VIRGINIA IT AGENCY

VIRGINIA REPORT ON CYBERSECURITY POLICIES

FISCAL YEAR 2020

vita.virginia.gov

June 11, 2021

Prepared and Published by:

Virginia Information Technologies Agency

Connecting – Protecting – Innovating

Comments on the

Fiscal Year 2020 Commonwealth of Virginia Report on Cybersecurity Policies

are welcome.

Suggestions may be conveyed electronically to
commonwealthsecurity@vita.virginia.gov

Please submit written correspondence to:

Chief Information Officer of the Commonwealth
Virginia Information Technologies Agency
Commonwealth Enterprise Solutions Center
11751 Meadowville Lane
Chester, VA 23836
cio@vita.virginia.gov

FY20 Virginia Report on Cybersecurity Policies

Contents

TABLE OF FIGURES

EXECUTIVE SUMMARY

Report Directive

The Fiscal Year 2020 Commonwealth of Virginia (COV) Comprehensive Cybersecurity Policies Review is the second such report by the chief information officer (CIO) of the Commonwealth. As directed by § 2.2-2009(C) of the Code of Virginia, as amended July 1, 2018, "the CIO shall conduct an annual comprehensive review of cybersecurity policies of every executive branch agency, with a particular focus on any breaches in information technology that occurred in the reviewable year and any steps taken by agencies to strengthen cybersecurity measures. Upon completion of the annual review, the CIO shall issue a report of his findings to the Chairman of the House Committee on Appropriations and the Senate Committee on Finance. Such report shall not contain technical information deemed by the CIO to be security sensitive or information that would expose security vulnerabilities."

The CIO established the Commonwealth Security and Risk Management (CSRM) directorate within the Virginia Information Technologies Agency (VITA) to fulfill his information security duties under §2.2-2009. CSRM is led by the Commonwealth's chief information security officer (CISO). VITA's CIO works with the CISO to address cybersecurity issues in the Commonwealth. Additionally, VITA is responsible for oversight of the Commonwealth's IT infrastructure, including establishing information security programs for the executive branch departments and agencies. VITA also oversees IT investments and acquisitions on behalf of state departments, agencies and institutions of higher learning and establishes IT security policy and standards for the Commonwealth.

Report Objectives

This report will examine the current state of cybersecurity policies in the Commonwealth's executive branch, including policy implementation and use, as well as data breaches that have occurred. The report will utilize information collected from audit reports, assessment documents, and cybersecurity incidents. In addition, this report will analyze data collected directly from agencies in a self-assessment survey where they rated how their agency has developed and implemented cybersecurity policies.

Documented cybersecurity policies are an essential tool in any organization. Cybersecurity policies and procedures provide a roadmap for day-to-day operations and create an internal control framework within an organization. Management uses this internal control framework to rely upon and ensure that the organization meets its objectives.

Having well written cybersecurity policies and procedures helps an agency ensure compliance with laws and regulations, identify and deter cybersecurity threats, respond to cybersecurity incidents, gives guidance for decision-making, and streamlines internal processes. Policies also enable agency management to make consistent cybersecurity based decisions.

Underlying Assumptions

- Improving cybersecurity policy compliance will result in an improved security risk posture for the Commonwealth.

- As agencies implement effective cybersecurity policies and procedures, they will improve security and further compliance with Commonwealth IT security standards, as well as other statutory and contractual mandates.

- Agency Information Security Officers are key to assembling and maintaining a well-managed set of cybersecurity policies.

- As VITA's Shared Centralized Services continue to mature and staffing increases, we expect that participating agencies will have performed an audit and risk assessment on nearly all of their sensitive systems. Timely performance of audits and risk assessments identifies problems that need correcting before they are exploited by cyber threats.

- Commonwealth wide security training and education will help limit the Commonwealth's exposure to increasing cybersecurity threats, but must be ongoing.

Conclusions and Recommendations

- Although Commonwealth agencies are required to develop agency policies and procedures, 21% of all security issues determined from agency audits and risk assessments were due to a lack of policy.

- Agencies often lack staff, resources and funding to devote to policy development and implementation. As a result, we recommend additional funding to address these IT security policy deficiencies.

- The Commonwealth has implemented several risk mitigation strategies to prevent breaches, including implementing vulnerability scanning services, offering audit services, and risk management services.

- In a national survey, Commonwealth agencies reported that the development and implementation of cybersecurity policies is slightly above the average of agencies from other states, but still significantly below optimal.

- End-of-Life (EOL) technology is a risk to the Commonwealth. End-of-life technology is hardware or software that has reached the end of its life cycle and is no longer supported by the manufacturer. There are a significant number of agencies still employing end-of-life hardware or software.

- The human factor is often the weakest link in the security chain. VITA has established a new training standard to improve IT security awareness that will help protect against

potential breaches. The new standard sets a required minimum baseline of knowledge areas that agencies must follow to educate their personnel and to help them identify and prevent potential cyberattacks.

- VITA has developed a quantitative cyber-risk analysis methodology to improve agency IT risk management decisions. Quantification of risk helps agencies focus on systems with the highest risk, allowing them to prioritize risk remediation accordingly.

- Ransomware continues to be a growing threat, particularly for state and local government agencies. In January 2021, VITA delivered a legislative report that evaluated the readiness of the Commonwealth to defend against ransomware attacks and made recommendations to improve its security posture.

- During the last fiscal year, agencies remediated more than 3,800 issues identified through the audits, risk assessments and vulnerability scans that VITA requires. VITA monitors remediation to ensure that issues are corrected in a timely manner and to provide technical assistance where needed.

REPORT

VITA's governance program over cybersecurity was used again this year as a starting point to address the review and reporting requirement of Virginia Code § 2. 2-2009(C). VITA uses laws, policies, standards and processes to help govern cybersecurity across the Commonwealth with particular focus on strategy, budgeting, risk management and incident response.

Commonwealth IT Security Governance Program

VITA has developed and maintained an IT security governance program for the Commonwealth. This program establishes an overall information security policy for the Commonwealth, supported by eight IT security standards. These IT security standards establish a baseline for information security and risk management for agencies across the Commonwealth. These baseline control activities include information security best practices, risk management practices and other specific requirements defined in each of the standards in addition to any statutory or regulatory requirements when applicable.

The Commonwealth IT security standards follow the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 rev. 4, *Recommended Security Controls for Federal Information Systems and Organizations* (https://nvd.nist.gov/800-53/Rev4). This federal government security publication provides a common language to address cybersecurity risk management. By utilizing an internationally recognized IT security standard like NIST SP 800-53, VITA is able to improve communications, awareness and understanding of IT security risks and issues between COV agencies, federal partners, local governments and private sector entities.

The controls in VITA's IT security standards support the development of secure and resilient information systems. These controls are the minimal safeguards that are required of agencies and information systems to maintain the integrity, confidentiality and security of Commonwealth information systems. These controls are categorized into 17 different groups or "families" of IT security controls (Figure 1).

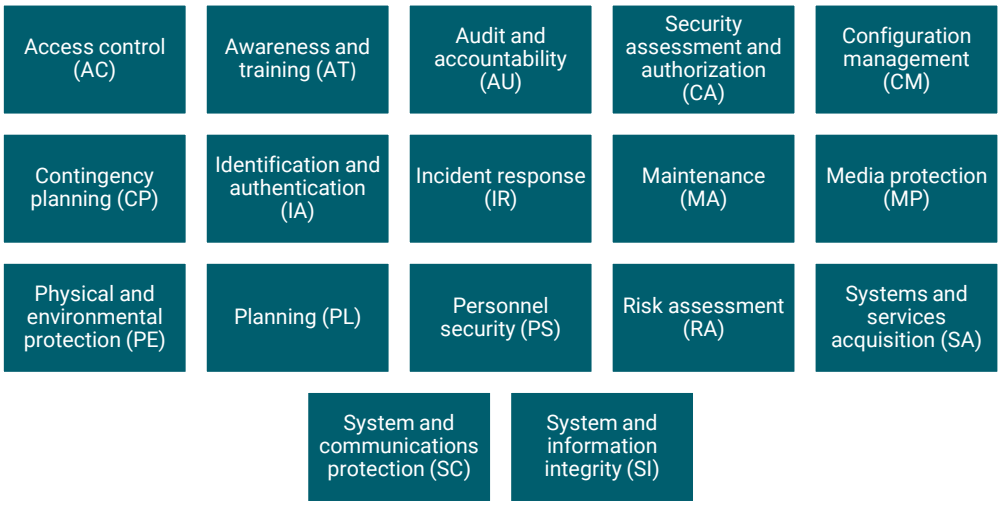


Figure 1: COV IT Security Control Families

Comprehensive Cybersecurity Policies

VITA has established governance requirements including IT security standards for Commonwealth agencies. These standards include the criteria and requirements for comprehensive agency IT security policies. VITA IT security governance requires agencies to develop IT security policies as part of their IT security programs. Policies define the overall requirements to secure agency information, help agencies meet compliance requirements and minimize the risk of data breaches.

The IT security standard that VITA utilizes categorizes IT security controls into 17 different groups or "families" of IT security controls. These security control families address the minimum baseline of management, operational and technical controls necessary to protect Commonwealth data. One of the core baseline controls requires an agency to develop and document policies that are relevant and appropriate to their agency business. Agencies must disseminate policies to agency personnel, contractors and service providers. This ensures IT security is communicated and understood in their organizations.

Compliance with Regulatory Requirements

In addition, security policies are necessary to comply with statutory and contractual security requirements. Commonwealth agencies process and store a lot of information, including personally identifiable information, protected health information, payment card information, and federal tax information. This information is subject to a wide variety of legal and

regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), Internal Revenue Service Publication 1075, Family Education Rights and Privacy Act (FERPA), and Payment Card Industry Data Security Standard (PCI DSS). These regulatory standards typically mandate that agencies develop policies that specifically address compliance with IT security requirements. This reinforces the need to implement security policies because the consequences for non-compliance can be harsh, including the potential for significant financial penalties.

Commonwealth Cybersecurity Risk Mitigation Strategies

Commonwealth Security and Risk Management uses several methods to identify and manage cybersecurity risks in the Commonwealth. These are described below.

Commonwealth of Virginia Information Security Annual Report

Annually, VITA issues a report to the governor on the state of IT security in the Commonwealth (https://www.vita.virginia.gov/Commonwealth-security/annual-reports/). The CIO is required to identify those agencies that have not implemented acceptable policies, procedures and standards to control unauthorized uses, intrusions or other security threats. The annual report is a check on the strengths and weaknesses on agency IT security programs and the overall state of Commonwealth security.

Shared Information Security Officer Services, IT Security Auditing Services and Vulnerability Scanning Programs

Since 2016, VITA has offered a shared services division to improve the IT security posture of agencies in the Commonwealth. The division specializes in providing IT risk management services, IT security auditing services and vulnerability scanning services. Risk assessments, audits, and vulnerability scanning are tools to assure that IT systems and IT security controls implemented by the agency are working as intended. In addition, this helps assure that Commonwealth business and the confidentiality of sensitive data are not adversely impacted.

