JTC Resource Bulletin

Responding to a Cyberattack

Version 1.0
Adopted February 17, 2016

Abstract

Cybersecurity threats are increasing 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 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

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

Laurie Dudgeon
Kentucky Administrative Office of the Courts

Robin Sweet
Nevada Administrative Office of the Courts

NACM Appointments

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

Paul DeLosh
Supreme Court of Virginia

Danielle Fox
Circuit Court for Montgomery County, Maryland

Kelly C. Steele
Florida Ninth Judicial Circuit Court

Jeffrey Tsunekawa
Seattle Municipal Court

NCSC Appointments

The Honorable O. John Kuenhold
State of Colorado

The Honorable Michael Trickey
Washington Court of Appeals, Division 1

CITOC Appointments

Jorge Basto
Judicial Council of Georgia

Casey Kennedy
Texas Office of Court Administration

Ex-officio Appointments

Joseph D.K. Wheeler
IJIS Courts Advisory Committee

NCSC Staff

Paul Embley
Jim Harris
Ilonka Dazevedo

Table of Contents

Abstract ii

Document History and Version Control ii

Acknowledgments iii

Table of Contents iv

Executive Summary v

Introduction 1

Lay the Groundwork 2

- Identify your court's essential data assets 2
- Enable logging and implement automated monitoring 3
- Be familiar with the laws governing data collection and privacy 3
- Map out the threat surface 3
- Review Terms and Conditions of contracts with vendors 4

Develop the plan 4

- Create a cybersecurity incident response team 5
- Plan primary and secondary communication channels 5
- Identify tasks and responsibilities 6
  - Assess 7
  - Block 9
  - Collect 10
  - Disseminate 12

Test the plan 15

Conclusion 15

Appendix: About Cyberattacks 17

- Targeted and Opportunistic Attacks 17
  - Targeted Attacks 17
  - Opportunistic Attacks 18
- Cyberattack Tactics 18
  - Unauthorized access 19
  - Malware and Viruses 19
  - Attacks that Disrupt Service 19
  - Ransomware 20
  - Zero-Day Exploits 20

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.

Lay the Groundwork

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

Identify your court's 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, financial transactional information, digital evidence, and personnel information.

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.

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.

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.

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.

Develop the Plan

Establish and document procedures to follow in the aftermath of a cybersecurity incident. The 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.

Create a cybersecurity incident response team

The team should include representatives from each department or organization that would be involved in handling an incident or notifying others and should meet regularly.

Plan primary and secondary communication channels

Anticipate that email and phone systems may not be functioning. Ensure the plan incorporates interdepartmental and cross-functional communications.

Identify tasks and responsibilities

Identify the specific tasks to be performed, who is responsible for each task, and who will cover those tasks in the event the designated individual is unavailable. The plan must help the court assess the scope of the incident, block further intrusion, collect key information, and disseminate information quickly and appropriately.

