. According to the Accenture 2019 *Cost of Cybercrime* report, "Training employees to think and act with security in mind is the most underfunded activity in cybersecurity budgets."[9] User behaviors including clicking on phishing links make up a quarter of all cyberbreaches.[10] At the same time, phishing is 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

[9] Bissell, Kelly, and Larry Ponemon. *The Cost of Cybercrime - Ninth Annual Cost of Cybercrime Study, Unlocking the Value of Improved Cybersecurity Protection*. Accenture, 2019.

[10] "Cost of a Data Breach Study." *IBM*, IBM Security and Ponemon Institute, 2019, www.ibm.com/security/data-breach. Covers data breach incidents between July 2018 and April 2019.

certifications. Untrained staff may unintentionally do more harm than good in attempting to re-route a network or stand up clean workstations.

Own it

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

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 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.

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

- **IT Security Officer**
  Ensures the team's responses meet legal mandates. May collect digital forensic evidence and/or act as liaison to law enforcement and other agencies.

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

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

- **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 an employee of the court. Ensure your response plan anticipates interdepartmental and cross-functional communications that will be required to work cohesively.

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

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.

- Anticipate the potential impact of the loss of essential data assets.
- Understand what functions depend on what data.

Document systems

Documentation may be used to review and address potential security gaps and will become the road map for recovery in the event of an incident.

- Keep network and application documentation up to date.
- Fully document backup and recovery processes and locations.

Create redundancy

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

- Regularly test backups by attempting to restore randomly selected files.
- Periodically attempt a full restore.
- At least one complete backup should be stored offline and off premise.

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.
- 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.

- 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.

Understand the implications of shared technology infrastructure

Court IT assets may sit on a network the court doesn't control and has little visibility into. It can be easy to simply assume the city or county has controls in place to guard against intrusion. Yet, local governments are increasingly targeted, and their cybersecurity controls and response plans have too often proven inadequate.

City and county networks may support municipal government 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.

- 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.

Be familiar with the laws governing data collection and privacy

Courts must not only protect the personally identifiable information (PII) they collect, but also obtain consent of system users to monitor communications in order to detect and respond to an intrusion.[11] 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 from 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.[12]

Anticipate malicious intent

Those who have experienced a cyberattack emphasize the importance of not underestimating malicious intent. Cyberattacks may not only target data but also

[11] 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.

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

> 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 behind cybersecurity incidents. Understanding that would have prompted much greater caution and swifter action.[13]

Developing the plan

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 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.[14]

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 your 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 exposure 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."

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

[14] United States Department of Justice. 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.

> 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.[15]

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 Cyber Incident Response introduces four basic task categories: assess, block, collect, and disseminate. These are not distinctly sequential steps, but 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.

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

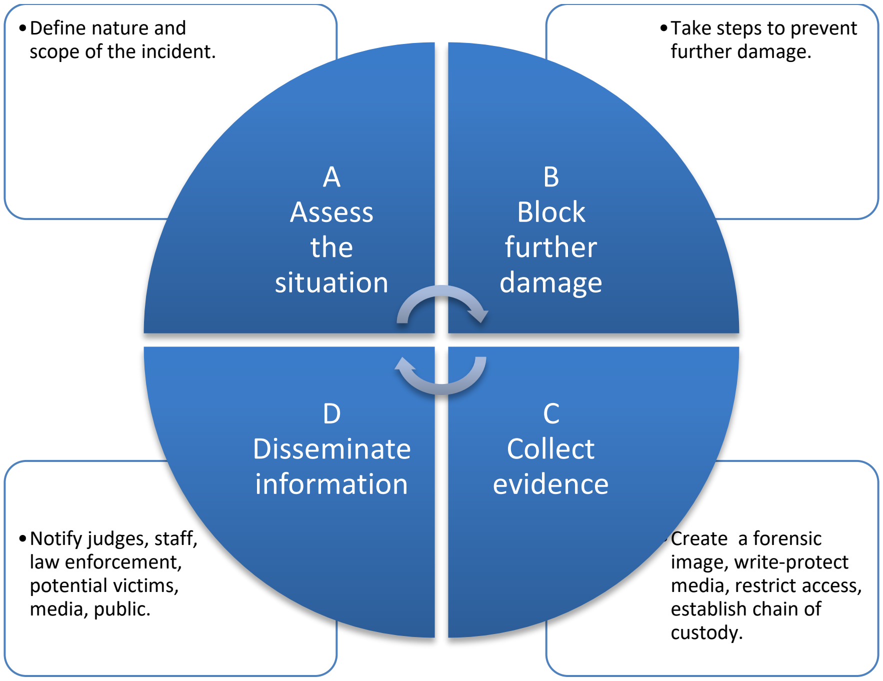
Define nature and scope of the incident.
Take steps to prevent further damage.
A Assess the situation
B Block further damage
D Disseminate information
C Collect evidence
Notify judges, staff, law enforcement, potential victims, media, public.
Create a forensic image, write-protect media, restrict access, establish chain of custody.