VITA's shared information security officer (ISO) and IT auditing services are available to any agency that does not have adequate staffing of its own or that may need additional assistance in these areas. There are currently 45 agencies participating in these services. Agencies that participated in VITA's shared ISO and IT auditing services have shown significant improvements in their security scores. Audits of sensitive systems owned by these agencies over a three-year period increased from 52% to nearly 70% from fiscal year (FY) 2018 to FY2020 (Figure 2). In addition, participating agencies saw the number of risk assessments performed on sensitive systems increase from 9% to almost 40% over the same three-year period (Figure 3). However, staffing issues in FY2020 affected the number of audits and risk assessments completed. As these services continue to mature and staffing increases, we expect that participating agencies will have performed an audit and risk assessment on nearly all of their sensitive systems.

Additionally, VITA has created a web application vulnerability scanning services program. Vulnerability scanning is a tool that can provide valuable insight into the possible weaknesses that a hacker might use to exploit Commonwealth websites. VITA regularly scans all public-

facing websites, which results in approximately 6,000 targets scanned annually. Additionally, all agency servers and computers with operating systems are scanned. VITA is in the process of integrating application-level scanning for all sensitive applications.

These shared services provide agencies with the means to identify gaps, prioritize issues and correct problems in security.

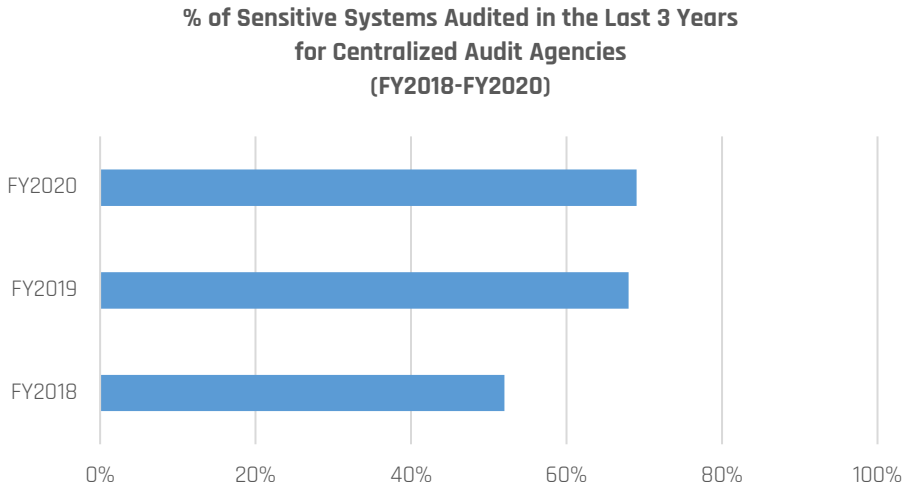


Figure 2: Audits Completed by Shared Audit Services

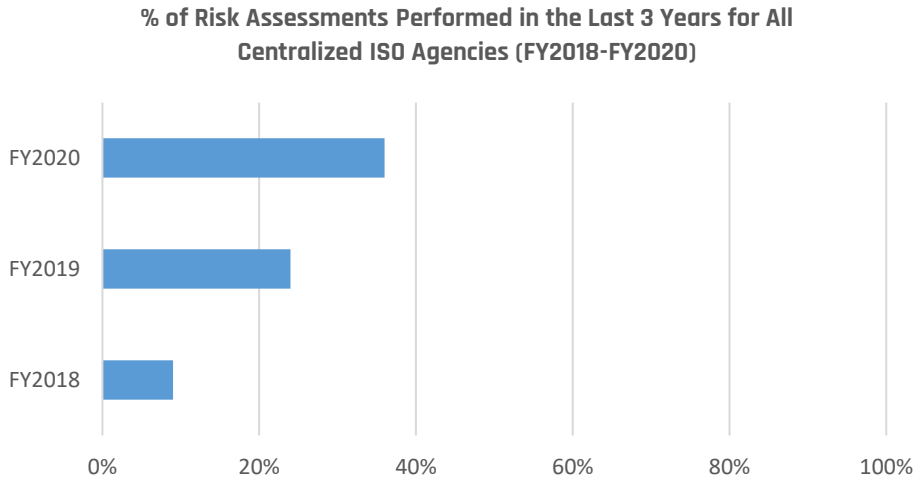


Figure 3: Risk Assessments Performed by Shared ISO Service

Information Security Officer Certification and Training

VITA IT security standards require all executive branch agencies to appoint an ISO to manage the agency's security program. Each appointed ISO must successfully complete IT security-specific training requirements, including the Commonwealth information security orientation that addresses the IT security requirements for Commonwealth information. ISOs are required to obtain 20 hours of continuing IT security education credits each year. In addition, VITA also provides resources on its website, including templates that agencies can use to develop their own policies. According to our recent annual information security report, 95% of executive branch agencies had a certified ISO. Analysis supports that an informed, trained ISO community leads to improved IT security outcomes for the Commonwealth.

Information Technology Acquisitions and Procurement

VITA has goverance oversight for IT acqusition and procurement and uses this authority to promote cybersecurity and make sure security standards have been implemented across the Commonwealth.

As a part of the IT procurement process, agencies are required to provide VITA with requests and justification for large IT projects and IT budgeting. These requests are reviewed by VITA to ensure that the proposed IT project aligns with the Commonwealth's overall IT strategy, policies and standards. Agency IT security programs are reviewed during this process. Agencies that have not implemented the appropriate IT risk management and IT audit compliance programs may be required to address those issues before proceeding with their IT projects or IT budget requests. Agencies presenting VITA with reasonable and achievable plans for correcting their programs before proceeding with future acquisitions helps guarantee that information security investments are appropriately prioritized in the Commonwealth.

Methodology

In order to review cybersecurity policies and perform an analysis of breaches for every executive branch agency, VITA compiled and analyzed information from several sources:

- *Enterprise Governance, Risk and Compliance system (eGRC):* VITA uses the eGRC system to understand how policies, regulations, processes and technologies affect each executive branch agency. This understanding helps VITA to better manage IT security risk and compliance for the Commonwealth. The eGRC also allows VITA to track and monitor agency IT assets and all IT security issues reported, including IT security incidents, IT security audit findings and IT risk assessment findings.

- *Results of the Nationwide Cyber Security Review (NCSR):* The Department of Homeland Security (DHS) and the Multi-State Information Sharing and Analysis Center (MS-ISAC) sponsor the annual NCSR, a self-assessment survey designed to measure gaps and capabilities of participating state and local governments. Commonwealth agencies subject to VITA governance completed the self-assessment. The NCSR evaluates cybersecurity policy and practice maturity. It also provides a tool to compare Commonwealth results with respondents from other states across the country.

- *The 2019 Commonwealth of Virginia Information Security Report:* As required by the Code of Virginia, VITA submits an annual report to the governor and General Assembly on the overall state of IT security in the Commonwealth and at each executive branch agency.

Policy Importance

Commonwealth of Virginia's executive branch agencies are required to establish and implement IT security policies. Security policies address requirements to ensure the confidentiality, integrity and availability of information. Commonwealth policies establish information security requirements for various attributes of security, including access control, incident response, personnel security and physical security. Agencies are responsible for developing, documenting and communicating these policies to all agency personnel and contractors.

There are several benefits to having documented cybersecurity policies. They clearly define the agency's position on security and provide evidence of due diligence, which can be of critical importance in the event of a data breach and/or litigation discovery. In addition, policies help ensure agencies comply with statutory and contractual data requirements that require IT security policies.

Agencies face obstacles in developing IT security policies. The most common challenges include a lack of dedicated resources to develop policies, lack of acceptance by agency management and lack of knowledge of the significance of effective cybersecurity policies. VITA has developed policy templates and other resources that agencies can utilize to overcome these issues.

Information security policies instruct employees and system users about required and/or prohibited actions regarding the preservation of data confidentiality, integrity and availability. Without policy documentation, users may take inconsistent or improper actions or misidentify who is responsible for executing certain functions and activities. Agencies should view their individual policies as the foundation of their security program and a roadmap for governance of security related activities.

When done well, information security governance effectively coordinates the security activities within an agency. It enables the flow of security-related information within an agency and ensures consideration of security-related policy requirements and compliance with those requirements during the decision-making process. Annual policy review and approval ensures each agency is adhering to Commonwealth standards, which in turn guides the governance process.

VITA requires agencies to develop cybersecurity policies with a multi-layered approach. At a minimum, an agency must have a policy for each of the 17 IT security control families referenced in Commonwealth IT security standards. To support the basic control family policies, an agency may also need policies and procedures that support specific areas of the agency's business. The following are examples of additional policies that every agency should consider:

- *Acceptable use policy:* This document stipulates the constraints and practices that a user must agree to for access to the agency's (Commonwealth's) network.
- *Confidential data policy:* This policy identifies how information is classified as "confidential" and how it must be handled and protected.
- *Logical access policy:* Logical access controls are the tools and protocols used for identification, authentication, authorization and accountability in computer information systems. A policy establishes the minimum logical access control measures needed for systems, programs, processes, and information.
- *Personnel policy:* This documents the screening, termination, transfer, sanctions and agreements, for employees and third parties in relation to system access.
- *Mobile device policy:* This policy would apply to any mobile hardware device that could be used to access, to store agency data or to access the agency's network. It defines the minimal mandatory protection requirements that a mobile device should have as well as additional compensating protection.
- *Incident response policy:* This documents the agency's plan for responding to an IT security incident. It lists the steps to take in case of an incident; establishes incident handling and communication requirements; allows the quick recovery of affected systems; determines the cause of the incident; and identifies preventive measures aimed at addressing future incidents.
- *Physical security policy:* This type of policy identifies the appropriate access controls, environmental controls, and protective controls that must be in place in order to protect physical computer systems and information resources from physical harm or unauthorized access and disclosure.

Cybersecurity polices that are easily understood, implemented and enforced can enhance employee and contractor knowledge on how to protect and secure Commonwealth data and systems.

Policy Deficiencies Based on Findings

An agency must review, analyze and implement each control of the Commonwealth's IT security standard in accordance with the sensitivity of the agency's systems and data.

Each control family includes the requirement that agencies establish a policy and procedures for the effective implementation of the IT security controls and control enhancements contained within that particular control family. The policy should also reflect the applicable laws, directives, regulations, policies, standards and guidance that the agency needs to address. Without established cybersecurity policies, an agency would not be able to effectively identify or implement the IT security controls needed to maintain the security of Commonwealth information.

VITA requires all agencies under its governance to submit the results of all IT security audits and IT risk assessments for analysis and monitoring. Software is used to track and categorize any issues identified and to monitor progress toward rectifying the issues. Analysts associate these issues to the specific agency IT system, IT security family and control affected.

VITA analyzed this data in order to review issues associated with cybersecurity policies. Of the 1,507 audit and risk issues reported to VITA in FY2020, 321 issues (21%) specifically identified the lack of, or failure of, policies and procedures as issues to resolve. (Figure 4).