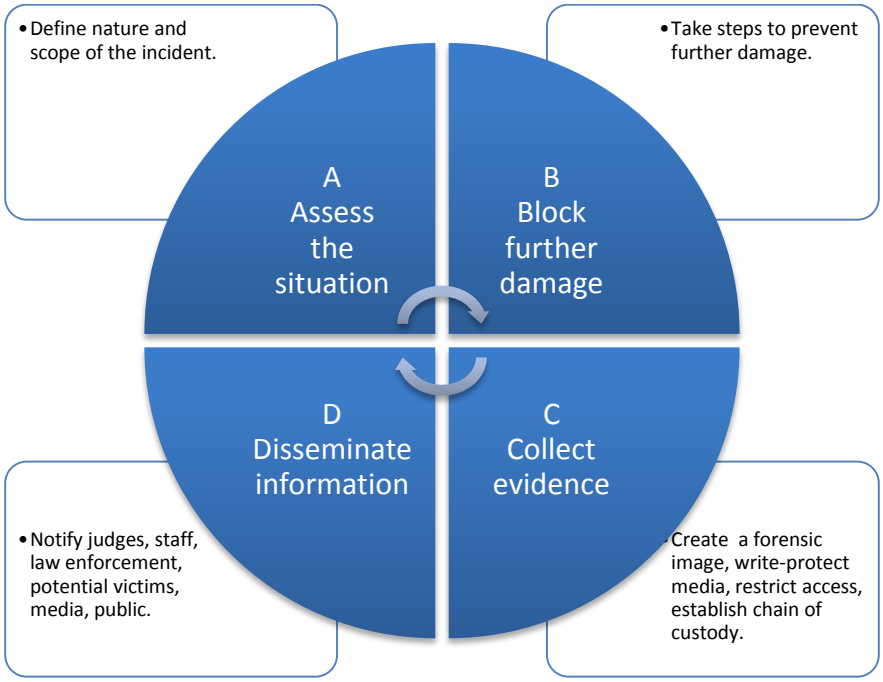

Figure 1 - ABCs of Cyber Incident Response

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.

Test the Plan

Test the plan least annually to ensure all systems across the enterprise are included, and personnel and contact details are still valid.

Introduction

"There are two kinds of organizations:
Those who have been hacked and those who will be."[1]

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, undiscovered for months or years.[2] Because courts will likely have cybersecurity incidents, they should have an established plan for responding.

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. A cyberattack may be used to gain access on an ongoing basis to networks or databases, resulting in a data breach (or cyberbreach).

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.

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 a cybersecurity incident because they don't manage large databases of credit card information. However, threats are real and increasing. James D. Comey, Director of the Federal Bureau of Investigation, 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

---

[1] Kaffenberger, Lincoln. "Five Steps Leaders Must Take to Prepare for a Cyberattack." *In Public Safety*. American Military University, 21 Feb. 2014. Web. 08 Sept. 2015.

[2] "… attackers still had a free rein in breached environments far too long before being detected—a median of 205 days in 2014." Threat Report: A View from the Front Lines." *Mandiant*. A Fireeye Company, 2015. Web. 11 Jan. 2016.

[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: About Cyberattacks.

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 plan in place can help courts respond more effectively, mitigating some effects of an attack and/or breach. This paper identifies the tasks that must be addressed in the aftermath of an incident, and the steps courts must take before an incident occurs in order to prepare.

Lay the Groundwork

An effective post-incident response plan requires that several 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 your court's essential data assets

Courts must know what data they hold, or that vendors hold on their behalf. What data exists and where is it stored? 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, juror identities, and other details stored digitally are vulnerable to a cybersecurity incident. Anticipate the potential impact of the loss of essential data assets. Understand what functions

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

depend on what data, and create redundancies so that data can be quickly recovered/restored if an incident occurs.

Enable logging and implement automated monitoring

Having the ability to detect an intrusion is essential. On an ongoing basis, capture and store log information from switches, routers, proxy servers, firewalls, etc. Implement user consent login banners/warnings. Make full use of monitoring, logging, and diagnostic tools on an ongoing basis, 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. 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 is an essential security measure that will dramatically improve the court's ability to investigate and respond to a cybersecurity incident.

Be familiar with the laws governing data collection and privacy

Courts with a web presence 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.[6] 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.[7]

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.[8] It includes network and software vulnerabilities, as well as humans. Identify potential points of entry, open ports,

---

[6] 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.

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

[8] 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. 26 Jan. 2016.

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 and alarm system monitoring.[9] 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.

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 when the source and extent are investigated. Contracts should include provisions allowing the court to audit the vendor's security procedures. Ensure you are part of *their* cybersecurity incident response plan.

Develop the plan

Establish and document procedures to follow in the aftermath of a cybersecurity incident. Ensure response procedures are logical within the context of your court's organization and processes, and align with existing court policies. If necessary, modify policies and processes.

> …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.[10]

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 will not be clear until the plan is tested, or executed in a real situation.

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.

---

[9] 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. 22 Jan. 2016.

[10] 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.

Create a cybersecurity incident response team

A court's cybersecurity incident response team should include representatives from each department or organization that would be involved in handling an incident or notifying others (either the public or within the court). 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.

