ACTIONABLE CYBERSECURITY RISK MANAGEMENT

Sajed Naseem
Chief Information Security Officer, New Jersey Judiciary

Ian Conklin
Court Executive 1B, New Jersey Judiciary

According to the National Institute of Standards and Technology (NIST), risk management is "the process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system."

Within courts, some processes or technologies may be considered "secured" or "hardened," and others may be considered to have risk that is "mitigated" or "acceptable." The ability to distinguish when to secure systems and when to mitigate risks is critical for courts.

Cybersecurity risk management is especially critical during the current global pandemic as many court staff are working remotely, and courts face additional stressors in providing justice remotely.

Cyberattacks have become increasingly common in the public sector, including in courts. Actionable cybersecurity risk management is increasingly relevant to courts due to the nexus between the global pandemic, a remote workforce, and increasing vulnerabilities in technology.

CREATING AN ACTIONABLE CYBERSECURITY RISK MANAGEMENT PROGRAM

State courts rely on information technology for processing millions of cases across many docket types. With an increasing reliance on information technology, there are increased risks to confidential court information and overall risk to court business functions. In a 2020 interview concerning the global pandemic and leadership, former President Obama stated the global pandemic has "torn back the curtain," revealing significant issues with leadership in organizations that showed lack of preparation for such a crisis (Burch, 2020).

The following steps may be important in building an actionable cybersecurity risk management program within a court system.

- Senior judicial and technology leadership should be incorporated into a risk management committee (RMC).
- The risk management program should cover all judicial functions (e.g., appellate, supreme, superior), administrative areas (e.g., business, information technology, or information security), and business partners (e.g., intergovernmental partners or vendors).
- Leadership should communicate the creation of a cybersecurity risk management program courtwide.
- The cybersecurity risk management program must cover all information types (public, administrative, and confidential) in the court's information classification policy.
- The cybersecurity risk management program should incorporate national standards (e.g., NIST Cybersecurity Framework, NIST Risk Management Framework, or Federal Information Processing Standards [FIPS] 199).
- Staff cybersecurity readiness and performance scores must be part of the court's cybersecurity risk management program (see Naseem and Rakoski, 2020).
- Cybersecurity risk management staff should be trained to support the program and provide additional training to stakeholders.

It is important to incorporate security analytics into the risk management program. This may include tracking the number of findings in risk assessments, audited systems, and risk levels. More mature cybersecurity risk management programs may consider measuring changes in people, processes, and technology and mathematically incorporating them into risk assessments.

> *The first principle is that you must not fool yourself—and you are the easiest person to fool.*
>
> - Richard Feynman, Nobel Laureate and Physicist

LEADERSHIP IN REDEFINING CYBERSECURITY

Court leadership must recognize that cybersecurity is not just an information security topic but one that involves all facets of the organization. The court's organizational culture should incorporate measuring the readiness and performance of court staff. Due to the global pandemic, problems with cybersecurity could harm remote court proceedings that could adversely affect health, families, and resources. "Digital" justice is here to stay.

Courts need not only physical but also digital leadership because the release of any confidential information, such as location of an individual, can harm the entire court system. Leadership must incorporate ethics into daily practice to answer critical questions related to best practices, safety, and overall management of court staff.

> *Cybersecurity can no longer be the concern of just the information security department. Within organizations, it needs to be everyone's business.*
>
> - Rothrock, Kaplan, and Van der Oord, 2020

INFORMATION CLASSIFICATION AND HANDLING

The risk management program must cover all information types in the court's information classification policy. Once all information types are covered, processes and technology must be developed to handle different information types. They would likely include the use of encrypting, two-factor authentication, and data loss prevention to confidential systems. It is critical to classify court information. Without proper information classification, it would not be clear what information should be protected, what controls should be used to handle that information, and what training should be provided to cross-functional teams.

INCORPORATION OF NATIONALLY RECOGNIZED STANDARDS

A cybersecurity risk management program should incorporate national standards. National standards, as opposed to internally developed standards, can provide clarity in case of conflict. This will also allow the risk management program to be consistent with vendors, technologies, and intergovernmental partners and allow for consistent contracts—for example, when drafting a memorandum of understanding.

As an example, FIPS 199 defines "moderate" risk as follows: "if the loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals" (see National Institute of Standards and Technology, 2004: 2, emphasis in original). This would be consistent when working with other courts, public institutions, and organizations that use the FIPS 199 standard.

