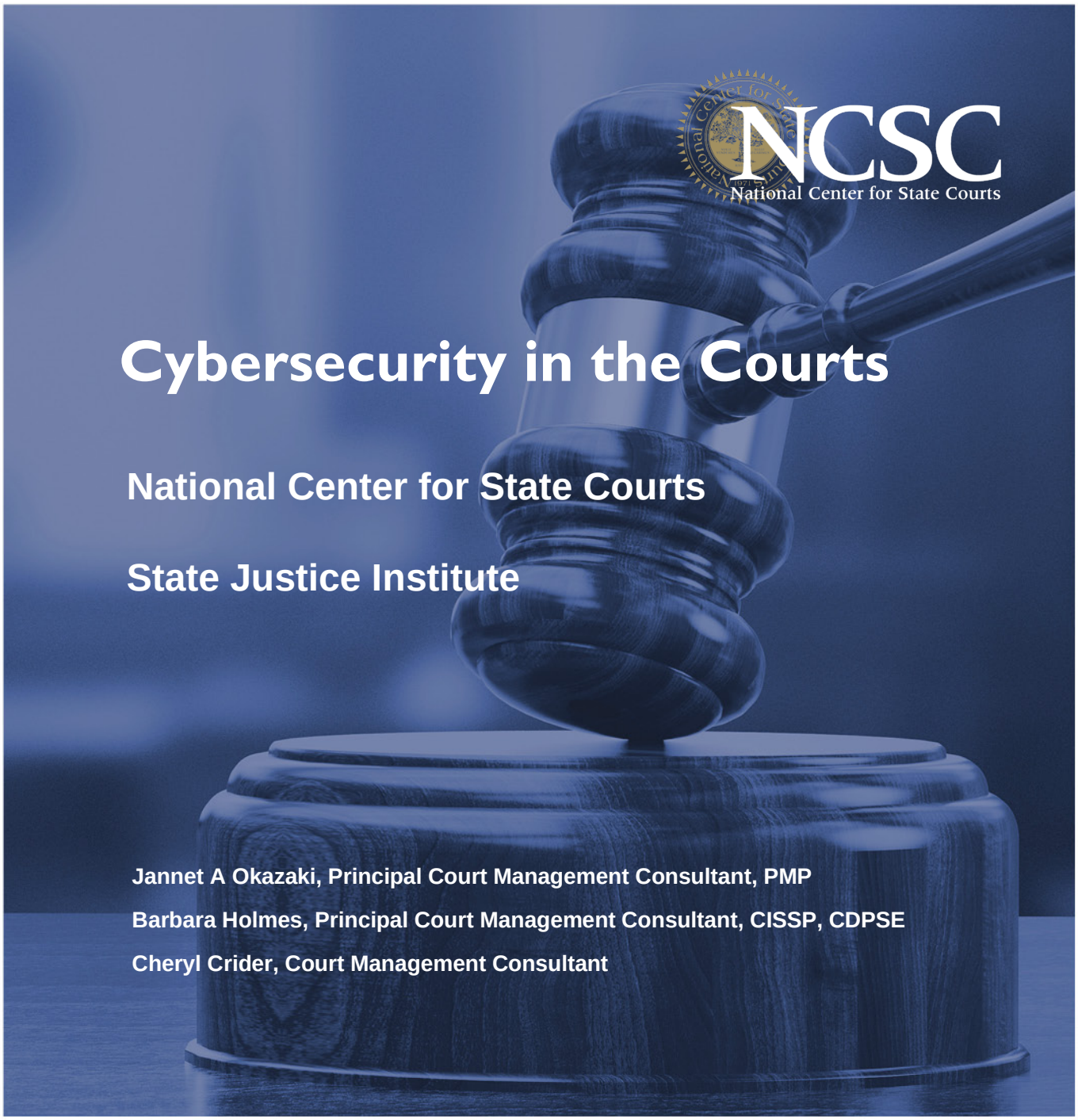


Cybersecurity in the Courts

National Center for State Courts

State Justice Institute

Jannet A Okazaki, Principal Court Management Consultant, PMP

Barbara Holmes, Principal Court Management Consultant, CISSP, CDPSE

Cheryl Crider, Court Management Consultant

DATE

December 30, 2022

PREPARED BY

National Center for State Courts

Court Consulting Services

National Center for State Courts

Court Consulting Services

Mike Buenger, Executive Vice President/COO

300 Newport Avenue

Williamsburg, VA 23185

Phone: (303) 293-3063

Fax: (303) 308-4326

ncsc.org

NCSC

National Center for State Courts

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

This project was funded by a grant from the State Justice Institute. The National Center for State Courts appreciates the participation of courts and subject matter experts. Those participants are not responsible for the views expressed in this report.

INTRODUCTION

Cyberattacks are on the rise and courts have increasingly found themselves to be the target of bad actors. The sensitive information courts manage can make courts particularly vulnerable. Courts and other local and state government agencies are being targeted, not just by ransomware, but also for data theft. Attacks are becoming more sophisticated and often involve many different methods (called attack vectors).

Potential disruption to courts has become such a significant risk that the Conference of Chief Justices and the Conference of State Court Administrators came out with Resolution 2 in Support of Increased Cybersecurity Practices in Court.

NCSC conducted on-site court assessments to identify key areas where the courts are vulnerable and to provide some assistance and guidance to courts on various strategies towards improving their cyber resilience. Select courts received a Cybersecurity Assessment using ratings and categories established by the National Institute of Standards and Technology (NIST). The assessment report rated levels of risk along with recommendations for remediation. These assessments provided some valuable insights and details about the nature of where these courts are struggling to implement important cyber hygiene and cyber resilience measures. These insights may be in common with similarly situated courts.

NCSC also followed up with an updated 2021 Cybersecurity Survey to evaluate against a previous 2017 survey. These results will be compared to determine any shifts in what courts face related to cybersecurity challenges and vulnerabilities.

OBJECTIVES

Protection, integrity and availability of court records and data are the primary objectives of Cybersecurity Risk assessments.