This team should meet regularly, and in the event of an incident, meet frequently to discuss and determine the best courses of action. Each individual on the team brings a unique organizational perspective that will be important in addressing all the implications of the cybersecurity incident.

Plan primary and secondary communication channels

Anticipate that organizational contact mechanisms (like email and phone systems) may not be functioning. Collect and protect contact information for individuals and organizations (personnel, IT vendors, security, police, etc.), both daytime and after hours/weekends. Depending on the court's organization, the

IT point of contact may not be an employee of the court. In some courts, IT functions may be the responsibility of the county IT department. Ensure your response plan anticipates any interdepartmental and cross-functional communications that will be required to work cohesively.

Identify tasks and responsibilities

Identify the specific tasks to be performed in the response as well as who is responsible for each task. The plan should also identify who will cover those tasks in the event the designated individual is unavailable. While IT will clearly lead efforts to address the technology ramifications, IT should not be the only department aware of and responding to an attack. Determine who will act as spokesperson: Chief Judge or Justice, PIO or other court leader. Ensure the spokesperson is the only one speaking publicly about the incident. Having multiple, divergent versions of the incident going out to the public and the press from multiple "official" sources will add confusion and complexity to communication efforts. Meeting regularly throughout the incident is critical to ensuring the response team is unified in their response efforts and that information is being communicated accurately, effectively, and in a timely way.

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.

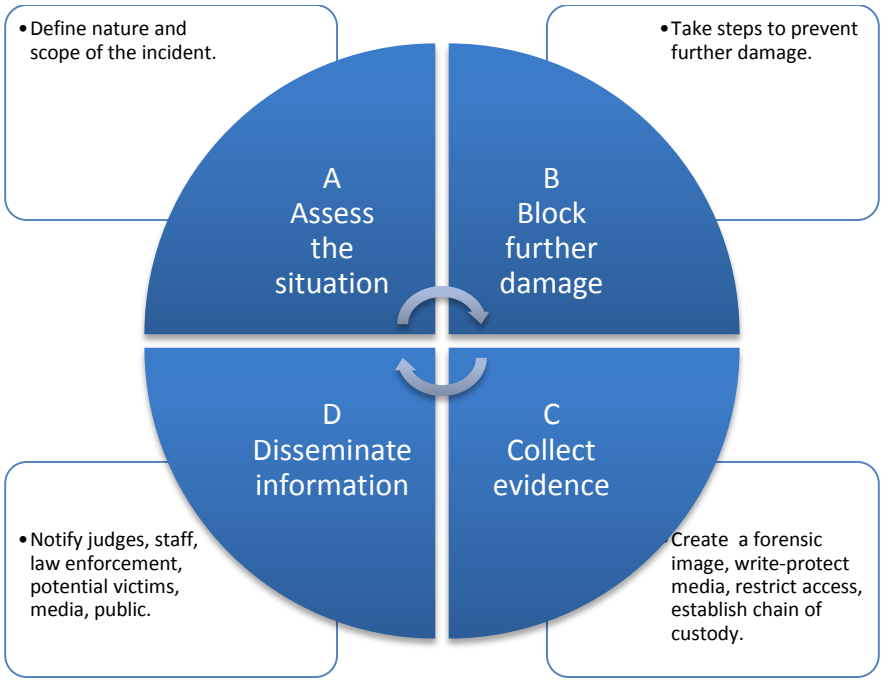

Figure 2 - ABCs of Cyber Incident Response

Assess

Recognizing a cybersecurity incident has occurred or is occurring is essential. While that may seem obvious, the reality is that the median number of days before an incident is discovered is more than 200.[11] This means that cyberattackers often have access to systems and data for more than six months before being detected.

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 is aware. 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 the FBI. In 2014, sixty-nine percent of institutions learned of a breach from an outside entity such as law enforcement.[12]

[11] "Threat Report: A View from the Front Lines." *Mandiant*. A Fireeye Company, 2015. p. 1. Web. 11 Jan. 2016.

[12] Ibid., p. 5.

