Beyond Buzzwords: Building an Information Security Foundation

Sajed Naseem Chief Information Security Officer, New Jersey Judiciary
Brian J. McLaughlin Court Executive 2a, New Jersey Judiciary

Cybersecurity is no longer just a buzzword, but a stark reality where an attack can debilitate organizations. This article discusses steps to build an information security foundation for courts, ideally supported by leadership and integrated into every level of the organization.

Cyberattacks are a reality for every public organization, including state courts. During these challenging times, it is critical to update court operations to incorporate information security requirements and to develop a plan to methodically respond to cyberattacks. This article discusses steps a judiciary can take to prioritize information governance and to build a foundation of cybersecurity best practices in every level of the organization.

Culture of Information Security

State courts rely on information technology for processing millions of cases across many docket types. With the increased use of information technology comes an increased security risk to court data and business operations. Recognizing that information security is no longer just an information-technology-office topic, but one that involves all facets of the organization, judiciary leadership should commit to establishing an organizational culture of information security.

Building a foundation for current competencies and continued improvement in information security can be accomplished by adopting and implementing a standard for information governance, managing vital internal and external relationships, and investing in protective infrastructure. Further, it involves bringing together technological units and other court offices through cybersecurity awareness, risk management, and incident response planning.

In laying the groundwork for a culture of information security, courts should explore various issues. The following questions provide a useful starting point:

- *Is judicial and administrative leadership invested in information security?*
- *Is information security more than just a technology topic in the court?*
- *Does the information security unit have autonomy and authority?*
- *Does the court have information security and cybersecurity awareness programs that are coordinated and measurable?*
- *Are all relevant layers of court management and operations involved in the court's cyber-incident-response program?*

…information security is no longer just an information-technology-office topic, but one that involves all facets of the organization, judiciary leadership should commit to establishing an organizational culture of information security.

Information Governance and Court Systems

An optimal information governance process is developed with stakeholders and takes risk, infrastructure, and awareness into account. Gartner (2019) defines information governance as "the specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving and deletion of information." Court systems have the responsibility of managing different categories of information, such as personal identifiers, victim/witness information, financial data, and employee records, just to name a few (McLaughlin, 2018). To govern that information, policies and procedures must be formulated, and court processes (business and technology) reviewed and audited.

For this comprehensive process, court systems should select an information governance standard, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF provides computer security guidance for how organizations can assess and improve their ability to prevent, detect, and respond to cyberattacks. Judiciary policies and procedures should be developed, evaluated, and refined based on the selected information governance standard.


Cyber
Security
Phishing
Access
Danger
Technology
KEY
Lock
Data
Attack
Harm
Virus
Spam
Server
Site
Key
Guard
Service
Safe
Devices
Worm
Trojan
Firewall
Protection
Detection
Password
Malware
Encrypted
Intruder
Hacker
Network
Systems
Spyware
Business
Target
Identity
Unauthorized
Vulnerabilities
Communications
Control
Information
Investigators
Harassment
Steal
Crimes
Code
Server
Stored
Worm
Future
Virus
Lock
Privacy
Cyber
Access
Malware
Password
Technology
Business
Security
Danger
Hacker
Server
Crimes
Spyware
Virus
Network
Future
Protection
Detection
Firewall
Information
Cyber
Control
Key
Server
Infection
Malware
Code
Detection

Managing Relationships

Managing internal and external relationships is essential to building and sustaining a foundation for information security. This task can be challenging because it requires negotiating, compromising, and challenging norms inside and outside of the organization. For information security to be implemented organization-wide and practiced by all employees, it must be incorporated into daily court operations, which necessitates buy-in from internal and external partners. Managing these relationships requires ongoing collaboration with stakeholders.

> *Among the most vital internal relationships necessary to establish a culture of security is that between the court's defined information security unit and the information technology office… these units must operate independently and cooperatively–and on equal footing.*

Internal relationships include those within any central administrative office, as well as all levels of courts (e.g., supreme, appellate, trial, and municipal courts). Among the most vital internal relationships necessary to establish a culture of security is that between the court's defined information security unit and the information technology office. To function appropriately, these units must operate independently and cooperatively—and on equal footing. This means separating the two offices both in the organizational reporting structure and in practice.

Working with judicial and administrative leaders, a chief information security officer can best set the vision for information security that is implemented organization-wide. Under the leadership of the chief information security officer, the information security unit should handle information governance and security, enterprise risk management, and cybersecurity awareness training separate from the development of information technology.

This allows information technology and information security to manage separate yet related areas and to take the same or different positions on critical issues. The two units should have unfiltered voices in the organization and should report to and engage directly with court leadership. Informed by the distinct perspectives of information security and information technology, court leadership can handle day-to-day decisions, as well as an incident or breach, when urgency is vital.

Successful internal relationships support courts' relationships with external stakeholders and users, including prosecuting authorities, public defenders, state agencies, law enforcement, bar members, and any other group that accesses the courts.

> *Cybersecurity awareness is both an internal and external imperative, as courts have many employees and external users.*

These external users interact with the courts through judiciary systems, as well as by email. Through these external relationships, courts can foster open communication to develop and adhere to appropriate memoranda of understanding and rules for professional engagement. Managing both internal and external relationships can position a judiciary to apply its information governance standard to judges, court staff, and other internal users, as well as to intergovernmental partners, attorneys, and others.