Specific objectives include:

- To assess the state of cybersecurity in the courts
- To provide guidance, policy recommendations, and help set priorities for future cybersecurity initiatives targeting areas that have the greatest need and urgency
- To offer free public publications and nonpublic resources that are directly provided to appropriate organizations and associations
- To educate and provide guidance to courts and court staff with respect to awareness of exposures
- To protect the integrity and availability of court records and services from cyber-attacks
- To provide much needed insight through assessments and analysis

NEED FOR THE PROJECT

There continues to be an increase in the number of cyber-attacks on the judicial branch at all levels from the appellate courts to local municipal courts, with a few high-profile court disruptions in the news. The judicial branch, as the third co-equal branch of government, must protect the integrity of its records and services to preserve the public's trust and confidence. The courts maintain a variety of records important to the public's interest such as those related to property ownership, family records, criminal records that are part of the nation's overall criminal history information, and civil records including those denoting final decisions related to businesses. The judicial branch is an important participant in both receiving and sharing information with other government entities. The information supplied by state courts is used in other processes important to the public's safety and other interests. The decisions and outcomes that are derived from interactions with the courts impact society as all levels.

Cybersecurity has been identified as a top priority by the Joint Technology Committee (JTC) and was also recognized as a top priority in a nationwide poll for education sessions to be featured at the Court Technology Conference (CTC) 2019. There has been a substantial

increase in requests to have education and guidance on cybersecurity

Many courts realize they need to make significant investments towards better securing their data and services, but they need assistance with those efforts. Cybersecurity incidents involve many layers of an organization's technology resources from infrastructure, software, and services to the human element. Understandably, these many layers are complex and challenging to manage. This project gathered critical information to map out the current state of cybersecurity in the state courts. This allows NCSC to provide updated resource publications that reflect the current challenges the court faces along with actionable recommendations to address those challenges.