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

Most email systems automatically screen for obviously suspicious emails purporting to require you to log in to your bank, credit card, or PayPal account. However, individuals are still responding to bogus links in sufficient numbers to make this a common cyberattack tactic. More 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 appear as if they are, in fact, actions being requested by trusted colleagues, managers, or potentially, 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 not subtle. Unlike malware or other disguised mechanisms, they are meant to be noticed. Ransomeware restricts a user's access to their system or data and often includes a demand for payment.

Assess the scope and impact

Use logs to help assess the scope of the intrusion. Automated logs can help identify which IT assets have been compromised and when events occurred.

> 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.[13]

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 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.

If hackers exploit a software flaw, apply a patch from the software maker that fixes the problem or implement a recommended workaround. If passwords were stolen, secure accounts and set new, complex passwords that will be harder to crack.

Do NOT modify or delete files that may be necessary to investigate the incident. Maintain a log of steps taken to block the intrusion.

Do NOT respond 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

[13] Tittle, Ed, and Earl Follis. "How Better Log Monitoring Can Prevent Data Breaches." *CIO*. CXO Media Inc., 24 Feb. 2015. Web. 08 Dec. 2015.

criminal liability.[14] Because many cyberattacks are launched from compromised systems, "hacking back" could easily damage another victim's system, not the hacker's.

Expand system monitoring and intrusion detection to ensure intruders do not regain access.

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 importantly, 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

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

[14] 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. 15 Dec. 2015.

> the integrity of the copy's authenticity. Safeguard these materials from unidentified malicious insiders and establish a chain of custody."[15]

Cybercriminals often unintentionally leave digital "crumbs" similar to the trail of bread crumbs Hansel and Gretel left to mark the path back home. 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."[16] Digital evidence may reveal the attacker's "intent, skill level, and knowledge of the target."[17]

> 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.[18]

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.

---

[15] McAndrew, Ed, and Anthony Di Bello. "How to Prepare for and Respond to a Cyberattack." *Network World*. Network World, Inc., 8 July 2015. Web. 18 Sept. 2015.

[16] 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. 15 Dec. 2015.

[17] Smith, Lee. "Targeted Vs Opportunistic Attacks." *Independent Information Security*. CQR, 15 Sept. 2014. Web. 16 Sept. 2015.

[18] "Threat Report: A View from the Front Lines." *Mandiant*. A Fireeye Company, 2015. Web. 11 Jan. 2016.

- Look for “hacker tools” or data stored from another intrusion on your network.[19]

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 (include 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.

Your plan’s designated spokesperson takes the lead in communicating key information to potential victims and the public.

- How the attacker gained access.

[19] 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.

- 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.

Because information (and mis-information) 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.

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. Based on the structure of the court, the response plan should define when and how all court personnel should be informed.

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. For tracking purposes, incidents (including unsuccessful cyber intrusion attempts) should be reported to the US Computer Emergency Readiness Team (US-CERT).[20] Computer crimes, intrusion episodes, and any attack on financial systems that involves fraud should be reported to the FBI.[21]

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.

---

[20] "Incident Definition." *US Computer Emergency Readiness Team - Incident Reporting System*. Department of Homeland Security, n.d. Web. 18 Sept. 2015.

[21] "When to Contact the FBI." *FBI*. 17 Mar. 2010. Web. 18 Sept. 2015.

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 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.

As of January 2015, all but three states (Alabama, New Mexico and South Dakota) had enacted legislation that requires companies to contact potential victims of a cyberattack. Each state's unique legislation specifies the obligation and defines any provisions unique to government entities.[22] 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 believes that notifying victims would "impede an investigation."[23]

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.

> More victims are publicly disclosing breaches and finding themselves in the media spotlight. The press, customers, and partners are beginning to realize that security breaches are inevitable. But at the same time, they are demanding more information—and asking more detailed questions. To prepare, organizations need an effective communication strategy. The best strategies are guided and informed by facts determined from a thorough investigation of the incident.[24]

---

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

[23] 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.

[24] "Threat Report: A View from the Front Lines." *Mandiant*. A Fireeye Company, 2015. Web. 11 Jan. 2016.

> 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. Courts should 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.