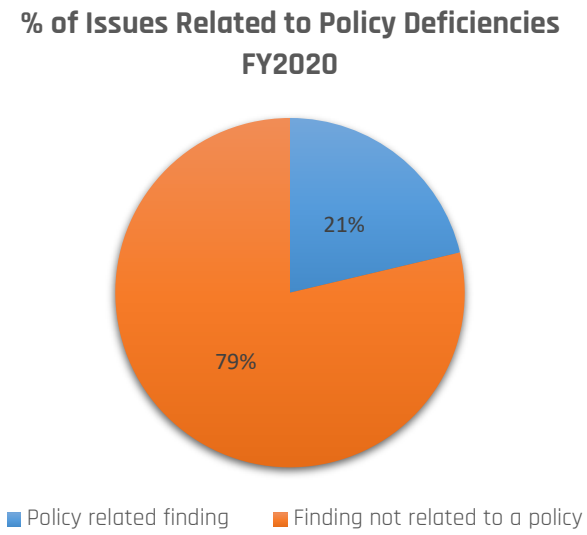


Figure 4: Issues Related to Policy Deficiencies

In addition, an analysis of the IT security control families that had policy deficiencies was performed (Figure 5). The "contingency planning" family had the most policy deficiencies in the fiscal year. The contingency planning control policy is important because it describes the controls necessary to help agencies quickly recover after an unforeseen event. The "access control" family had the second most policy issues noted. Access control is a critical security area that defines the requirements for entering or accessing a system or location, how this access is managed, and under what circumstances access can occur. Agencies are required to continually develop, enhance and implement all required policies to ensure the proper protection of Commonwealth information.

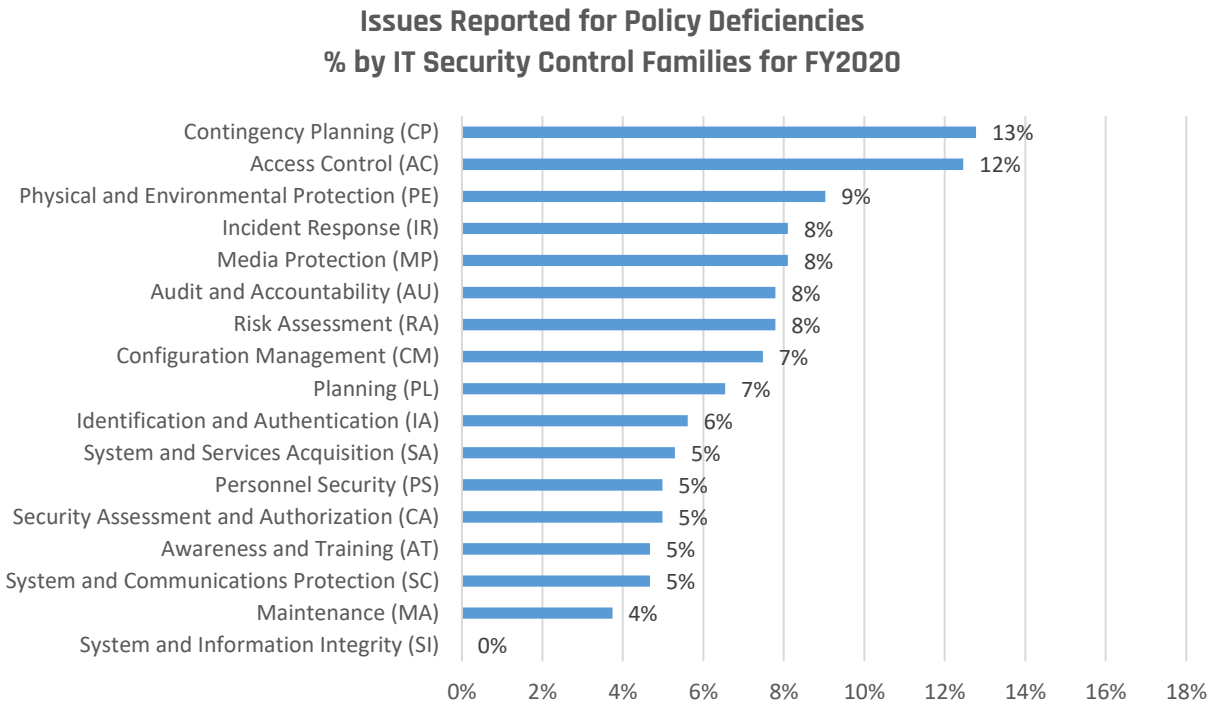


Figure 5: Policy Deficiency Issues by IT Control Family Group

The table below highlights the associated risks related to policy deficiencies listed in Figure 5 (above).

SEC501 Control Family	% Agencies Reporting a Policy Deficiency	Risk
Contingency planning	13%	The lack of a contingency planning policy affects an agency's ability to prepare and respond to unexpected events (e.g. natural disaster, pandemic).
Access control	12%	Most of the security threats and risks to an organization are the result of inadequate and improper access control. A poor access control policy can expose the organization to unauthorized access of data and programs, fraud or the shutdown of computer services
Physical and environmental	9%	A documented physical and environmental policy will afford the appropriate protection to avoid damage or unauthorized access to information and systems.

SEC501 Control Family	% Agencies Reporting a Policy Deficiency	Risk
Incident response	8%	A documented incident response policy is critical for an organization to identify and respond to security incidents and events. An incident response policy provides the overall strategy for defining a breach, the roles and responsibilities of the security team, tools for managing a breach, steps to take to address a security incident, and the notification requirements following a data breach.
Media protection	8%	Media protection requirements establish an effective media protection program to manage data and information risks relating to media access, storage, transport, protection and disposal. Ineffective media protection can result in loss, misuse or exposure of confidential information.
Audit and accountability	8%	Without appropriate audit and accountability logging and review, an attacker's activities can go unnoticed, and evidence of whether or not the attack led to a breach can be inconclusive.
Risk assessment	8%	The lack of an established risk assessment policy can result in an inadequate understanding of exploitable vulnerabilities, the impact on business and the identification of control requirements to ensure continued delivery of sustainable services.
Configuration management	8%	Lack of configuration management can cause serious problems with reliability, uptime and the ability to scale a system. In addition, without a documented configuration management policy the agency will lack an effective methodology for documenting, validating and releasing system changes.
Planning	7%	Without a documented planning policy, the IT organization will be unable to ensure consistent system security and privacy plans/assurance, rules of behavior, security and privacy system architectures and effective baselines.

SEC501 Control Family	% Agencies Reporting a Policy Deficiency	Risk
Identification and authentication	6%	The absence of a formal identification and authentication policy can prevent the organization from properly identifying and authenticating users and granting access to devices in compliance with IT security requirements.
System and services acquisition	5%	A well-documented system and services acquisition policy contributes to the correct allocation of IT resources and effective management of the system development life cycle. It also assists with acquiring systems that satisfy security and privacy requirements and meets established regulations.
Personnel security	5%	Studies have shown that employees and insider threats are the biggest risk to an organization. An effective personnel policy establishes controls on the hiring, training and termination of all personnel.
Security assessment and authorization	5%	The security assessment and authorization policy allows an organization to approve and manage the exchange of information between systems and develop plans to remediate assessment weaknesses or deficiencies. Without this policy, it is difficult to ensure that only properly secured and authorized systems are placed into operation.
Awareness and training	5%	A documented policy for awareness and training can help minimize a substantial portion of security events brought about by untrained (or improperly trained) users. The policy should be aligned with IT and security programs and overall business risks.
System and communications protection	5%	Without a system and communications protection policy, management may lack the ability to communicate clearly and effectively to employees. This can result in a lack of visibility to strategic goals and objectives, poor execution on strategic visions, tactical delivery failures and misrepresented management intentions.

SEC501 Control Family	% Agencies Reporting a Policy Deficiency	Risk
Maintenance	4%	The absence of a maintenance policy impedes the ability of an organization to complete the necessary maintenance, diagnostic and repair activities to preserve the confidentiality, integrity and availability of information systems.
System and information integrity	0%	A system and information integrity policy will provide requirements that are critical to protecting IT systems, including providing protection from internal and external threats to data and/or information systems.

Figure 6: Policy Risks

Operational Risk Indicators

VITA monitors risk indicators or issues that could operationally jeopardize the security of the agency or the Commonwealth. The most common, and one of the most serious issues of this type, is when an agency is using hardware or software that is no longer supported by the manufacturer because it has reached end of life (EOL). Often, the hardware or software supporting an end-of-life or "legacy" application cannot be updated to protect against newly discovered security threats. This is because the application will not function correctly on newer supported systems. Hardware or software that cannot be updated to operate securely poses a greater risk of being exploited and attacked.

An agency may request approval to deviate from updating the end-of-life software or hardware if there is a specific business need by submitting an exception request to the CISO. The requesting agency must fully document the business need, mitigating safeguards and residual risks.

- Three agencies resolved all of the outstanding EOL issues from FY19 during FY20 (DEQ, DGS and VDEM).
- Three agencies resolved some of their FY19 EOL issues during FY20 (VDH, VEC and VSP).
- Four agencies added additional EOL issues in FY20 and did not resolve any EOL issues from FY19 (DARS, DWR, DOE and VDOT).
- Fourteen agencies did not resolve any EOL issues in FY20 from the previous year (noted with an asterisk below).

The chart below compares unresolved EOL issues from FY19 to FY20 for affected agencies.