FOCUS GROUPS

NCSC created a focus group to review the analysis of the 2017 and 2020. The focus group was comprised of individuals who are subject matter experts in areas of cyber security as well as those in specific management roles that govern and manage cyber security within the courts. This focus group discussed key points from the analysis and assisted with identifying court sites that should be considered for more in depth review. Focus group members are those in court technology that specialize in cybersecurity planning, resilience, and response. The group also included decision makers in the executive team such as Court Administrators, court managers, and those involved in continuity of operations planning.

Cyber security strategies and issues can be broad and complex, so the focus group used the initial electronic surveys from 2017 and 2021 to recommend the top priorities and approaches for conducting the in-depth survey for the selected sites. The results of the survey gave some indications of the levels of maturity in different areas of cyber defense, recovery, response, planning, infrastructure, and staffing or available skill sets.

This report outlines the findings and provides recommendations as reviewed by the focus group. The report will be used by NCSC to coordinate with appropriate organizations and associations to assist the courts with improving cyber security readiness and response capabilities. Due to the sensitive nature of cyber security, some aspects of the findings will not be published publicly to avoid disclosing vulnerabilities.

TASKS, METHODS, AND EVALUATIONS

Surveys were used to collect information from a broad number of courts nationally about the state of their cybersecurity technology, policies, and planning. The survey instrument was on-line, and was distributed broadly to members of several associations including the Conference of Chief Justices (CCJ), the Conference of State Court Administrators (COSCA), the National Association of Court Managers (NACM), and the Court Information Technology Officers' Consortium (CITOC). Built upon NCSC's 2017 and 2021 cyber security surveys this project provides a more detailed mapping of the court's cyber readiness and response capabilities through more in-depth assessments. The questions from the 2017 survey were reviewed internally and with select Court CIOs to refine and update the 2021 survey tool. The 2021 survey collected more information and details than the 2017 survey. Due to the pandemic, the 2021 survey received fewer responses. In 2017, there were 138 respondents and in 2021 there were 70 courts responding.

For the on-site assessments, NCSC conducted a kickoff meeting with the selected courts to determine areas of concern, identify information to be collected, and to prepared for the on-site assessment including scheduling interviews with key staff and management. At the on-site assessment, the NCSC team conducted interviews, continued data collection, reviewed secure and non-secure areas within court facilities, and observed common areas and office space. Interviews included court staff, contractors, and other government agency staff especially if there were applications, network, and infrastructure services shared with other government agencies. Other agencies may include the Clerk of Court, City Information Technology, County Information Technology and possibly other court stakeholders depending on level of integration and sharing. General findings, ratings based on the NIST guidelines, and recommendations were provided to the courts in a comprehensive report.

IN-DEPTH CYBER SECURITY ASSESSMENTS

To enhance the high-level cyber security status of the courts from the surveys, a detailed in-depth assessment of a select few court sites was conducted. The in-depth assessment covered a cross section of court types such as centralized/decentralized, varied levels of advancement, and court case volumes. This assessment utilized a combination of remote

interviews and meetings, and a review of critical areas and interviews at the on-site assessment, and a more focused review of the court's self-reported priority areas of focus.

Results of the assessments are generalized in this report to protect the privacy of the participating courts that have agreed to the assessment. Based on the sensitivity of the information gathered and analyzed, NCSC has begun to use knowledge gained from these assessments to develop both public and internal resources in the form of reports, guidance, educational materials, and other assistance to courts.