Figure 2 - ABCs of Cyber 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 279 – more than 9 months -- in 2019.[16] 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 may occur through a news story or contact from

[16] "Cost of a Data Breach Study." *IBM*, IBM Security and Ponemon Institute, 2019, p. 6. www.ibm.com/security/data-breach. Covers data breach incidents between July 2018 and April 2019.

the FBI. In 2014, sixty-nine percent of institutions learned of a breach from an outside entity such as law enforcement.[17]

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.

Phishing Messages

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.

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.

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.

[17] "Threat Report: A View from the Front Lines." *Mandiant*. A Fireeye Company, 2015. p. 5. Web.

> A key tool in recognizing data intrusions is the lowly log file, a standard feature of almost every operating system, application, server platform and related software in the corporate IT world.[18]

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.
- Implications for court clients 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.

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

[18] Tittle, Ed, and Earl Follis. "How Better Log Monitoring Can Prevent Data Breaches." *CIO*. CXO Media Inc., 24 Feb. 2015. Web.

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.[19] Because many cyberattacks are launched from compromised systems, "hacking back" could easily damage another victim's system, not the hacker's.

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
- Identity of victims

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

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.

> "Ideally, the victim of a cyberattack will make a forensic image of the affected computers as soon as the incident is detected. Doing so preserves a record of the system for analysis and potentially for use as evidence at a trial. Restrict access to these materials in order to maintain

[19] Cybersecurity Unit, Computer Crime & Intellectual Property Section. *Best Practices for Victim Response and Reporting of Cyber Incidents*. Washington, D.C.: Cybersecurity Unit, Computer Crime & Intellectual Property Section, 2015. *Justice.gov*. Department of Justice, Apr. 2015. Web.

> the integrity of the copy’s authenticity. Safeguard these materials from unidentified malicious insiders and establish a chain of custody.”[20]

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.”[21] Digital evidence may reveal the attacker’s “intent, skill level, and knowledge of the target.”[22]

> As the tools, techniques, and procedures of criminal and APT [Advanced Persistent Threat] actors coalesce, you must scrutinize actors’ intent and motivations. Only then can you properly assess the potential impacts of security incidents, respond appropriately, and create a security strategy appropriate for the threats you face.[23]

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.
- Note when system settings changed.
- Identify new or altered user accounts or permissions.

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

[21] Cybersecurity Unit, Computer Crime & Intellectual Property Section. *Best Practices for Victim Response and Reporting of Cyber Incidents*. Washington, D.C.: Cybersecurity Unit, Computer Crime & Intellectual Property Section, 2015. *Justice.gov*. Department of Justice, Apr. 2015. Web.

[22] Smith, Lee. "Targeted Vs Opportunistic Attacks." *Independent Information Security*. CQR, 15 Sept. 2014. Web.

[23] "Threat Report: A View from the Front Lines." *Mandiant*. A Fireeye Company, 2015. Web.