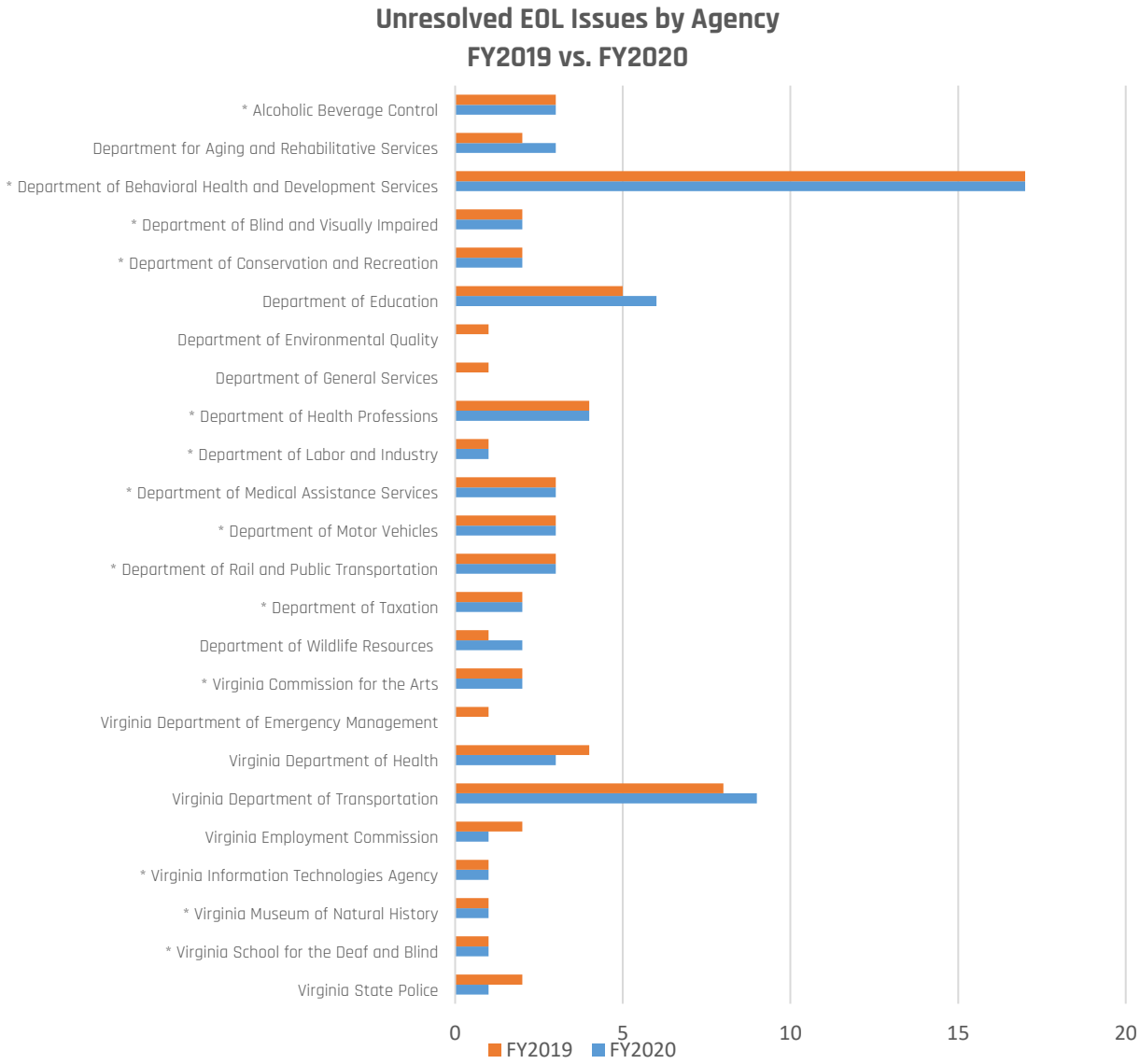


Figure 7: Unresolved EOL by Agency FY2019 compared to FY2020

Nationwide CyberSecurity Review Analysis

Annually, the Commonwealth participates in the Nationwide Cybersecurity Review (NCSR).This is a self-assessment survey aligned within the NIST cybersecurity framework (CSF) to evaluate an agency's cybersecurity posture. Each agency participating in the survey ranks their performance on a maturity scale for five core cybersecurity functions: *identify, protect, detect, respond and recover*.

Identify: The activities measured for this function are key for an agency's understanding of their internal culture, infrastructure and risk tolerance.

Supporting categories:

Asset management: The data, personnel, devices, systems and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

Business environment: The organization's mission, objectives, stakeholders and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities and risk management decisions.

Governance: The policies, procedures and processes to manage and monitor the organization's regulatory, legal, risk, environmental and operational requirements are understood and inform the management of cybersecurity risk.

Risk assessment: The organization understands the cybersecurity risk to organizational operations (including mission, functions, image or reputation), organizational assets and individuals.

Risk management strategy: The organization's priorities, constraints, risk tolerances and assumptions are established and used to support operational risk decisions.

Protect: The activities under the protect function pertain to different methods and activities that reduce the likelihood of cybersecurity events from happening and ensure that the appropriate controls are in place to deliver critical services.

Supporting categories:

Access control: Access to assets and associated facilities is limited to authorized users, processes or devices, and to authorized activities and transactions.

Awareness and training: The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures and agreements.

Data security: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity and availability of information.

Information protection processes and procedures: Security policies (that address purpose, scope, roles, responsibilities, management commitment and coordination among organizational entities), processes and procedures are maintained and used to manage protection of information systems and assets.

Maintenance: Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

Protective technology: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures and agreements.

Detect: The quicker an agency is able to detect a cybersecurity incident, the better positioned it is to be able to remediate the problem and reduce the consequences of the event. Activities found within the detect function pertain to an organization's ability to identify incidents.

Supporting categories:
Anomalies and events: Anomalous activity is detected in a timely manner and the potential impact of events is understood.

Security continuous monitoring: The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

Detection processes: Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

Respond: An agency's ability to quickly and appropriately respond to an incident plays a large role in reducing the incident's consequences. As such, the activities within the respond function examine how an agency plans, analyzes, communicates, mitigates and improves its response capabilities.

Supporting categories:-
Response planning: Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.

Communications: Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

Analysis: Analysis is conducted to ensure adequate response and support recovery activities.

Mitigation: Activities are performed to prevent expansion of an event, mitigate its effects and eradicate the incident.

Improvements: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Recover: Activities within the recover function pertain to an agency's ability to return to its baseline after an incident has occurred. Such controls are focused not only on activities to recover from the incident, but also on many of the components dedicated to managing response plans throughout their life cycle.

Supporting categories:

Recovery planning: Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

Improvements: Recovery planning and processes are improved by incorporating lessons learned into future activities.

Communications: Restoration activities are coordinated with internal and external parties, such as coordinating centers, internet service providers, owners of attacking systems, victims, other Commonwealth security incident response teams (CSIRTs) and vendors.

Using a maturity scale measurement, each agency evaluates itself on several activities that support each core function. The scale goes from one (activity is not performed) to seven (activity is optimized). NCSR recommends a minimum maturity level score of five.

Level one: ***Not performed***. Activities, processes and technologies are not in place.

Level two: ***Informally performed***. Activities and processes may be substantially performed, but they are not documented and/or not formally approved by management.

Level three: ***Documented policy***. The agency has a formal policy in place.

Level four: ***Partially documented standards and procedures***. The agency has a formal policy and has begun the process of developing standards and procedures to support the policy.

Level five: ***Implementation in process***. The agency has formally documented policies, standards and procedures and is in the process of implementation.

Level six: ***Tested and verified***. The agency has formally documented policies, standards and procedures. Implementation has been tested and verified.

Level seven: ***Optimized***. The agency has formally documented policies, standards and procedures. Implementation has been tested, verified and reviewed regularly to ensure continued effectiveness.

On average, Commonwealth agencies that participated in the NCSR, rank themselves very close to the recommended minimum maturity level score in the five core cybersecurity functions. Commonwealth agency scores are also slightly above the scores of other state agencies and territories that participated in the survey (Figure 8).

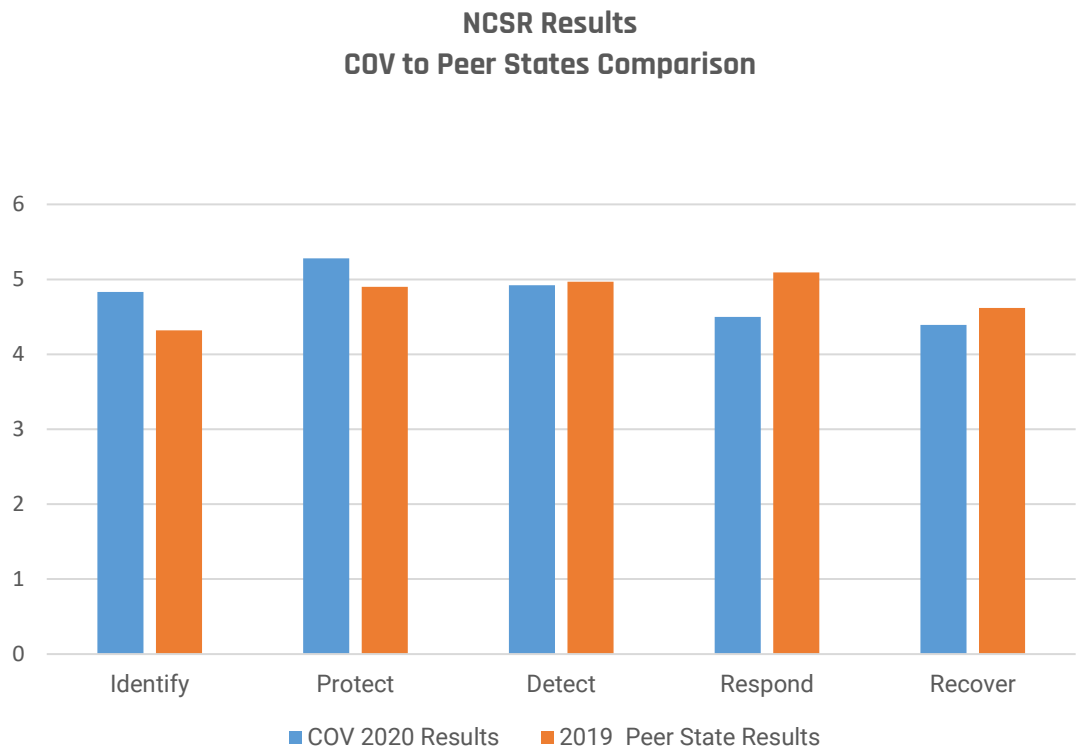


Figure 8: COV to Peer State Comparison of NCSR Results

Nationwide CyberSecurity Review Policy-Related Questions

The NCSR survey requires that each agency evaluate itself as it relates to over 100 questions in various IT security areas. Several policy-specific activities that support the core cybersecurity functions were analyzed to determine if the self-assessments identified any particular strengths or weaknesses.

Agencies rated themselves in the NCSR as to the maturity of their *organizational cybersecurity policies*. An organizational cybersecurity policy is a key component in assuring that an agency's cybersecurity culture, infrastructure and risk tolerance has been documented and understood by its employees and contractors. Almost half of the agencies indicated in their self-assessments that their organizational cybersecurity policy was either "optimized" (22%) or "tested and verified" (23%) (Figure 9). In last year's survey, agencies generally rated themselves slightly higher than they did this year. No agency completing the survey indicated that this control was "Not performed."

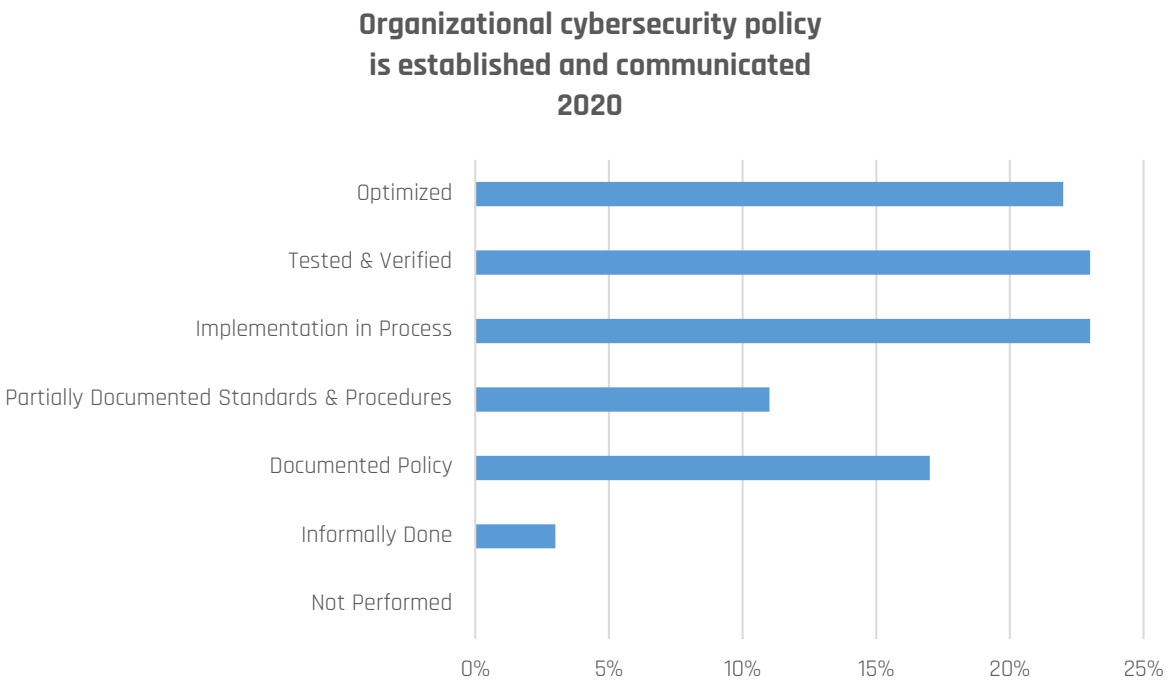


Figure 9: NCSR Results for Organizational Cybersecurity Policy

Managing legal and regulatory requirements is important to assure that agencies are complying with all federal and state laws as well as other requirements. Overall, agencies scored themselves as performing very well in this area: 20% of the agencies considered themselves "optimized" and an additional 22% believe this area has been "tested and verified" (Figure 10).