Areas included in the cybersecurity assessment:

- Infrastructure
  - Redundancy capabilities
  - Network segmentation
  - Physical Security and Environmental Controls
  - Access Controls/Authentication
  - Backup/Recovery
  - Off site and offline capabilities
- Applications
  - On premises applications (local)
  - Online applications and services (Cloud)
  - Web applications and presence
  - Social media
- Administrative
  - Planning and plan maturity
  - Service Providers
  - Government
  - Vendor
  - Contracts/Interlocal Agreements/MOUs
  - Documentation review
  - Staffing/skill sets review
  - Gap analysis

RESULTS

Court On-Site Assessments

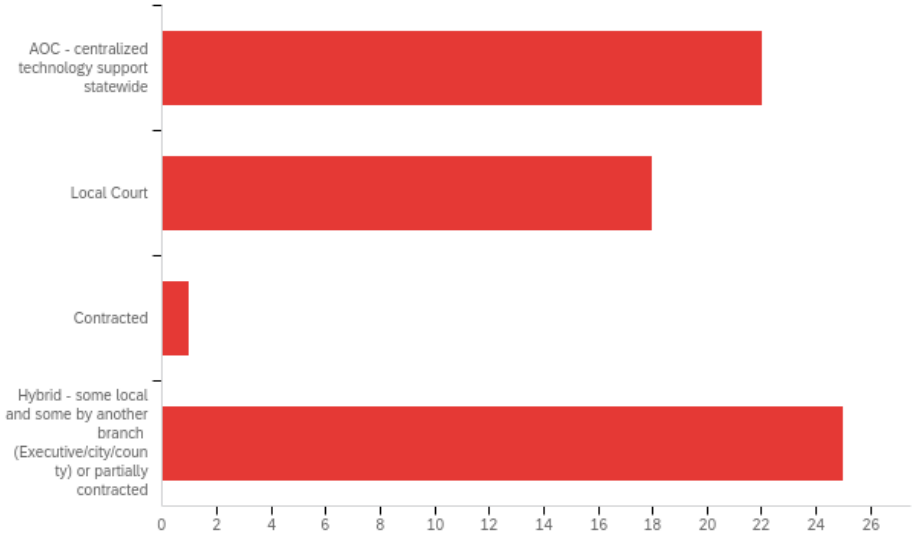
There were many insights gained from the court assessments. The two courts selected were at the local court level (Municipal/County). Both courts had already had issues with cyber-attacks disrupting court operations. Some common challenges these courts faced in maintaining proper cyber protections, response, and recovery include:

1. Courts are provided infrastructure and communication services from another government agency. This may be the executive branch, county, or city information technology provider. There is often no clear definition of roles and responsibilities such as in a Memorandum of Understanding (MOU) or other procedural document or agreement. This often leads to gaps, delays, and lack of understanding of the courts priorities in recovering mission critical systems during a crisis.
2. Technology staffing is not organized with the correct levels of coverage or skill sets to adequately meet the needs of the court. Often the court is reliant on another government agency which may not fully understand the needs of the court or the risks that may exist in the environment.
3. Court staff are not receiving fundamental cybersecurity training to be better operators of the court's technology resources and managers of the court's electronic data.
4. Often courts do not have an acceptable use policy related to technology resources or the policy is out of date.
5. Courts are often not included in the emergency or project planning for technology if it is provided by another government agency.
6. There may be some conflicts of interest related to proper separation of government entities data and work product on shared environments due to lack of clarity in an agreement or other policies.
7. There are disparities in technology response and planning capabilities depending on the level of court. The State level courts have more resources than local courts although this not to say that those resources are adequate.
8. Local courts benefit from sharing network and infrastructure resources with other government agencies so long as proper planning, policies and agreements are in place. There are economies of scale to be gained in sharing resources and skill sets.

Survey Comparisons

NCSC, working with focus group members, updated the most recent survey by adjusting existing questions for clarity and adding questions to go more in depth about cyber resilience status. Although these adjustments were made, there are many valuable areas for comparison between the two surveys.

Who manages your IT? (2021 Survey Only)



Many courts have IT services that is managed by other government agencies or contracted services. Unless there are policies and agreements in place for shared or managed services, there may be a high risk of issues related to cyber resilience and response.

