State court systems are guardians of sensitive data for individuals and organizations. To best address the threat of a cyberattack, internal coordination and external collaboration are essential in data governance.

Cybersecurity: Protecting Court Data Assets*

Brian J. McLaughlin, Adjunct Faculty, Department of Public Administration, Villanova University

When it comes to digital data assets, state court systems are not unlike financial institutions, retail companies, health-care providers, and other government organizations. This extraordinary public responsibility makes them a high-value target for cybercriminals. The threat of a cyberattack is not just an IT department problem; it is an organization-wide problem. Over time, the judicial branch has successfully used technological developments to improve the court process. Yet the increasing cyber threats are too significant for courts to address on their own. While there are indispensable technical tools, this article highlights administrative strategies to prevent and respond to cyberattacks. For effective data governance, state court systems must coordinate internally and collaborate externally with the executive and legislative branches.

Defining Cybersecurity

In our hyper-connected world, the technology that we rely on also makes us more vulnerable. State court systems are no exception. The many benefits of technology are accompanied by risks and challenges. Unfortunately, cyberattacks on individuals and organizations continue to rise in frequency and sophistication. The Federal Bureau of Investigation (2017) reported that cyberattacks in the United States caused over $1.3 billion in victim losses during 2016. Generally, cybersecurity involves the protection of computers and information systems from theft, damage, or disruption. More specifically, Craigen, Diakun-Thibault, and Purse (2014) define cybersecurity as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (p. 17).

Cybercriminals seek undetected access to target information systems. Through this invasion, they may perform data exfiltration, which is the unauthorized transfer of data from a computer or device. Cybercriminals may also hold data hostage until a ransom is paid by the host organization. Additionally, they could try to sabotage data integrity and information systems. All three of these acts could catastrophically damage an organization's operations and credibility.

* This article presents the personal views of the author, and does not represent the New Jersey judiciary.

Cyber Threats

The FBI defines a cyber incident as "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" (2017). While data breaches can happen in many ways, this article focuses on the potential for targeted attacks. Four types of cyberattacks are particularly concerning for state courts.

1. **Phishing** uses social engineering to solicit personal information from unsuspecting users to compromise their own systems. Phishing e-mails appear legitimate and manipulate users to enter items, such as usernames or passwords, that can be used to compromise accounts. Spear-phishing, a more personalized method, could target specific judges and court employees.
2. **Ransomware** infects software and locks an organization's access to their data until a ransom is paid. Through phishing e-mails, drive-by downloading, and unpatched software vulnerabilities, cybercriminals attempt to extort users by encrypting their data until certain conditions are met. The result is a temporary or even permanent loss of data.
3. **Advanced persistent threat (APT) attacks** attempt to maintain ongoing, extended access to a network by continually rewriting malicious code and using sophisticated evasion techniques. A successful APT attack results in complete invisible control of systems over a lengthy period time. APTs typically use socially engineered attacks to get a foot in the network door.
4. **Code-injection attacks** involve the submission of incorrect code into a vulnerable computer program without detection. Through these attacks, cybercriminals trick the target system into executing a command or allowing access to unauthorized data. The most common code-injection attack uses Standard Query Language (SQL) through an online application.

It is important to note that all these threats can evolve, while new cyberattack methods can emerge.

Targeting Courts

State court systems are guardians of sensitive data for individuals and organizations. Court records are crucial in the functioning of our society. Preserving these official records is a responsibility long held by judicial-branch administrators. The Judiciary Act of 1789 created the first position of district court clerk to record deeds and judgments of the courts (Sec. 7). Much has changed in the nearly 229 years since. Today, modern court administrators have extensive data-governance responsibility. Data governance includes the people, processes, and technology required to properly handle an organization's data assets. Included under this umbrella are data quality, usability, integrity, security, and preservation. Data governance truly touches all aspects of a court organization.

> *"…there are multiple entry points for data breaches in the judicial branch…judiciary case management systems, networks, servers, cloud storage, software programs, WiFi systems, employee devices, and an array of court-specific technology."*

The landscape of court technology has changed rapidly, as digital tools help facilitate the business process of the court. This proliferation of technology has improved the judiciary's access and transparency, while also significantly increasing data storage and the digital footprint. Consequently, there are multiple entry points for data breaches in the judicial branch. These include judiciary case management systems, networks, servers, cloud storage, software programs, WiFi systems, employee devices, and an array of court-specific technology. No longer is just one desktop PC assigned

to each employee within a court facility. Judges and court staff now use laptops, tablets, and smartphones to conduct court business. These devices are used outside the confines of the courthouse, accessing networks within and across jurisdictional lines.