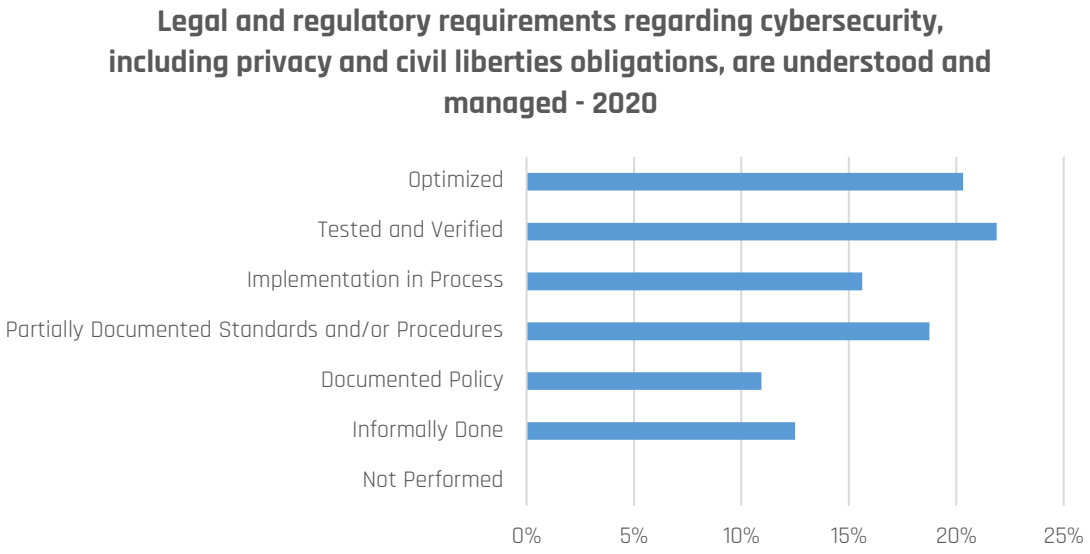


Figure 10: NCSR Results for Legal & Regulatory Requirement Policies

Policies for governance and risk management processes address cybersecurity risks so that any potential issues or gaps in performance are promptly identified and corrected. Overall, agencies scored themselves as performing well in this area (17% optimized and 23% tested and verified). In addition, 27% indicate that these processes are currently being implemented (Figure 11).

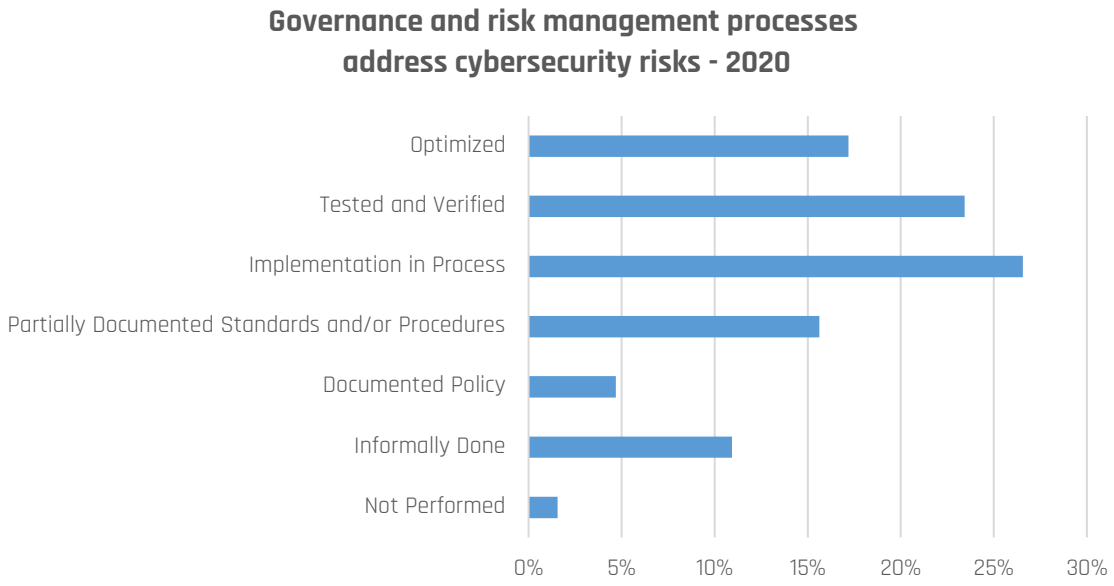


Figure 11: NCSR Results for Governance and Risk Management Processes

Agencies were also asked to score themselves on how well they are complying with policies and regulations related to their physical operating environment. Maintaining adequate control over the physical operating environment provides assurance that organizational IT assets are protected and secured. For this analysis, we looked at agencies that utilize the COV data center managed by VITA (executive branch agencies) and agencies that manage their own data centers (independent and higher education agencies) (Figure 12).

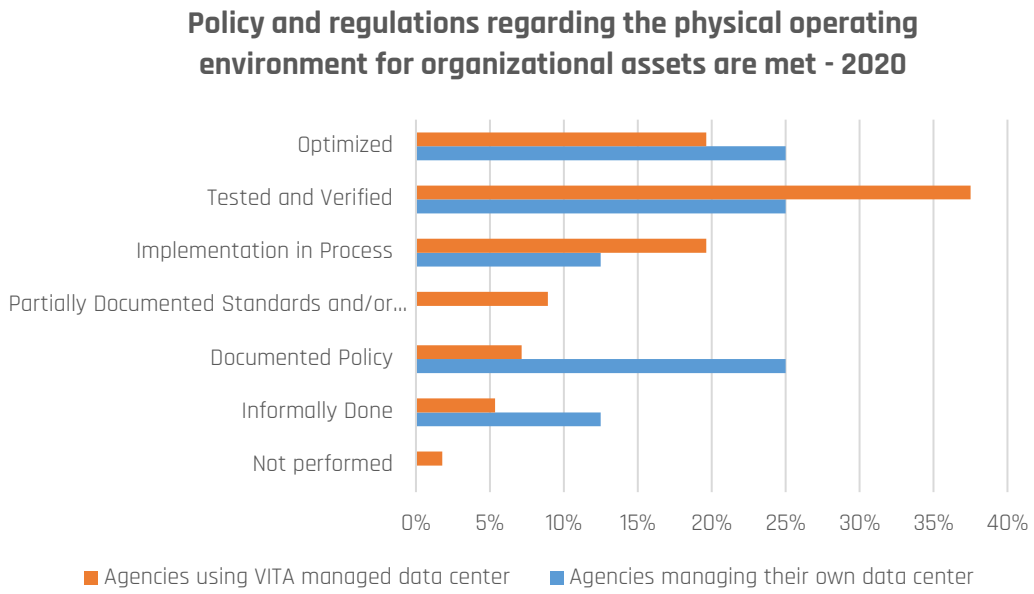


Figure 12: NCSR Results for Physical Operating Environment Policies

Policy Gap Analysis

The NCSR survey leveraged 108 sub-categories organized into the five functions of the cybersecurity framework: *Identify; Protect; Detect; Respond; and Recover*. Most agencies self-reported on the survey that they have at least a "documented policy" for most of the supporting sub-categories. However, for 25 of the 108 sub-categories, over 25% of the agencies taking the survey, reported that the activity was either "not performed" or "informally done" -- meaning that the agency had no "documented policy" in place.

Not having a documented policy means that employees and contractors at an agency do not have a clear statement of the rules, guidelines and regulations. It also means that the agency is functioning at one of the lowest (least mature) levels for the sub-category requirement. The lack of a documented policy has critical implications for cybersecurity and can lead to or exacerbate situations that cause a breach or discloses confidential data.

The table below identifies the sub-categories where at least 25% of the agencies participating in the NCSR survey reported that they ***do not have a documented policy***" in place.

NCSR Cybersecurity Framework CORE CATEGORY	NCSR Sub-Category	% of Surveyed Agencies Without a Documented Policy	Cybersecurity Framework Control Gap
IDENTIFY	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	29%	Policy should require that a criticality analysis is performed for each categorized IT resource and the findings be documented.
IDENTIFY	Organizational risk tolerance is determined and clearly expressed	26%	Risk tolerance is determined as part of the organizational risk management strategy to ensure consistency across the organization. Organizations also determine what levels of risk (combination of likelihood and impact) indicate that no further analysis of any risk factors are needed.
IDENTIFY	Risk responses are identified and prioritized	25%	In the risk prioritization step, the overall set of identified risk events, their impact assessments, and their probabilities of occurrences are "processed" to derive a most-to-least-critical rank-order of identified risks. A major purpose of prioritizing risks is to form a basis for allocating resources.
DETECT	Unauthorized mobile code is detected	32%	Policies and procedures should be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code. Unauthorized mobile code can be used to read and write files and to run and attach programs, providing a high risk for the

NCSR Cybersecurity Framework CORE CATEGORY	NCSR Sub-Category	% of Surveyed Agencies Without a Documented Policy	Cybersecurity Framework Control Gap
			distribution of malicious code.
DETECT	External service provider activity is monitored to detect potential cybersecurity events	25%	Third party employee access to confidential data must be tracked actively based on the principle of least privilege.
PROTECT	Effectiveness of protection technologies is shared	26%	Results of annual security tests should be shared with appropriate stakeholders. External stakeholders must be approved by the agency executive management prior to report distribution.
RESPOND	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	37%	Information sharing can help prevent future incidents and foster improved security analysis. The exchange of information can improve critical infrastructure operations and could help vendors make stronger products and services. It can help build knowledge of long-term trends, giving network defenders a better understanding of emerging cyber threats and shifts in exploitation methods.
RESPOND	Coordination with stakeholders occurs consistent with response plans	31%	A large cybersecurity incident will impact numerous stakeholders both inside and outside of the agency. In addition to the need to engage IT and information security personnel to recover from the incident and forensic personnel to investigate it, the agency may have to involve its executive leadership, legal counsel, communications

NCSR Cybersecurity Framework CORE CATEGORY	NCSR Sub-Category	% of Surveyed Agencies Without a Documented Policy	Cybersecurity Framework Control Gap
			personnel and other stakeholders in the course of its incident response efforts.
RESPOND	Forensics are performed	29%	The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.
RESPOND	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e. g. internal testing, security bulletins or security researchers)	28%	A vulnerability disclosure policy facilitates an agency's awareness of otherwise unknown vulnerabilities. It commits the agency to authorize good faith security research and respond to vulnerability reports.
RESPOND	Response plans incorporate lessons learned	28%	One significant activity that can improve cyber incident response and enable the timely mitigation of threats is the transfer of knowledge after an incident as part of a formalized "lessons learned" phase of the incident response life cycle. Integrating successful processes and procedures from previously successful incident response activities can play a critical role in determining whether a business will suffer in terms of operational integrity, reputation and legal liability.