Information Security Infrastructure

Risk reduction should be one focus of the information security infrastructure. With the push for courts to enhance operations through new and expanded initiatives in information technology, there is a need to balance technological enhancements with risk reduction. A strong information security infrastructure protects areas of risk. Some key protections include secure authentication, encryption, data loss prevention, network access control, and incident response. Cyber threats are always changing, with many increasingly sophisticated threat actors and near daily news reports on data breaches, ransomware, phishing, and data loss. A strong information security infrastructure starts with a robust foundation of vision, strategy, architecture, process innovation, and deployment of technologies suited for the organization to mitigate these threats. Finally, it is important to measure results to identify areas in need of improvement. This requires engaged support by leadership and throughout many levels of the organization.

Cybersecurity Awareness

To minimize risks and costs, information governance seeks to encourage behaviors in people and institutions that foster an information-centered organizational culture (Brown and Toze, 2017). Cybersecurity awareness is both an internal and external imperative, as courts have many employees and external users. With a large user base, the information governance process should include a persuasive cybersecurity awareness presence, so user behavior aligns with best practices in attack prevention.

> *The goal is to instill in all employees an understanding of the role of information security in their daily work and to reinforce the impact of their daily conduct in this area.*

No defense is complete without a strong cybersecurity awareness program. Court systems should consider various steps to prioritize cybersecurity awareness, such as:

- *annual recognition of Cybersecurity Awareness Month every October to provide classes for all employees on phishing, identity theft, social media, and information governance;*
- *cybersecurity posters on phishing, identity theft, social media, and information governance to serve as an ongoing reminder of these issues;*
- *required cybersecurity training for all employees to ensure continued education and growing familiarity with best practices;*
- *informational cybersecurity cartoons shared with employees to stimulate engagement; and*
- *review of cybersecurity principles and practices as part of employee performance expectations to provide accountability.*

Cybersecurity awareness is critical for developing a vibrant information security culture. The goal is to instill in all employees an understanding of the role of information security in their daily work and to reinforce the impact of their daily conduct in this area. Management guru Peter Drucker once said, "You can't manage what you can't measure" (Wolcott, 2016). Courts may use various methods to measure the levels of employee cybersecurity awareness. These tools could include surveys or quizzes that can help the information security unit tailor relevant trainings to achieve the organization's objectives.

Risk Management: Integration of Court Units and Information Security

Risk management in the use of information technology, and its integration within the court system, requires balancing the benefits of technology with an understanding of the potential vulnerabilities inherent in any non-paper system.

In evaluating and managing information security risks, state courts must consider all internal and external-facing systems. Effective risk management requires court managers, business experts, and the information security unit to collaborate as these areas converge. In risk assessment, court managers and business experts provide the information security unit with insight about their unit's data and operations to enable identification and evaluation of potential threats and vulnerabilities. Assessing these risks provides increased oversight and risk mitigation for information systems. It further enables a court to develop an appropriate plan to manage the identified risks.

Cyber Incident Response

Consistent with a standard of information governance, and in conjunction with establishing a culture of information security, courts should plan for potential cyber incidents. Cyber incidents cover a broad range of activities, ranging from a simple phishing attempt sent to a court employee's e-mail address, all the way to a scenario where a threat actor hacks and takes control of a court's case management system. The Multi-State Information Sharing and Analysis Center (MS-ISAC), within the United States Department of Homeland Security, is a valuable resource for state and local governments. MS-ISAC compiles information on cyberattacks and provides guidance on incident prevention, protection, response, and recovery. An incident response plan should involve many internal court units and may link to the organization's continuity of operations plan or disaster recovery plan. In addition to educating employees to preempt cybersecurity vulnerabilities, court systems should also plan to respond to any cybersecurity attack that could occur.

Summary

State court systems are guardians of sensitive data. The increasing threat of a cyberattack, big or small, amplifies the responsibility of courts to protect this data through all available means. A culture of security recognizes that everyone in the organization—not just information technology and information security—must protect and secure data. Ultimately, managing court records is an enduring core function for any judiciary.

Building the foundation for a strong and evolving information governance process moves beyond buzzwords and slogans to a comprehensive approach that engages every member of the organization. It includes proactive prevention—through internal and external relationships, protective infrastructure, and ongoing cybersecurity awareness—as well as practical steps to identify, mitigate, and respond to vulnerabilities through risk management and incident response planning. With the ever-present threat of cyberattacks, these steps are vital to safeguarding the information entrusted to state courts.

References

Brown, D. C. G., and S. Toze (2017). "Information Governance in Digitized Public Administration." 60 *Canadian Public Administration* 581.

Gartner Research (2019). "IT Glossary—Information Governance." Retrieved from http://tinyurl.com/y342pymo.

McLaughlin, B. J. (2018). "Cybersecurity: Protecting Court Data Assets." In D. W. Smith, C. F. Campbell, and B. P. Kavanaugh (eds.), *Trends in State Courts 2018*. Williamsburg, VA: National Center for State Courts.

Wolcott, R. C. (2016). "Don't Be Tyrannized by Old Metrics." *Harvard Business Review*, September 23. Retrieved from http://tinyurl.com/y46r8o75.