Test the plan

Once the plan is in place, **test it at least annually** to ensure all systems across the enterprise are included, and personnel and contact details are still valid. Practicing response procedures on a regular basis will help courts respond more efficiently and effectively, reducing the damage resulting from an actual cyberattack.

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.

> …the US has a patchwork system of federal and state laws, and regulations that can sometimes overlap, dovetail and contradict one another… The proliferation of security breaches in recent years has led to an expansion of this patchwork system of privacy laws, regulations and guidelines which is becoming one of the fastest growing areas of legal regulation.[25]

Cybersecurity is a rapidly changing landscape, and new laws and rulings could impact the court's response plan.

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 cyberattack. Functional and full-scale exercises simulate an actual attack.[26]

Conclusion

Cyberattacks are a reality in today's data-driven world. As threat actors become more sophisticated and attacks are more frequent and more commonly publicized, courts must be prepared to confront incidents in full view of the public. Anticipating risks and

---

[25] Jolly, Ieuan. "Data Protection in United States: Overview." *Practical Law*. Thomson Reuters Legal Solution, 1 July 2015. Web. 28 Jan. 2016.

[26] For more information, see "Exercises." *Ready.gov*. Department of Homeland Security, n.d. Web. 11 Jan. 2016.

preparing to effectively respond can help courts act with greater confidence in the event of a cybersecurity incident. 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.

Appendix: About Cyberattacks

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

Targeted and Opportunistic Attacks

When a hacker attacks broadly hoping to discover vulnerability, the attack is considered "opportunistic." These are the most common kind of attacks. If the attack is focused on a specific individual, organization or industry, it is a "targeted" attack. While both kinds of cyberattacks are disruptive, targeted attacks are more dangerous.

Targeted Attacks

In 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.

> Today, common criminals, organized crime rings, and nation-states leverage sophisticated techniques to launch attacks that are highly targeted and very difficult to detect.[27]

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, or generally wreak havoc.

Cybercriminals may be looking for ways to disrupt automated security measures. In a suspicious incident at Turner Guilford Knight Correctional Center in Miami, Florida in 2013, all of the cell doors at a maximum-security wing opened simultaneously, setting prisoners free.[28]

"Spear-phishing" is a clever and graphic term that describes a targeted attack using email with malicious files attached. Information is the target. "Every

---

[27] *US Cybercrime : Rising Risks, Reduced Readiness: Key Findings from the 2014 US State of Cybercrime Survey*. United States: PricewaterhouseCoopers, 2014. *PwC Cybersecurity and Privacy*. PricewaterhouseCoopers LLP, 2014. Web. 10 Sept. 2015.

[28] Zetter, Kim. "Prison Computer 'Glitch' Blamed for Opening Cell Doors in Maximum-Security Wing." *Wired.com*. Conde Nast Digital, 16 Aug. 2013. Web. 15 Sept. 2015.

organization is at risk of being the target of a spear-phishing attack."[29] 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[30]. Infected emails were sent to employees, who unintentionally downloaded attachments.

Opportunistic 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 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.

In 2013, the Washington State Court system experienced a cyberattack that exposed personally identifying information including 160,000 social security numbers, names, and driver's license numbers for more than a million Washington State residents.[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

---

[29] 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. 18 Sept. 2015.

[30] 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.

[31] Fisher, Dennis. "Washington Court Data Breach Exposes 160K SSNs." *Threatpost*. The Kaspersky Lab Security News Service, 10 May 2013. Web. 15 Sept. 2015.

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 operation, gather sensitive information, or gain unauthorized access. 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. Malware may be used to covertly track an individual’s system or web use, or physical location.

Malware can take many form 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.

“Computer contaminant” may be the term used in state statutes to describe malware.

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[32] 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.

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 ransomware, and if it occurs, to disconnect from the Internet immediately so that data isn’t transmitted and from the internal network so that the ransomware does not spread.

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 in which 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. Software companies regularly release patches, which are modifications made between release cycles. Many software makers include an automated update feature. Ensure systems within your organization are configured to update software regularly.

---

[32] 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.