NCSR Cybersecurity Framework CORE CATEGORY	NCSR Sub-Category	% of Surveyed Agencies Without a Documented Policy	Cybersecurity Framework Control Gap
RESPOND	Response strategies are updated	28%	Never let a good incident go to waste. There are two positive benefits from an incident: The first is that an incident often clearly illustrates both needs and impacts; an incident is often the best time to get additional investment to prevent the next one.
RESPOND	Incidents are contained	28%	Incident activity that is not properly contained and handled can escalate into a bigger problem that can ultimately lead to more damage. A security incident is analogous to a forest fire. Once an incident and its sources are detected, action must be taken to contain the damage.
RESPOND	Incidents are mitigated	28%	Preparing for possible incidents is one of the most important steps in impact mitigation as it allows the incident response team to be able to respond quickly and effectively in case of an incident. Once an incident has been detected, an effective and prompt response is critical for mitigating the impact of a breach.
RESPOND	Information is shared consistent with response plans	26%	The incident response plan should include steps for escalating incidents to the executive response team, which determines the appropriate stakeholders and when to communicate the details of the incident.

NCSR Cybersecurity Framework CORE CATEGORY	NCSR Sub-Category	% of Surveyed Agencies Without a Documented Policy	Cybersecurity Framework Control Gap
RESPOND	Newly identified vulnerabilities are mitigated or documented as accepted risks	26%	The existence of a vulnerability does not always mean that it must be remediated. The organization may choose to accept the risk. All accepted risks should be documented and be approved to prevent them from being reassessed in the future.
RESPOND	Incidents are categorized consistent with response plans	25%	Security incidents should be categorized according to the potential for restricted data exposure, the criticality of a resource, scope and the potential for persistence using a High-Medium-Low designation. The goal is to provide a framework to ensure that potential computer security incidents are managed in an effective and consistent manner.
RESPOND	Personnel know their roles and order of operations when a response is needed	25%	When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate individuals so that all who need to be involved will play their roles. Incident response policies should include provisions concerning incident reporting—at a minimum, what must be reported to whom and at what times. Secondly, every incident helps the agency learn more about its processes and its organization; how systems interact but more importantly, how people interact.

NCSR Cybersecurity Framework CORE CATEGORY	NCSR Sub-Category	% of Surveyed Agencies Without a Documented Policy	Cybersecurity Framework Control Gap
RECOVER	Reputation is repaired after an incident	34%	An incident response policy must also document the steps that the executive team must take to repair reputational damage and communicate with external stakeholders.
RECOVER	Recovery plans incorporate lessons learned	31%	Security incidents should include a "lessons learned" meeting after an incident response.
RECOVER	Recovery strategies are updated	31%	The information security steering committee should review the agency's recovery strategies annually and recommend any necessary changes for improvement.
RECOVER	Recovery plan is executed during or after a cybersecurity incident	29%	Agency must assure that the document recovery plan is utilized during IT security events that require a formal response.
RECOVER	Public relations are managed	28%	Public relations is an important component of an incident response policy. Assign someone representing executives at the agency to oversee external communications and official messaging during an IT security incident.
RESPOND	The impact of the incident is understood	28%	In order to be able to perform impact analysis of an incident at a point in time, historical snapshots of the environment must be captured and available for incident response teams.

NCSR Cybersecurity Framework CORE CATEGORY	NCSR Sub-Category	% of Surveyed Agencies Without a Documented Policy	Cybersecurity Framework Control Gap
RECOVER	Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	25%	The agency's information security officer must continually report to agency executives throughout the response and recovery process.

Figure 13: NIST Cybersecurity Framework Policy Gaps

VITA will work with the agencies reporting poor performance in the above elements of the cybersecurity framework to ensure that these areas are being addressed through documented policies and procedures.

In general, the self-reported results on the NCSR roughly align with the IT security risk ranking that VITA is tracking for each agency. The 25 agencies that gave themselves the top overall scores on the NCSR survey were compared with the report card results of VITA's most recent COV cybersecurity report (https://www.vita.virginia.gov/Commonwealth-security/annual-reports/).

Agency	FY2020 NCSR Self-Assessment Score (highest to lowest)	COV 2020 Annual Cybersecurity Report Card Score (average of Risk and Audit Scores)
Department of Historic Resources	100. 0	87. 5
Virginia Museum of Fine Arts	100. 0	71. 0
Virginia Workers Compensation Commission	98. 9	89. 0
Virginia Retirement System	97. 0	87. 5
Office of State Inspector General	95. 6	88. 8
Virginia Department of Agriculture and Consumer Services	95. 0	93. 8
Department of Motor Vehicles	92. 5	85. 9
Office for Children's Services	91. 9	93. 4
Virginia Information Technologies Agency	91. 5	91. 6
Department of Accounts	91. 9	82. 4
Library of Virginia	91. 0	81. 9
Department of Small Business and Supplier Diversity	89. 6	100. 0
Department of Treasury	89. 9	72. 1
Department of Human Resource Management	85. 7	97. 5
Department of Aviation	84. 7	95. 2
Department of Health Professions	84. 7	100. 0

Agency	FY2020 NCSR Self-Assessment Score (highest to lowest)	COV 2020 Annual Cybersecurity Report Card Score (average of Risk and Audit Scores)
Department of Behavioral Health and Development Services	82. 3	45. 8
Department of Housing and Community Development	83. 1	73. 5
Department of Conservation and Recreation	82. 4	77. 3
Department of Corrections	80. 4	83. 0
Department of Labor and Industry	77. 6	83. 4
Department of Wildlife Resources	78. 8	71. 0
Virginia Museum of Natural History	77. 4	100. 0
Marine Resources Commission	75. 8	93. 8
Virginia Racing Commission	78. 0	91. 5

Figure 14: NCSR Results compared to COV Annual Report Card Score

Additionally, the average self-reported NCSR score by Commonwealth agencies, per secretariat, was compared with the average score reported by similar groupings on the NCSR by peer states. In some instances, Commonwealth secretariat assignments were re-aligned in order to align with the NCSR's peer state group reporting. In general, the Commonwealth secretariats score higher than similar peer state groupings.

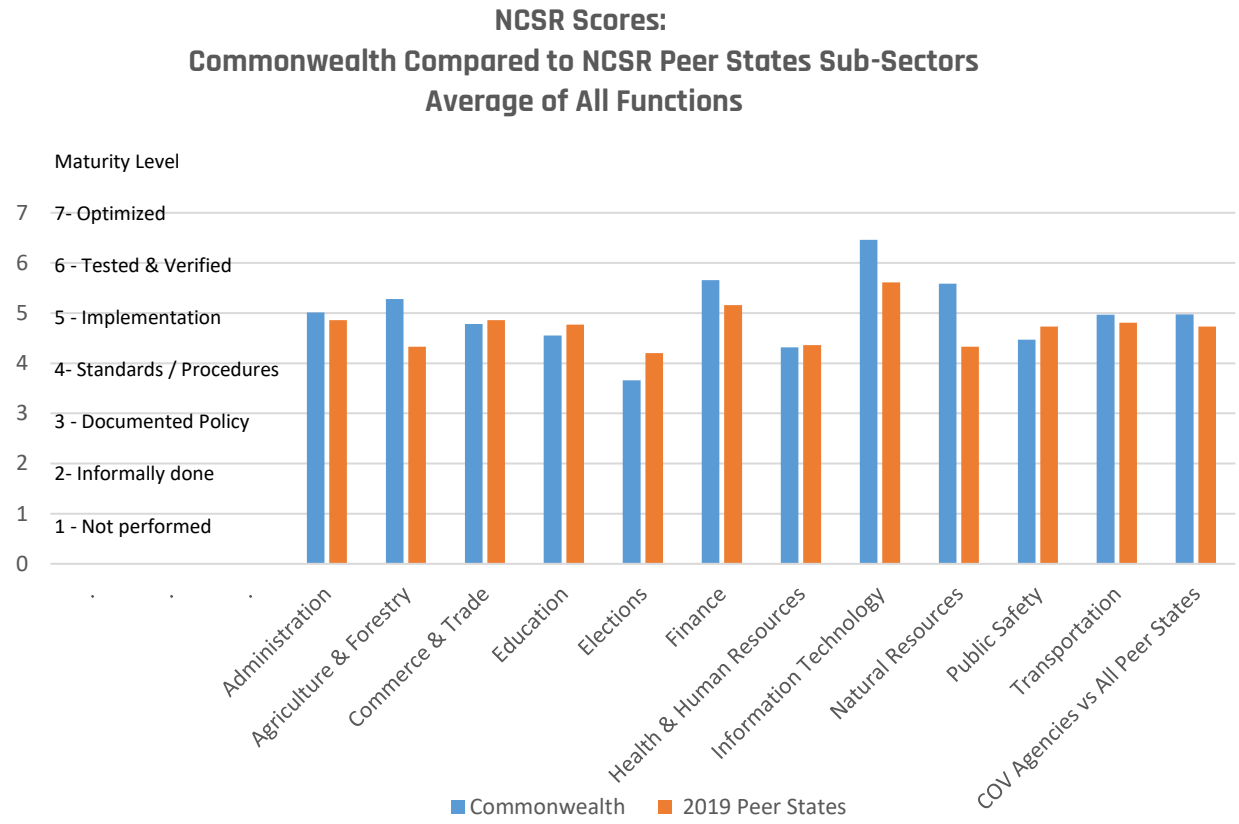


Figure 15: Comparative Scores by COV Secretariat/NCSR Peer State Sub-Sectors

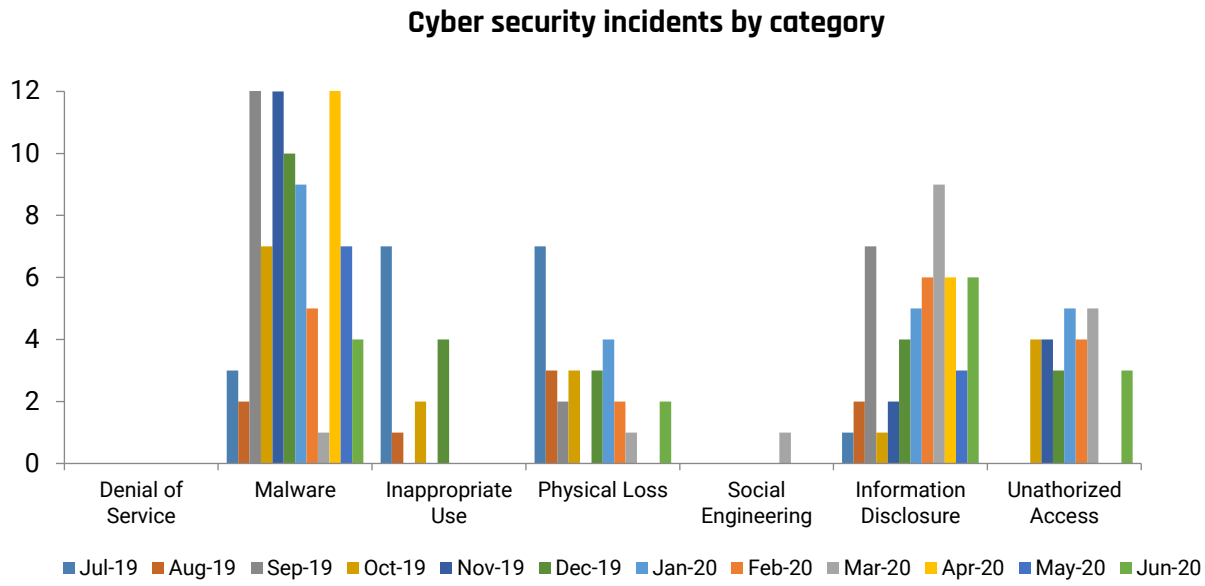
Analysis of Cyber Incidents

The Code of Virginia, §2. 2-603(G), requires all executive branch agency directors to report IT security incidents to the CIO within 24 hours of discovery in accordance with IT security standard SEC501. The Commonwealth Security Incident Response Team (CSIRT) then categorizes each security incident based on the type of activity. CSIRT identifies a cyber incident as an event that threatens to do harm, attempts to do harm or does harm to the system or network. According to the 2020 Commonwealth IT Security Annual Report, the Commonwealth experienced more than 66 million attack attempts on the network and blocked more than 50,000 pieces of malware. Despite many layers of protection, the Commonwealth still experienced nearly 200 IT security incidents in calendar year 2020.