Though most court records are nonconfidential, there is plenty of information legally shielded from public view. Beyond the damaging consequences of disrupting court operations, cybercriminals can target the trove of sealed and confidential information in judiciary systems. A sample of this data includes:

- personal identifiers, including Social Security numbers and bank account numbers
- victim information in domestic violence and sexual assault cases
- confidential informants and search warrants in criminal cases
- family court files involving children and families
- medical and psychological reports
- testimony within sealed transcripts and recordings
- intellectual property and trade secrets
- jury and grand jury records
- metadata within judiciary documents
- judicial deliberation records
- employee personnel data in HR files
- court financial records

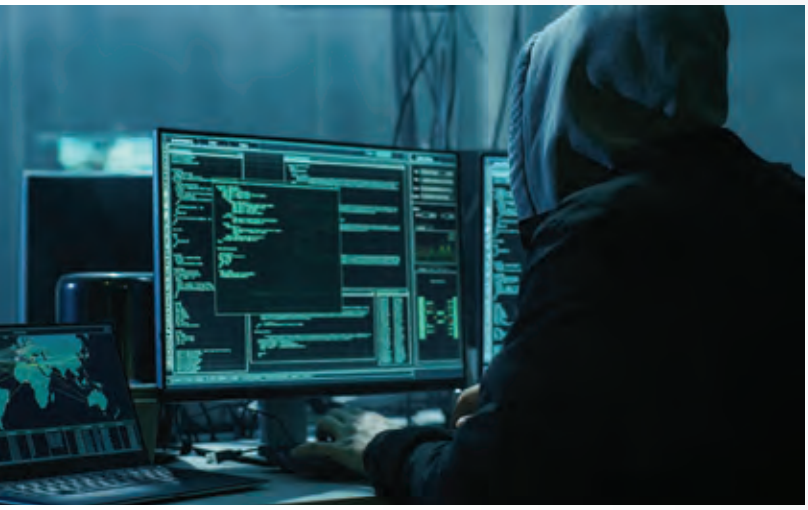
This information is shielded from public view to protect the privacy of litigants, children, witnesses, judges, and employees. Courts are entrusted with these records, and consequently face varying degrees of liability if they fail to keep them secure. Many are negatively impacted by a cyberattack on a court: litigants, witnesses, victims, judges, lawyers, court staff, the organization itself, and the public as a whole.

For example, the Washington State Administrative Office of the Courts public website suffered a data breach in 2013 effectuated through an unpatched vulnerability in Adobe software. Hackers obtained access to approximately 160,000 Social Security numbers, along with the names and driver's license numbers of millions of people. Washington's AOC responded immediately. They collaborated with the state's executive branch, including the Office of Chief Information Officer and Consolidated Technology Services, along with other organizations, to manage the response and improve security measures (Washington State Chief Information Officer, 2013). The AOC communicated with potential victims and explained the attack to the public. They launched a website and hotline to answer questions about the breach. Finally, they undertook significant security enhancements to prevent another breach. Other recent victims of cyberattacks include the Columbiana County Juvenile Court and Kankakee County Circuit Clerk's Office in Ohio, as well as the Minnesota Judicial Branch.

Court data assets are valuable for cybercriminals for several reasons. First, this information could be used for criminal purposes. Second, holding this type of data for ransom can force court officials to pay to restore their access, as Columbiana County and Kankakee County both did in recent years. Third, access to judiciary systems could enable cybercriminals to manipulate court data records, placing the credibility of the judicial process in

"Many are negatively impacted by a cyberattack on a court: litigants, witnesses, victims, judges, lawyers, court staff, the organization itself, and the public as a whole."

peril. Fourth, confidential records could be used as part of legal strategy in a host of docket types. Finally, data breaches can bring court operations to a halt as response measures are executed.



The National Association of State Chief Information Officers (NASCIO) designates security and risk management as the top priority facing state government (2018). Court systems cannot address this complex priority alone. Appropriate for the judicial branch, Agranoff and McGuire (2003) define public-sector collaborative management as "the process of facilitating and operating in multiorganizational arrangements to solve problems that cannot be solved, or solved easily, by single organizations" (p. 4). In addition to critical practices to employ internally, courts require the resources of executive and legislative branches to best address cyber threats. Any collaborative partnership should have clearly established roles and responsibilities for each party.

Preventing Cyberattacks

A multifaceted approach is required to prevent data breaches and begins with a detailed cybersecurity strategic plan. The plan's mission is to develop, implement, and maintain appropriate cybersecurity programs. As a result, the strategic plan helps to limit damage, minimize work stoppage, and aid law enforcement in any investigation. It should be a living document that adapts to new information. In this phase, identifying and understanding digital data assets is a vital step to protecting them. Court officials must be aware of relevant laws, statutes, and standards that guide their recordkeeping process.

Once assets and system vulnerabilities are identified, IT staff can establish layers of protection and monitoring protocols. Regular testing of cyberattack defenses is essential, as is adjusting systems to new threats. As part of the strategic plan, clear cybersecurity metrics should be designated. For example: How are information systems evaluated in real time? The National Institute of Standards and Technology (NIST), within the United States Department of Commerce, provides highly regarded standards, practices, and policies to follow for evaluating cyberattack defenses. Another important question: How often are security systems audited? A cybersecurity audit, often performed by an independent party, is a methodical validation of cyber policies and their accompanying control mechanisms.