The number of courts that have responded that they have experienced a disruptive cyber incident increased from 18% to 33%. Where data exfiltration occurred, the majority of the time is was another entity such as the FBI who discovered it.

Courts are trending towards not purchasing cyber insurance. Some courts may be covered under a statewide policy managed by the Executive Branch or local city or county. Courts have also expanded their awareness of security benchmarks to measure compliance from focus on CJIS to also include FedRamp, StateRamp, and PCI. About 60% of respondents

to the 2021 survey reported that a Vulnerability and Threat Assessment was completed at least annually.

Between 2017 and 2021 the number of courts that stated that there is someone in their organization responsible for cybersecurity dropped. This may be due to the difficulty in recruiting and retaining this skill set, especially as the pandemic has increased the demand. Many courts still need work on having tools to capture baselines of activity that can be used to measure threat risk, but these tools need the proper staff to manage them and monitor the activity. However, the use of vendor services to work with IT team has increased and cyber resilience tests such a pen testing increased from 31% to 59%.

Courts have improved on having Security Awareness Training for staff, contractors, and stakeholders that use court technology systems and resources. Most courts have this training as mandatory. Courts have the training at least annually, but most courts responded that it was more frequent than once a year. Courts have also improved in having a formal acceptable use policy or guidelines in place with most have a formal employee sign off. Telework policies were included in 59% of the respondents' policies.

When asked about Continuity of Operations Planning, only 41% stated that they had data assets cataloged and classified. Most courts that have a plan responded that IT staff were involved in its development. The number of courts that stated they had a procedure for responding to a cyber security incident dropped slightly. Having a communication plan for cyber incidents is important due to legal requirements, and many courts have the communication plan included in any response plan whether it be a discrete cyber plan or as part of a Continuity of Operations Plan. Surprisingly, many courts do not have a set plan update procedure after testing or if it was used in an incident. Many courts have not completed a catalog of data assets or data classification critical to the prioritization of recovery efforts and determination of recovery and outage tolerance thresholds. Planning for cyber incidents and refinement of incidence response gaps appear to be areas in need of additional assistance for many courts.

Top 3 Concerns

The 2021 survey asked respondents about their top 3 concerns. Of the answers received, these were the top 3 main concerns.

1. Ransomware
2. Phishing
3. Data Leaks/Exfiltration

There were many other serious concerns. These included remote access, business continuity, cloud-based systems, incidence response, disaster recovery, business continuity, insider threats, unauthorized access, issues with outdated infrastructure, access controls, employee vigilance, education, public misinformation, possible manipulation of court records, weak firewall and password strength, social media usage risks on the enterprise network, outside agency access, infiltration of government provided shared network spreading to the court, data management, secure cloud backups, challenges of remote work and more distributed endpoints, compromise and vulnerabilities of the application system(s) (CMS), and zero-day exploits.