Malware attacks accounted for the largest number of incidents, followed by information disclosure as summarized in the chart below. As the largest category of incidents, malware is a constant threat to Commonwealth devices and data. Malware programs are designed to infect legitimate users' computers to damage systems or provide unauthorized access to sensitive data. Malware can use multiple attack vectors to carry out cyberattacks. Phishing emails containing malicious links or attachments and infected website redirection are the two primary avenues of attack. Information disclosure incidents continued to be a threat. These incidents all revolve around the user. These often involve cases where users send unencrypted

emails containing sensitive data, or where physical documents were misfiled and sensitive information was mailed to the wrong recipient. While multi-factor authentication protects credentials from being exposed and utilized, it has not resolved the human error that is often associated with data disclosure. Providing additional security awareness training will help to protect both Commonwealth employees and data (Figure 16).

Figure 16: Cyber security incidents by category



Security awareness training is critical to protecting COV employees, systems and data from cyberattacks. As the attack landscape is constantly changing, the last line of defense remains the same – the employee. While technical controls can be put in place to protect the environment, the most effective approach is employee training. The COV IT security standard requires all employees to take security awareness training annually. This allows a large amount of time between training for attackers to develop new techniques and employees to forget what they have learned. In order to supplement this yearly training, CSRM has developed a service where agencies can request simulated phishing campaigns to reinforce security awareness training. Phishing campaigns test established procedures to determine if employees know when and where to report suspicious emails and it provides insight into gaps in the employees understanding of what tactics are employed that lead to a successful phish.

Cybersecurity incident trends continue to be monitored. CSRM has been working diligently to protect Commonwealth systems from cyber threats. As best practices are implemented and additional layers of protection are added, attackers develop new tactics to compromise systems. CSRM is continually investigating new security controls to protect the environment from compromise.

Critical exploits in the wild decreased from the previous year. Zero day vulnerabilities are newly discovered vulnerabilities that do not have patches available. These vulnerabilities are prime targets for attackers. Attackers develop exploit code using these vulnerabilities to install malware on a device before the manufacturer can provide an update or patches can be

applied. As attackers publish the exploit code in the wild, these zero day vulnerabilities pose an increased risk to the environment.

During 2020, the total number of critical exploits tracked by VITA decreased from 181 to 14, a 92% decrease. As agencies put more data into the eGRC system, the vulnerability reports can be tuned to only include those products that are being used. This tuning resulted in a decrease in the number of critical vulnerabilities being tracked.

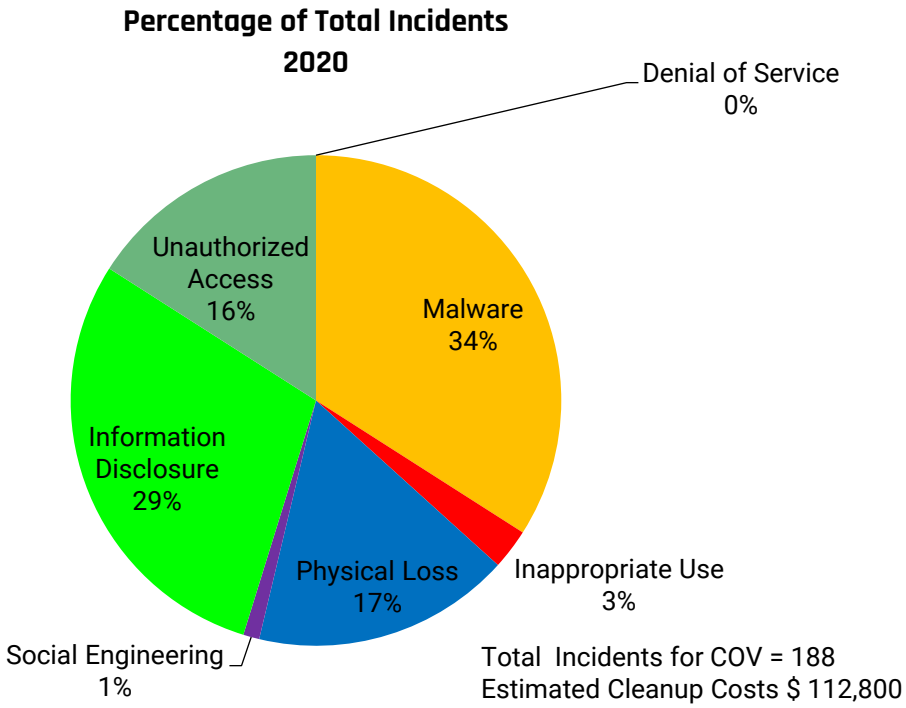
Cyber intelligence from Commonwealth partners

Reported security incidents are analyzed and grouped into one of the following categories described below:

- Denial of service - Loss of availability of a COV service due to malicious activity
- Inappropriate usage - Misuse of COV resources
- Information disclosure – COV data was exposed to recipients that did not have a need to know this data. COV systems were not accessed as part of the disclosure.
- Malware - Execution of malicious code such as viruses, Trojans, ransomware, spyware and key loggers
- Social engineering – Attempt to get the user to click on a malicious link, open a malicious attachment or provide confidential information, such as account credentials
- Physical loss - Loss or theft of any COV resource that contains COV data
- Unauthorized access - Unauthorized access to COV systems and/or data

During 2020, malware was the top category for security incidents. Information disclosure moved to second place followed by physical loss, unauthorized access, inappropriate use and social engineering. The COV environment did not experience any denial of service (DOS) attacks during 2020.

Figure 17: Incidents by category



Ransomware

Ransomware is a type of malicious software that is designed to deny access to a computer system or data by encrypting it until a ransom is paid to the hacker. Infections typically occur via phishing emails, poorly secured network and services or vulnerabilities in infected websites.

Ransomware attacks against state and local governments were the top cybersecurity industry story in 2020. Numerous government entities in the United States were attacked by ransomware hackers compared to other industries (Figure 18). In the Commonwealth, we have seen 20 attempted ransomware attacks in the past three years. VITA continues to remain vigilant against this type of attack.

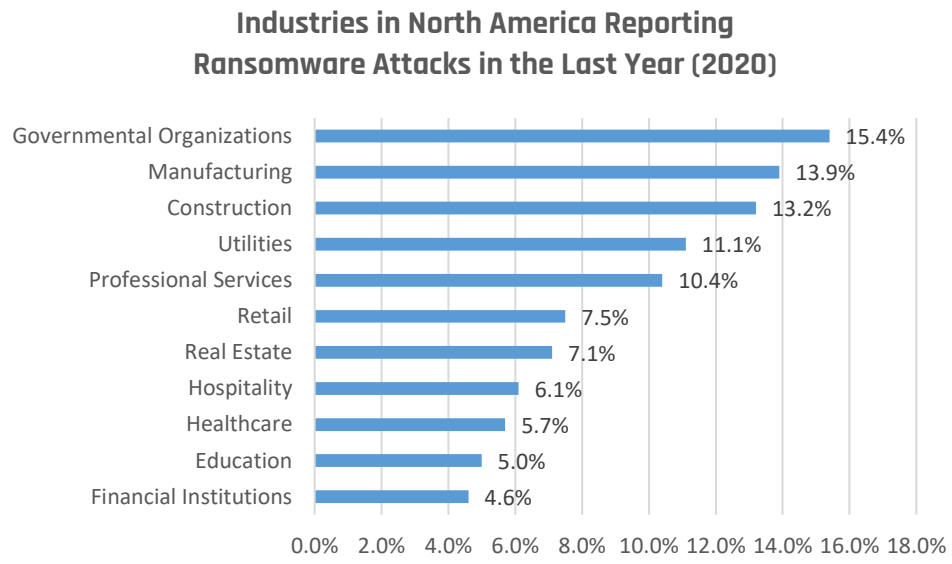


Figure 18: Ransomware Attacks in North America (Source: Safety Detectives)

Multiple factors contribute to ransomware's threat. Governments, like businesses, are increasingly providing services digitally and, thereby, increasing the numbers of systems and channels that could be attacked. Government sometimes struggles to keep pace with technology, which can result in outdated or vulnerable technologies remaining in place. In addition, government's susceptibility to ransomware and other cyberattacks is aggravated by a severe shortage IT security talent. A CyberEdge Group report found that 85% of organizations are experiencing a shortfall of skilled IT security personnel, and survey respondents cited "lack of skilled personnel" as their biggest obstacle to adequately defending against cyber threats. This shortage can be magnified in state governments due to fiscal restraints.

The estimated cost of ransomware attacks in the U. S. in 2020 was $20 billion; the cost in 2019 was $11.5 billion, and the cost in 2018 was $8 billion. Payouts to ransomware perpetrators have been rising along with the number of attacks. A 2020 CoveWare report states that ransomware payments have been rising since 2018 and that the average ransom payment in the second quarter of 2020 was $178,254 – a dramatic 60% jump from the first quarter of the year.

Ransomware can be devastating to an organization, and government entities are frequent targets. Recovery after a successful ransomware attack can be a difficult process. The services of a data recovery specialist may be needed. Even when victims pay to recover their files, there is no guarantee that they will recover their files and avoid further problems. Although the financial costs of ransomware are often significant, direct costs alone are not the extent of the risk: loss of data, organizational trust and credibility can occur.

Some cities, like the City of New Bedford and the City of Lafayette, have agreed to pay ransomware attackers. Other victims such as the State of Louisiana and Greenville, North Carolina have refused to pay. Recently, the U. S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has advised against paying ransom to cybercriminals.

Agencies should contact VITA and law enforcement to coordinate ransomware response activities.

In 2020, the General Assembly directed VITA to study the Commonwealth's ransomware attack preparedness, House Joint Resolution 64 (HJ64). The report was published in January 2021.

To gain insight into how public bodies in the Commonwealth perceived their level of threat from ransomware, VITA sent a survey to state agencies and institutions of higher learning. The following figure (Figure 19) is based on those responses. More than 75% of those respondents indicated that ransomware is a real threat to their organization.