- 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 employees, partner agencies, and the public. The 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.

[24] United States Department of Justice. 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.

- 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.
- 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. Have a way to communicate with the local bar association so they can provide this information to local members.

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.

[25] "Incident Definition." *US Computer Emergency Readiness Team - Incident Reporting System*. Department of Homeland Security, n.d. Web.

[26] "When to Contact the FBI." *FBI*. 17 Mar. 2010. Web.

Other courts and agencies

A cyber 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.

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 identifying 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 employee 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 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.

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

[28] United States Department of Justice. 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.

> 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.

> …organizations who conducted extensive testing of an IR plan had an average total cost of a breach that was $1.23 million less than those that neither had an incident response team or tested their incident response plan…[29]

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.[30]

- Revisit monitoring and logging mechanisms to ensure they are functioning as intended.
- Reevaluate and, if necessary, reprioritize essential data assets.
- Periodically review laws relating to data collection and privacy.

[29] “Cost of a Data Breach Study.” *IBM*, IBM Security and Ponemon Institute, 2019, p. 9. www.ibm.com/security/data-breach. Covers data breach incidents between July 2018 and April 2019.

[30] For more information, see "Exercises." *Ready.gov*. Department of Homeland Security, n.d. Web.

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 cyber response plan is essential. 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 identifying 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.

> Today, common criminals, organized crime rings, and nation-states leverage sophisticated techniques to launch attacks that are highly targeted and very difficult to detect.[31]

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.

[31] *US Cybercrime: Rising Risks, Reduced Readiness: Key Findings from the 2014 US State of Cybercrime Survey*. PwC Cybersecurity and Privacy. PricewaterhouseCoopers LLP, 2014. Web.

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.[32]

"Spear-phishing" is a clever and graphic term that describes a targeted attack using email with malicious files attached. Information is the target. "Every organization is at risk of being the target of a spear-phishing attack."[33] The most likely targets of spear-phishing attacks in the courts are judges, administrators, and elected officials.

Cyberspies collect proprietary or classified information that may be either profitable or advantageous. Operation Shady Rat used a spear-phishing attack to successfully steal government and corporate data from more than 70 agencies, including eight state and county governments, over a period of five years before being discovered by McAfee Security in 2011.[34] Infected emails were sent to employees, who unintentionally downloaded attachments.

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 employees, 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

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

[33] Federal Bureau of Investigation. San Diego Division. *FBI Warns of Spear-Phishing E-Mail with Missing Children Theme*. *The FBI*. Federal Bureau of Investigation, 26 Aug. 2013. Web.

[34] Alperovitch, Dmitri. *Revealed: Operation Shady RAT*. www.McAfee.com. Rep. Santa Clara, CA: McAfee, 2011. Web. See page 4 for a breakdown of organizations impacted.

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 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.[35]

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. According to Ryan Cox of SiliconANGLE, DOS (Denial of Service) or DDoS (Distributed Denial of Service) attacks are the single largest threat[36] to the Internet, and the devices, organizations, and individuals that it serves. Some of the largest DoS attacks have temporarily crippled operations for online payment providers, banks, social media websites, and even the US stock market.

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.

[35] Wilbur, Jeff. "The silent rise of cryptojacking." *SC Magazine*. CyberRisk Alliance, LLC. 17 Dec. 2019. Web.

[36] Cox, Ryan. "5 Notorious DDoS Attacks in 2013 : Big Problem for The Internet of Things." *SiliconANGLE*. SiliconANGLE Media, 26 Aug. 2013. Web. 10 Sept. 2015.

Ransomware

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

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.[37] 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." According to the Symantec 2019 Internet Security Threat Report,[38] formjacking is on the rise.

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

[38] *Internet Security Threat Report (ISTR) 2019*. Vol. 24. Symantec Corporation, Feb. 2019, www.symantec.com

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.

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 “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.

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-premise backup to facilitate recovery if online backups are compromised.	Advanced
□	Segment the network.	Advanced