CYBERSECURITY READINESS AND PERFORMANCE AND RISK MANAGEMENT

Humans are fallible. No matter the nature, scope, or extent of an organizational cybersecurity event, invariably at some point, a witting or unwitting action of an individual inside an organization will facilitate a cyber event. Every aspect of securing, defending, and attacking a system has a human element, which profoundly affects all other components and guarantees that there can be no silver bullet in cybersecurity.

Specifically, the reliance of organizational cybersecurity on employees' keen sense of cyber readiness and performance can be defined by three dimensions where organizations provide actionable knowledge to their employees, affect their attitudes toward cybersecurity, and consequently affect a behavioral shift in their cyber interactions. These three dimensions constitute the Knowledge (K), Attitude (A), and Behavior (B), or K-A-B, cyber awareness model (see chart for a sample quantification of K-A-B of employees in different court functions).

CYBERSECURITY READINESS AND PERFORMANCE MODEL USING K-A-B

Dimension	Knowledge (%)	Attitude (%)	Behavior (%)	AWARENESS
Employee #1	19	8	23	**50**
Employee #2	11	15	4	**30**
Employee #3	33	33	15	**81**

APPLYING SECURITY ANALYTICS TO RISK MANAGEMENT

Even with advances in technology, managers need to be aware of what to look for and how to focus their security efforts to get the greatest return. Managers must understand assets, know their people, apply security analytics, and cover the basics.

Using the K-A-B model, it is critical for courts to incorporate cybersecurity readiness and performance scores, as well as vulnerability data (e.g., time needed to mitigate critical, high, medium, and low vulnerabilities), into their risk management programs. As an example, if a team of court staff are working on a project with confidential information within the family division and their cybersecurity readiness and performance scores are below acceptable levels, they may require additional custom training to fill those gaps (such as information classification or cybersecurity training), or a new project team with more experience might be needed to run the project.

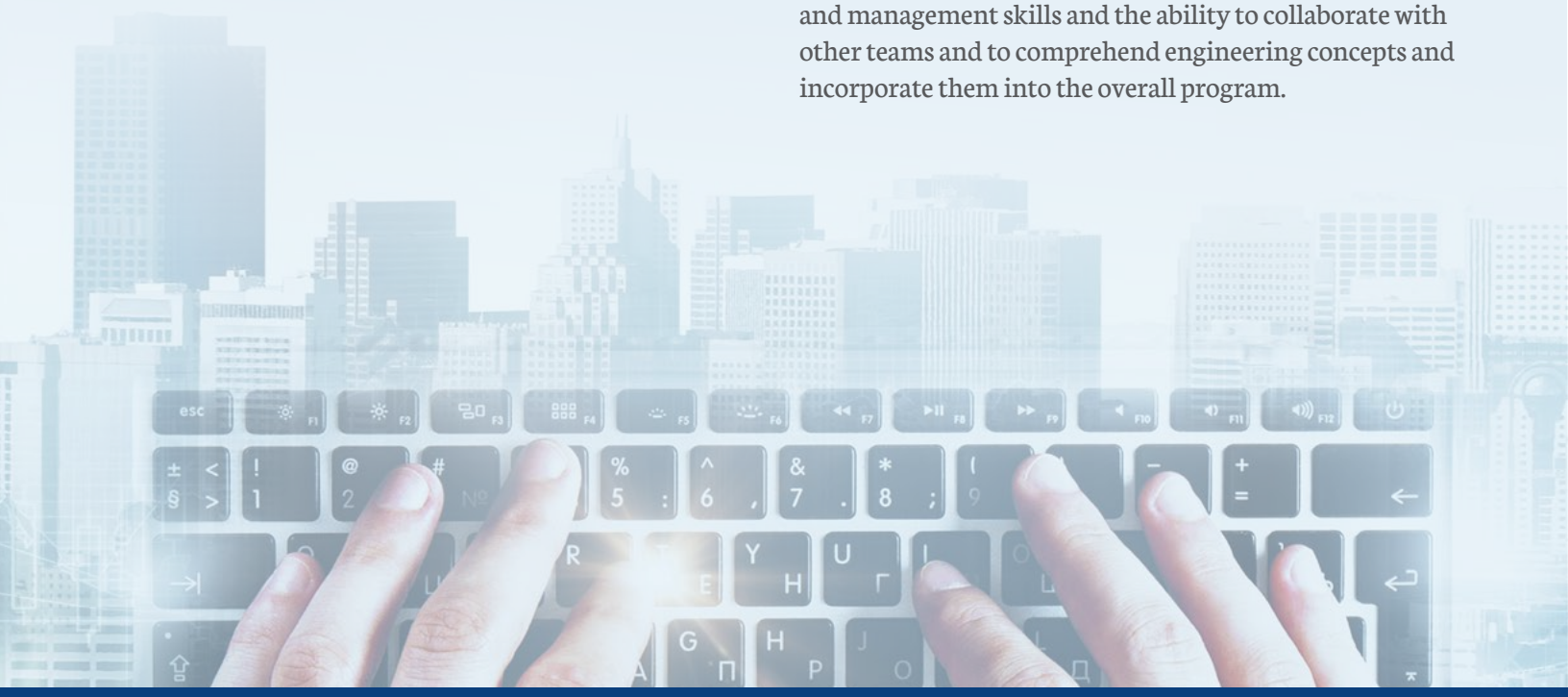
The goal of the cybersecurity risk management program is to protect the court and public from harm by developing the competency of court staff, department processes, and overall information security functions. This could entail mitigating vulnerabilities, incorporating best practices into computer configurations, applying critical software updates on time, and looking for anomalous network behavior, among other activities.