State legislatures have a pivotal role in cybersecurity defense. The legislative branch is responsible for regulating information technology practices, passing laws for cybercrime, and providing funding for enhanced security. Keeping pace with cybercriminals requires state courts to be on the cutting edge of security and virus-detection technology. Investing in preventative security measures can save more money than recovering assets and covering losses. Cyber-liability insurance is a fast-growing tool that helps organizations cover the financial burden of cybersecurity incidents. In an era of challenges for public budgeting, courts should carefully tailor their funding requests to provide an appropriate defense. Established communication channels with legislative committees, in addition to executive-branch agencies, are critical to understanding cybersecurity developments.

Judicial and administrative leaders create the culture of cybersecurity within their organization. Communication,

threat awareness, and security education are central to building a robust culture focused on minimizing security risks. People, not systems, are often the weakest link in cybersecurity defenses. Workplace technology policies, regular employee training, and computer-user agreements are key steps to prevent compromising activity. This is particularly important for social-engineering attacks on employees, which directly target individuals.

Responding to Cyberattacks

Even with the best of intentions and diligent preventative measures, data breaches happen. A cyber-incident-response team should be created in the planning process. Immediate, strategic action on the part of the victimized organization is required to minimize damage and expedite recovery. Essential first steps for courts include pinpointing the area of intrusion, minimizing exposure and attack surface, and understanding the scope of the attack. For example: Was just a family-court case management system compromised? Was the breach confined to only certain courts in the state? Data on all attack-related events must be collected and logged, as it will be vital in the attack investigation.

After a breach is discovered, the attack should be reported to at least one law-enforcement agency. Within the federal executive branch, the United States Department of Justice, Department of Homeland Security (DHS), and FBI provide guidelines and best practices for responding to cyberattack incidents. These agencies supply secure forms to report cyber incidents for analysis. The Multi-State Information Sharing and Analysis Center (MS-ISAC), created by DHS, is the key resource for cyber-threat prevention, protection, response, and recovery for state and local governments. MS-ISAC is a voluntary and collaborative effort that serves as a central resource for situational awareness and incident response for state and local governments. Membership is open to all state and local governments at no cost. The Washington State AOC collaborated with MS-ISAC to determine the scope of their 2013 data breach.

"Communication, threat awareness, and security education are central to building a robust culture focused on minimizing security risks. People, not systems, are often the weakest link in cybersecurity defenses."

In addition to data-asset threats, shutting down court systems because of a cyberattack can have massive operational impact on normal court business. In these instances, courts must be able to hold time-sensitive and constitutionally mandated hearings, as well as issue warrants and orders. Courts also have to consider filing access for those parties bound by a filing statute of limitations. When necessary, impacted jurisdictions can issue an order tolling case activity during operational disruption. Sharing timely and accurate information to all impacted by the breach is crucial. Once the type of attack is identified and understood, sharing this information with other court systems is beneficial. Creating a heightened awareness for specific attacks, along with actionable information, provides great value to the court community.

Summary

State court systems have an extraordinary responsibility as the public guardians of sensitive digital data assets. Fortunately, the judicial branch is up to the challenge. The best administration of justice has long required the use of modern management techniques in daily court operations (Tolman, 1960). Safeguarding confidential court records remains essential to protecting the rights and liberties of individuals and organizations. To harness the resources necessary to protect the public's data, the threats posed by cyberattacks must be met with increased internal coordination and collaboration across branches. Through this process, courts can establish a data-governance framework that protects the privacy of all involved in the judicial process.

References

Agranoff, R., and M. McGuire (2003). *Collaborative Public Management: New Strategies for Local Governments.* Washington, DC: Georgetown University Press.

Craigen, D., N. Diakun-Thibault, and R. Purse (2014). "Defining Cybersecurity." *Technology Innovation Management Review*, October, pp. 13-21.

Federal Bureau of Investigation (2018). "Law Enforcement Cyber Incident Reporting: A Unified Message for Local, State, Tribal, and Territorial Law Enforcement." Online at https://tinyurl.com/ycgr8w5v.

Federal Bureau of Investigation Internet Crime Center (2017). 2016 *Internet Crime Report*. Washington, DC: Federal Bureau of Investigation. Online at https://tinyurl.com/ycmbpsaj.

The Judiciary Act of 1789, 1 Stat. 73. Federal Judicial Center, Washington, D.C. Online at https://tinyurl.com/yb87tqhy.

National Association of State Chief Information Officers (2018). "State CIO Top Ten Policy and Technology Priorities for 2018." Lexington, Ky., and Washington, D.C. Online at https://tinyurl.com/y9pjvgjg.

Tolman, L. L. (1960). "Court Administration: Housekeeping for the Judiciary." 328 *Annals of the American Academy of Political and Social Science* 105.

Washington State Chief Information Officers (2013). "Statement from Michael Cockrill, CIO." Press release, Office of the Chief Information Officer. Online at https://tinyurl.com/yc297yme.