HOW TO MITIGATE CYBERSECURITY RISKS WHEN YOU DON'T FULLY CONTROL YOUR IT ENVIRONMENT

Paul Embley
Technology Services Director, Court Consulting Services, National Center for State Courts

Many government, court, and court-related offices have experienced cybersecurity incidents in the past year, and the number is projected to increase with the evolution of ransomware as a service and other innovative ways for hackers to work together. A common problem within court-related entities is lack of control over the IT environment. Often, the court is sharing the city or county network, email services, and other aspects of IT. Sharing resources can save money, but it also means a lack of control over cybersecurity detection, prevention, and amelioration. The old adage "trust but validate" is appropriate here in that many courts trust that the IT provider has everything under control, but have no idea how cybersecurity has been implemented.

If a city or county is attacked, there are sometimes no safeguards in place to isolate other agencies they are supporting. These may include county or city health departments, hospitals, transportation providers, and city/county offices and courts. For this reason, courts may not be prioritized when remedies are applied to protect other vital services. And, depending on what agencies experienced the intrusion, the city/county may have multiple fronts on which to try to stop the attack.

The time to assess your court's cybersecurity position within a larger state, county, or municipal IT ecosystem is before an attack occurs. What you don't know CAN hurt you.

There are some primary strategies for addressing cybersecurity risks. These include avoiding the risk through preventative strategies, such as isolating a network, detecting an intrusion through signature-based or behavioral patterns, and reacting to an identified security incident, for example, through isolation of the affected equipment. It is important for courts to know the measures their service provider has put in place for each of these categories.

So, what should court leaders do to protect themselves when relying on another government entity for IT services? Here are a few tips:

CATALOG, CLASSIFY, AND PRIORITIZE

- Ensure the IT staff has a complete inventory of software, applications, and servers that are used by the court. Lack of knowledge about resources can result in an inability to prioritize protection and restoration after a cyber-attack occurs. Failure to inventory can can result in limited or no access to an application that is critical to a user's job. In one court, users were left with no access to important forms and records for probation supervision, for example.
- Assist the IT staff in understanding and classifying data so that they are aware of how secure data resources are. For example, using *public*, *sensitive*, and *secure* classifications of data helps them understand the importance of protection. Often, the IT staff is distanced from business processes and does not realize where sensitive data resides to prioritize protection of it. In coordination with IT, the court's IT governance group should ideally go through a data-categorization process.
- Document the IT group's backup and restoration approach and include the backup location in the IT inventory. Once the priorities of the business applications are established, IT will have a better idea of how critical those are. This allows staff, with the assistance of IT governance, to determine how often data must be backed up, and what amount of data can be lost without harming the business. Most court data will need at least nightly backups. A best cybersecurity practice is to store backups off the primary network. Hackers are increasingly looking specifically for backup files that they can encrypt to cause further damage to restoration efforts. This is particularly true on Windows workstations and servers. An often-missed process is regularly testing the restoration of backup files to ensure they are capturing critical data correctly. Because IT staff are often under-resourced, they may miss this important step.

OPEN UP COMMUNICATION BETWEEN THE COURT AND THE IT PROVIDER

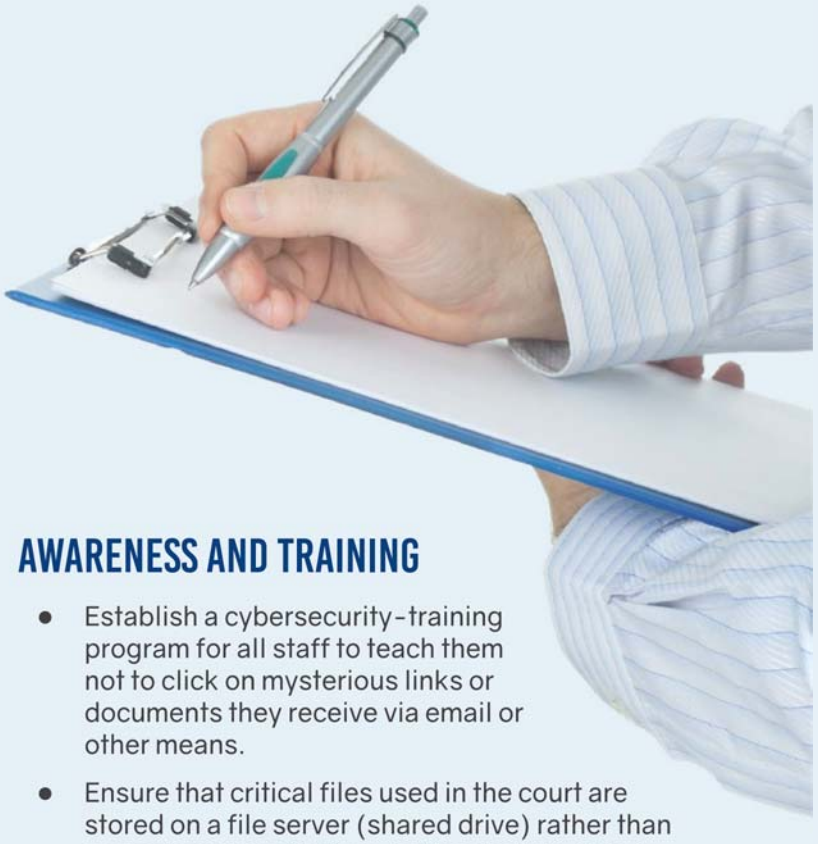
- If there is a lack of communication between the court and the IT provider, court staff may not be aware of where they should establish internal protections or ways to address cyber-attacks. Request that the IT provider establish a governance group so that all agencies can understand what is going on in the IT environment. Include your chief information officer/IT director (CIO) and primary business liaison in these group meetings. As part of this process, agencies can request information about the cybersecurity structure that has been put in place to understand what prevention, detection, or remedies would be present for an intrusion.
- Court staff and provider technical staff sometimes don't speak the same language. It is wise to find the individual in your organization that can bridge that communication gap, even if they are nontechnical. Identify a sponsor who is powerful enough to influence the situation and advocate for the courts. This may be a judge or a chief executive.
- Courts that lack internal technical staff should consider contracting with a vendor to act as the court's liaison to the IT provider. If communication with the provider is difficult, this might be done as part of an initial risk assessment performed by a neutral third-party.