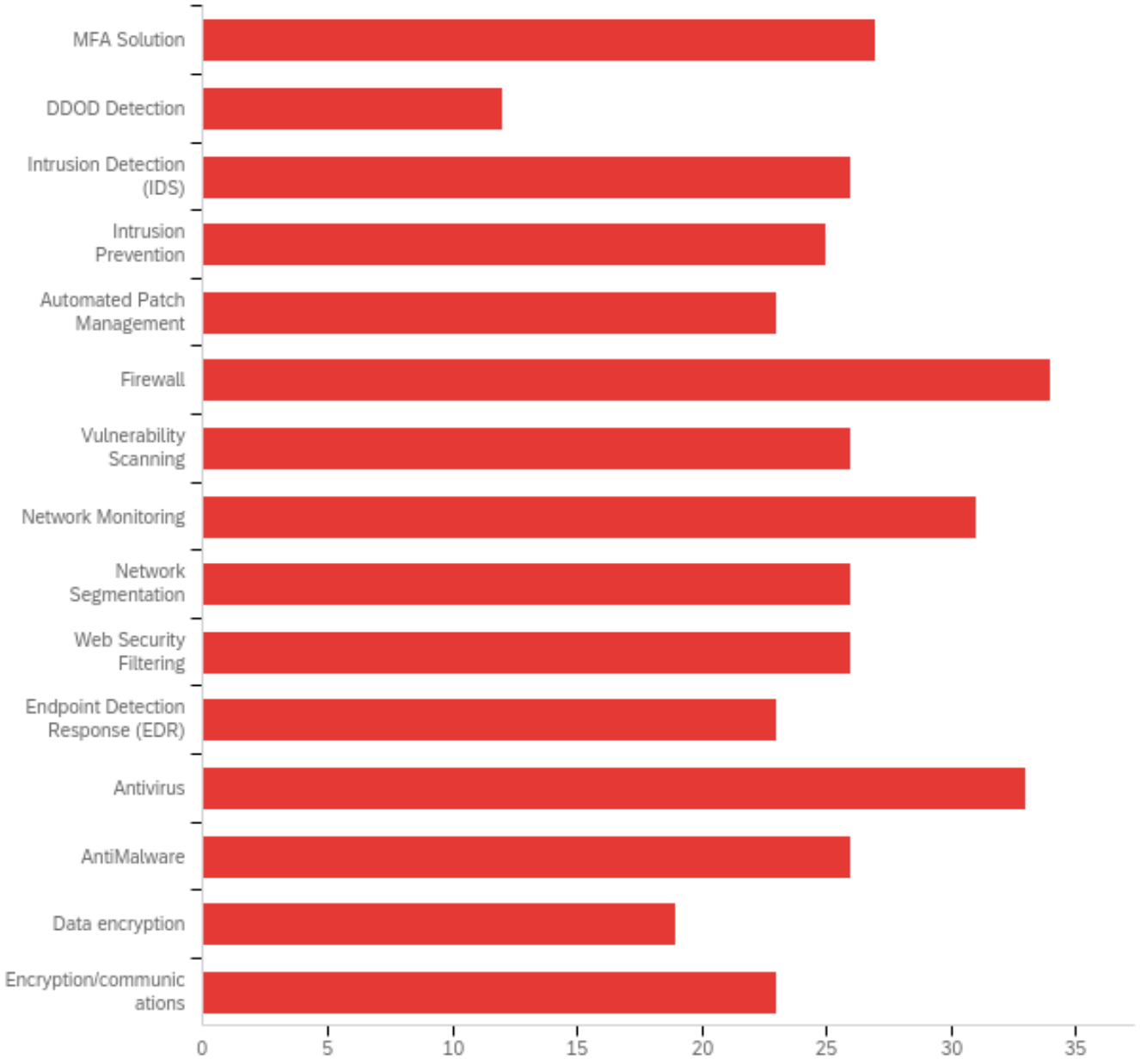
Obstacles to Improving Cybersecurity

The 2021 survey asked respondents to describe the main obstacles to improving cybersecurity. The top responses:

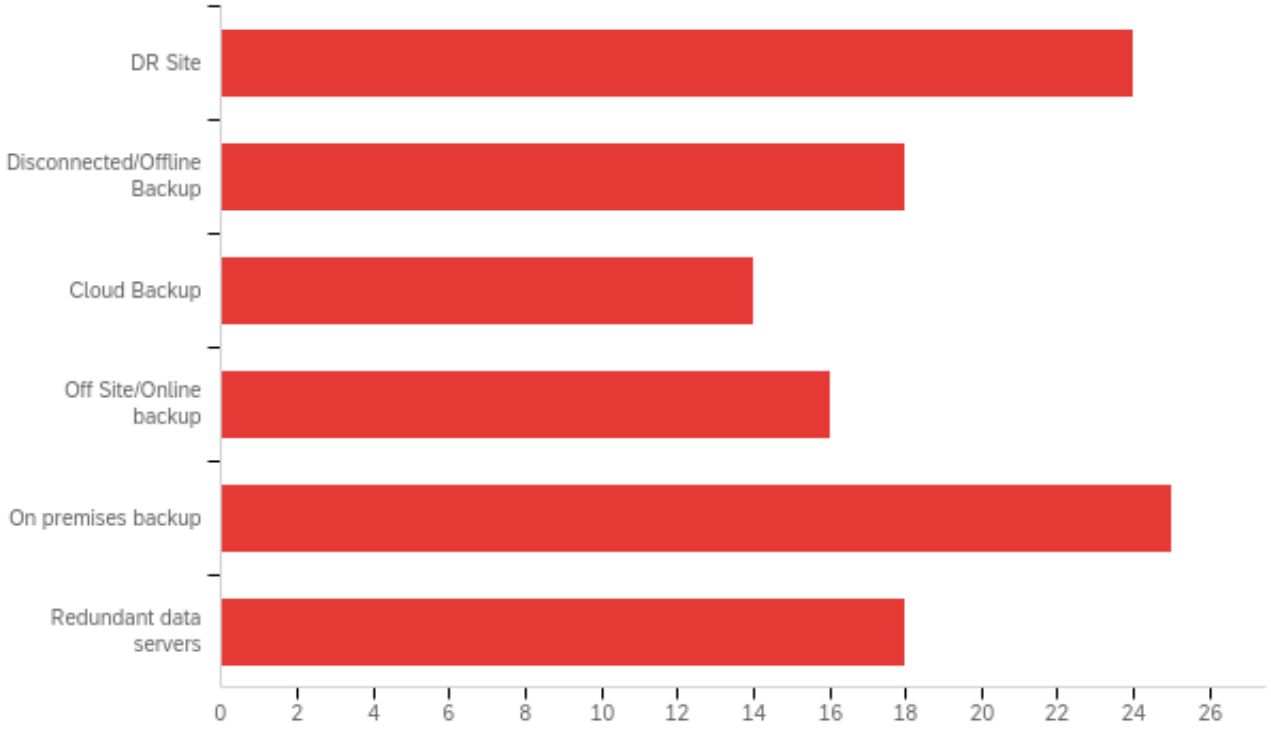
1. Time and Funding
2. Dedicated personnel (cybersecurity)
3. Other government agency is in control and the court does not have a seat at the table. (Governance)
4. Lack of user awareness about good cyber computing habits
5. Lack of policy and planning
6. Gaps in existing technology skill sets and lack of availability of talented human resources.

Some insights regarding the tools and processes used for cyber resilience were collected in the 2021 survey and show some of the methods and levels of effort to protect the courts systems and data.

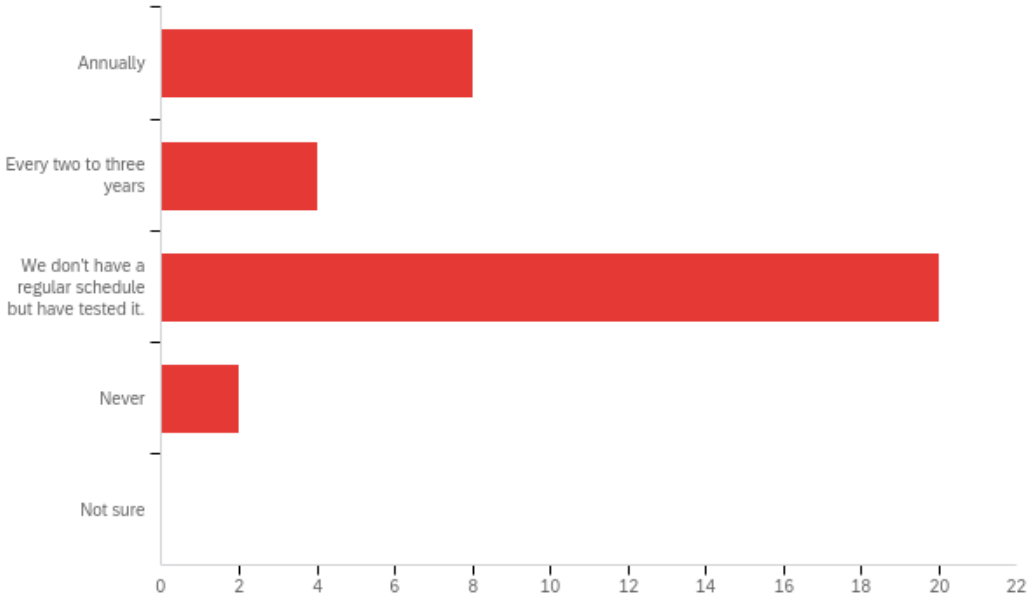
Cybersecurity Tools and Processes (2021 survey only)