TEAMWORK

Court leadership needs to consider teamwork in building a strong cybersecurity risk management program. This program needs to be housed within the office of the administrative director, operationalized by the chief information security officer. The risk management team should be trained to support the program and provide additional training to cross-functional teams (e.g., judicial, administrative, or technological). Defining the risk management program is the first step; however, teamwork at all levels of the court is what holds the program together.

This leadership can be incorporated into the risk management committee (RMC). The RMC should document regular meetings with cross-functional management teams in judicial, business, and technology divisions to complete risk assessments, get their buy-in, and inform the RMC of changes in risk (such as project being done without a memorandum of understanding, changes to a vendor, or lack of training).

As technology departments adapt toward increasingly agile bimodal processes and refine security and risk governance toward increased agility, switching from a "control" to an "influence" mind set will help avoid enforcing a formal risk appetite at initiation, but provide guidelines at the outset (see McMillian and Scholtz, 2018). This allows for reconciliation of risk requirements during the build and scale-out phases and better conflict resolution, while building better trust among the cross-functional teams. The cybersecurity risk team should have strong leadership and management skills and the ability to collaborate with other teams and to comprehend engineering concepts and incorporate them into the overall program.



CONCLUSION

The pandemic has taught us that leadership is critical for the overall health of court systems. Since March 2020, many court systems have worked diligently to enable court staff to work remotely and hold remote court proceedings through the pandemic. Given the increased reliance on information technology, the cybersecurity risk management program is even more important due to the additional risks to courts—for example, hackers targeting remote employees, COVID-related phishing emails, or social-engineering attacks. A cybersecurity risk management program starts with leadership and requires defining information classification levels, vigilantly following nationally recognized standards, and incorporating cybersecurity readiness and performance and security analytics into the program. Such a program is held together by a trained and accountable risk management team.

Building the foundation of a strong risk management program will allow the courts to reopen normally for the public in the future, while accounting for risks in a measurable way. Courts have a good opportunity to incorporate ethical standards, the K-A-B model, and risk management principles to provide justice digitally and physically.

REFERENCES

Burch, S. (2020). "Obama Says Coronavirus Has 'Torn Back the Curtain' in Poor Leadership." *The Wrap*, May 16. Perma link: https://perma.cc/GE59-K9QJ.

McMillan, R., and T. Scholtz. (2018). "Bimodal IT Is Having an Impact on Security Governance." Report, Gartner Inc., Stamford, Conn.

Naseem, S., and R. L. Rakoski (2020). "The 'Sippy Cup' Program: Redefining Cybersecurity Awareness." *New Jersey Law Journal*, May 28.

National Institute of Standards and Technology (2020). "Risk Management." Information Technology Laboratory, Computer Security Resource Center. Perma link: https://perma.cc/276D-4BFV.

— (2004). "Standards for Security: Categorization of Federal Information and Information Systems." Computer Security Division, February. Perma link: https://perma.cc/CV7F-YYU9.

Rothrock, R. A., J. Kaplan, and F. Van der Oord (2020). "The Board's Role in Managing Cybersecurity Risks." In McKinsey and Company (comp.), *Perspectives on Transforming Cybersecurity*. Orig. pub. *MIT Sloan Management Review*, winter 2018. Perma link: https://perma.cc/PUC6-KSMG.