Have an agreement in place that clearly defines the roles of the court's IT staff and the role of the service provider. This agreement can identify priorities and how cybersecurity events will be managed. It is better to have the response planned in advance rather than trying to figure it out in the middle of a cyber-event.

> *While establishing a court-based security program can be daunting, recovering from an incident will undoubtedly be much worse.*

ESTABLISH CONTROLS AND MAINTENANCE PROCEDURES

- Assist your IT staff in evaluating the current environment and establishing the appropriate controls. These may be data or file encryption, a firewall between the court's node of the network and the provider, network segmentation from other agencies, logging tools, or other mechanisms for detecting, protecting or mitigating an intrusion.
- Ensure that all servers and applications that are under the court's control are updated regularly and have up-to-date patching. Older versions of software have vulnerabilities that are well-known to hackers who look for low-hanging fruit that are easy to infiltrate. Patches are updates to software that are often designed to fix a security vulnerability. For those servers not under your control, have a regular report on any outstanding patches.
- If there is in-house software development/ maintenance in place, ensure that developer files are stored within a server-based configuration management tool like Team Foundation Server (TFS) so that their work is not lost in an attack. In one court, all of a developer's application updates were lost and his hard drive was stolen or misplaced during a ransomware attack. Keep in mind, physical security is just as important, if not more important than electronic remedies.
- The court should be on its own network segment. This allows for court specific security requirements to be applied without impacting other organizations in a shared environment. This separation also creates additional barriers to intrusion.
- Use multifactor authentication methods for access to high-value assets. Although having to type in a PIN that is sent upon initiating a login is an additional step and slightly inconvenient, the inconvenience of cyber-event recovery is far worse. It is far more difficult for hackers to circumvent passwords and PINs sent to external devices. Multifactor authentication would likely have prevented the most recent court attacks.



AWARENESS AND TRAINING

- Establish a cybersecurity-training program for all staff to teach them not to click on mysterious links or documents they receive via email or other means.
- Ensure that critical files used in the court are stored on a file server (shared drive) rather than on workstations that are not backed up. This is a difficult sell to end users that need a greater awareness about cybersecurity. Making them understand that workstation files are the most likely to be encrypted in a ransomware attack is an important aspect of an overall cybersecurity awareness program.

You may want to further protect yourself through an IT and cybersecurity audit conducted by a third party, such as NCSC or another certified entity. This provides an objective look into the vulnerabilities and controls that have been put into place in the IT environment. As an independent entity, the auditor can often act as a "go-between" if there are difficulties interacting with the IT provider and can better document and explain the risks and remedies to business leaders.

While establishing a court-based security program can be daunting, recovering from an incident will undoubtedly be much worse. It is worth the effort to understand your cybersecurity position before an attack occurs. Even small, incremental steps forward can make a tremendous difference.

REFERENCES

Chapple, M., J. M. Stewart, and D. Gibson (2018). *ISC² Certified Information Systems Security Professional Official Study Guide*. 8th ed. Indianapolis: Wiley and Sons.

Conrad, E., S. Misenar, and J. Feldman (2017). *11th Hour CISSP*. New York: Elsevier, New York.

Doffman, Z. (2020). "Hackers Attack Microsoft Windows Users: Dangerous Threat Group Exploits COVID-19 Fear." *Forbes*, March 16.

Information Systems Audit and Control Association Certified Information Auditor Review Manual, 12th ed. (2019). Schaumberg, IL: ISACA.

Open Web Application Security Project (2008). *Code Review Guide, V1.1*. Bel Air, MD: OWASP Foundation.

Preston, W. C. (2021). "How to Protect Backups from Ransomware." *Network World*, February 15.