Data Backup Processes that respondents use (2021 survey only)



How often do you test backup and recovery of data and systems? (2021 survey only)



DISSEMINATION

Publications and reports are being provided to both the CCJ/COSCA Security Committee and the COSCA/NACM Joint Technology Committee (JTC). Sensitive cybersecurity assessment information will be shared only with the court assessed and detailed insights with the appropriate court associations for purposes of planning future strategies and education planning.

This project report will be posted on the NCSC cyber website and published in the library.

PRODUCTS

The public papers and reports are made available online at no cost. Some reports and information will not be published but will be used internally. Insights from both the public and private information will be used to assist with providing guidance to court organizations and associations about future steps and strategies to improve the court's cyber resilience. Cybersecurity Assessment Reports (To the assessed courts only)

- Cybersecurity in The Courts Report
- Update JTC Paper - Cybersecurity 101
- Actionable Cybersecurity 2020

CONCLUSIONS

The use of the survey instruments and assessments provide valuable information for existing cyber security publications to be updated and provides meaningful insights into the status of a court's cyber security. These insights will help courts to prioritize cybersecurity strategies, develop and improve existing plans, refine policies, and address gaps and trends. Many courts continue to struggle with funding, recruiting needed talent, and setting aside time to implement cyber security training and technology. Often policy and planning development is hampered by the complexity of having another government entity providing some level of technology support such as communications and infrastructure. Courts continue to work on addressing these

challenges with many expressing a willingness to share some level of knowledge with other courts.

After analysis of both the survey and assessments, there are two groups that courts may fall into. These group differ in key characteristics as it relates to the funding resources, governance, infrastructure maturity, and current technology skill sets available.

The first group are courts that are is understaffed and behind on many of the fundamentals such as in areas of planning, testing, staff, and policy development. They will need a general technology assessment to identify starting points for planning and staffing. These courts will need assistance establishing some governance. This will help move the court forward with establishing agreements and policies leading to a better understanding and relationship with service providers (government and private). There is most likely a need for some cybersecurity and data privacy training fundamentals.

The second group are courts that have relatively good staff coverage and skill sets with some planning and policies in place. These courts will need more assistance with refining and testing plans and looking at potential gaps in the recovery process. There would need to be more emphasis on a holistic continuity of operations plan that would also include cybersecurity incidents. These courts may also want to look more closely at areas such as vendor relationships, data exchange vulnerabilities, data recovery times and processes, and improving relationships with strategic partners for continuity of operations planning and recovery.

The NCSC and other court organizations/associations should work with court associations to develop a means for court security, continuity of operations planners, technology security professionals, and policy planners to collaborate, engage, and provide input on future tools, education, and other needs. Technology evolves at a rapid rate as cybersecurity attacks also evolve quickly. Constant vigilance, education, and support will be a constant need to maintain cyber resilience and to protect data privacy. To project the privacy, availability and confidentiality of data is fundamental to maintaining a high level of public trust and confidence in the courts. As a branch of government that provides critical and constitutionally guaranteed services, the court must ensure due diligence to protect its data.