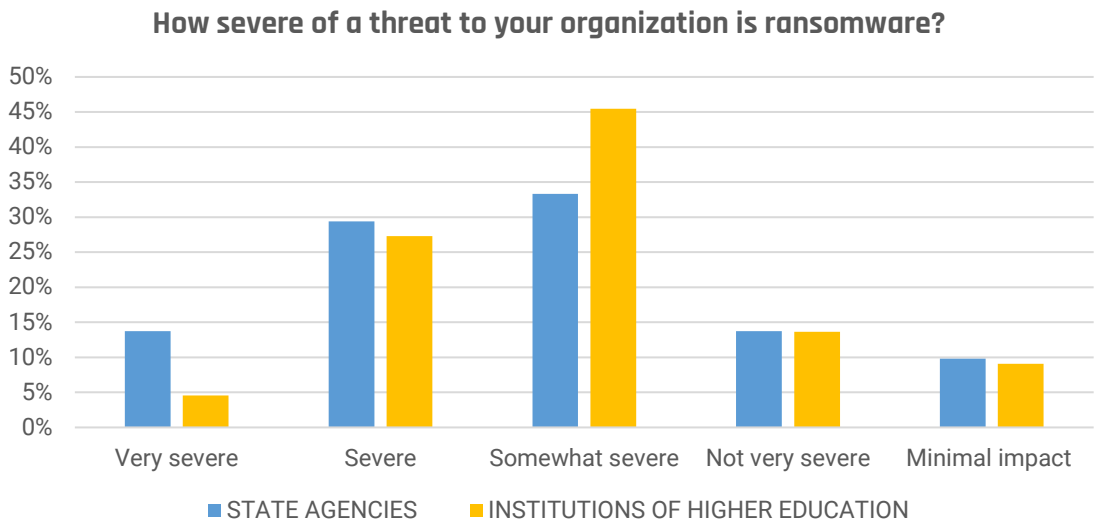


Figure 19: Severity of Ransomware Threats

Incident Response

The Code of Virginia §2. 2-603 (G) requires executive branch agency directors to report cyber incidents to VITA within 24 hours of discovery. Incidents can be reported 24/7 using an online incident reporting form (located at https://www.vita.virginia.gov/Commonwealth-security/incident-reporting/) or by calling the Commonwealth's help desk. Attacks frequently compromise personal and business data, and it is critical to respond quickly and effectively when security breaches occur. Rapid incident response can minimize loss, prevent theft, and stop the disruption of services that can be caused by incidents. A systematic incident response process also promotes consistent incident handling, so that the appropriate actions are taken to address incidents and agencies are better prepared to protect against future attacks according to NIST.

All reported incidents are sent to VITA's incident response team (CSIRT). The CSIRT will categorize and prioritize the incident based on the activity that occurred.

Quantitative Cybersecurity Risk Analysis

VITA developed a methodology to estimate the potential financial impact associated with data breaches associated with cybersecurity incidents within the Commonwealth executive branch, independent agencies and institutions of higher education. The methodology was established to provide a quantitative tool for Commonwealth leadership to use to protect the Commonwealth's bond rating, as well as to make informed, risk-based decisions related to IT investments, cyber liability insurance and security exceptions.

This analysis determines the residual risk associated with each IT system that an agency owns. Residual risk is the amount of risk, or danger, associated with a data breach after all natural and inherent risks have been mitigated by risk controls. The residual risk is used to estimate the potential financial loss associated with cybersecurity incidents. The estimated loss is based on the detailed system information provided by the agency, including IT audit findings, IT risk assessment findings, the number of records the system processes, the presence or absence of critical IT controls in the system and other factors.

It was determined that the potential financial loss of one Commonwealth data record was $4,800. Based on the millions of records processed by agencies on a daily basis, and other risk factors used in the analysis, the estimated cost of a breach quickly increases exponentially. The table below includes the top 10 agencies with potentially the most system residual risk.

	Agency
1	Department of Motor Vehicles
2	Department of Social Services
3	Virginia Retirement System
4	Department of Treasury
5	Department of Medical Assistance Services
6	Virginia Employment Commission
7	Virginia State Police
8	Department of Corrections
9	Department of Emergency Management
10	Department of Taxation

Figure 20: Top 10 Agencies with Most System Residual Risk

Utilizing the estimated costs of a data breach that were determined by our quantitative risk analysis methodology, VITA worked with the Department of Treasury to develop a cyber insurance program for the Commonwealth. The Department of Treasury, under the 2020

Appropriations Act (Chapter 1289, Item 285 H), purchased cyber insurance for executive branch agencies.

Treasury's cyber insurance program includes coverage for the following:

- *Data breach response and crisis management:* In the event of a breach, agencies are required by law to notify affected parties and in some cases, offer credit monitoring services to victims. This can add to overall data breach costs. In addition, coverage for crisis management can help limit the negative impact due to adverse publicity on the agency's reputation.

- *Privacy regulatory defense, awards and fines:* Dealing with multiple states and federal regulatory agencies (which oversee data breach laws and regulations), can be a significant expense for a state agency. This policy assists in the costs of working with regulators during investigations and in the payment of regulatory fines and penalties levied against the agency stemming from the breach.

- *Data privacy liability:* This coverage will defend an agency against legal claims brought by a stakeholder who suffered a significant financial loss after their personal data was compromised. A typical suit could allege that the agency was negligent in failing to protect the stakeholder's personal information, and that their loss was directly attributable to the agency's negligence.

- *Cyber extortion/ransomware:* Ransomware and similar malicious software are designed to steal and withhold key data from organizations until a steep fee or ransom is paid. Cyber liability insurance can help recoup losses related to cyber extortion.

- *Business interruption:* A cyberattack can lead to an IT failure that disrupts business operations, costing an affected agency both time and money.

- *Data and assets protection:* This coverage can help pay for costs incurred to recover or replace electronic assets and data that have been compromised, damaged, lost, erased or corrupted.

- *Social engineering fraud:* Many hackers initiate social engineering campaigns through the practices of phishing, baiting and other online scams. Frauds due to social engineering can be particularly expensive.

Strengthening Cybersecurity

Agencies have taken steps to strengthen their cybersecurity postures, including addressing more than 3,800 issues in FY2020 related to audits, risk assessments and vulnerability scans. Agencies addressed issues in various aspects of information security, with most issues being resolved in the following three control families this year: awareness and training (23%), maintenance (23%) and access control (12%). Agencies added new controls and enhanced existing security measures, such as providing improved IT security awareness training to Commonwealth employees to prevent a potential breach, conducting appropriate maintenance on equipment to keep it secure, and terminating IT accounts timely and accurately to protect Commonwealth data. The chart below (Figure 21) shows ALL IT security issues (not just policy-related issues) that have been closed / resolved in FY 2020 in each IT security control family.

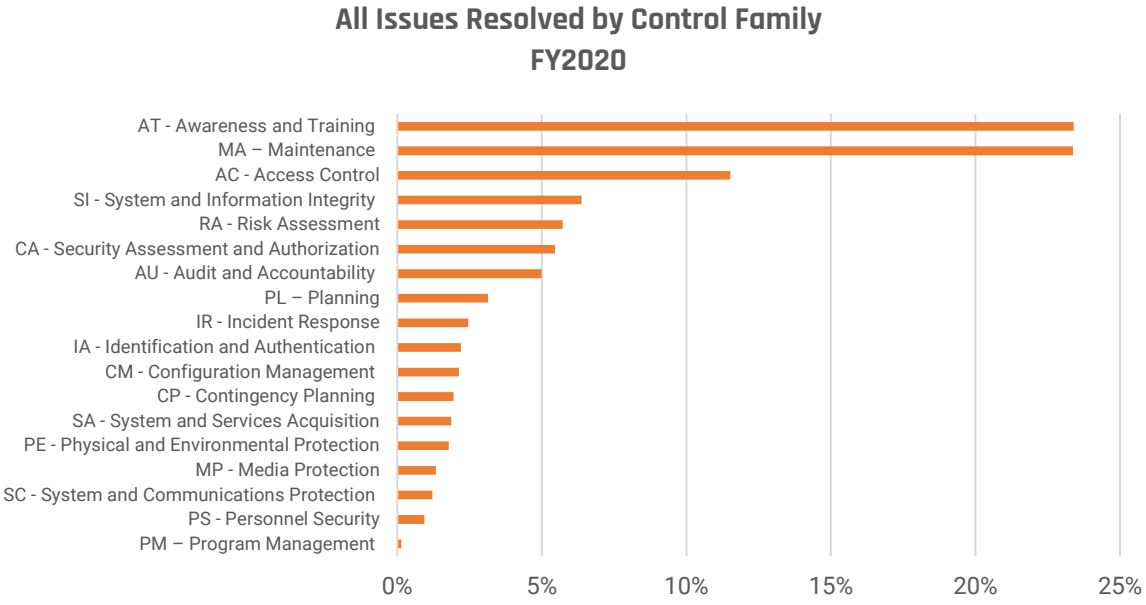


Figure 21: Issues Resolved by Control Family

IT security issues specifically related to a policy failure or lack of a required policy that were closed or resolved in fiscal year 2020 are categorized by IT control family in the chart below (Figure 22). Issues were noted in nearly every area of information security this year, with most of the policy-related issues occurring in the areas of incident response (13%), audit and accountability (12%) and access control (12%).

Figure 22: Resolved Policy Issues by Control Family

CONCLUSION

Effective cybersecurity policies are a critical component of a comprehensive cybersecurity program. Each agency must establish and follow cybersecurity policies and procedures that are suited for their agency's business, relevant for the types of data the agency handles, and appropriate for the laws and regulations applicable to the agency.

VITA has implemented risk mitigation strategies, such as publishing the annual *Information Security Report* and offering shared services to Commonwealth agencies, including ISO services, IT audit services and vulnerability scanning services. In addition, VITA encourages ISO education through an ISO certification process that includes an orientation and other training processes that help ensure agency personnel understand Commonwealth security requirements. VITA also uses its governance authority to address risk by ensuring that agencies place appropriate priority on addressing IT security concerns.

Based on the NCSR self-assessment results, Commonwealth agencies have implemented policies and procedures slightly better than our peer states around the country, but there are still significant improvements to be made. Analysis of trends in IT security issues determined that policy issue deficiencies occurred most frequently in the contingency planning and access control security families. To be effective, policies must address management, operational and technical controls. VITA has established standards addressing these areas, including a new IT security awareness training standard that requires training for Commonwealth employees to help them identify and prevent potential cyberattacks. Standards and policies also require that appropriate technical controls are established to prevent unauthorized access to sensitive Commonwealth information.

VITA's quantitative cyber-risk analysis method developed in 2019 has continued to mature in 2020 and is being used to guide and prioritize Commonwealth and agency IT risk management decisions. The quantitative cyber-risk model assigns actual dollar amounts to each system indicating the potential financial loss that could occur if the system were hacked, breached or compromised in some manner. Agencies that process many sensitive records, have systems that lack critical IT security controls, or have *not* undergone an audit or risk assessment could suffer from particularly costly breaches based on our model. As a result, investments should be made to prioritize remediating these risks accordingly.

Agencies have taken steps to strengthen their cybersecurity posture, including addressing more than 3,800 security issues during the year. Implementing new controls and enhancing the existing controls further promotes the confidentiality, integrity and availability of Commonwealth information.

The Commonwealth cybersecurity program has matured with consistent focus towards the ongoing operational needs of each agency, guided by enhancements in services and technology to protect the data and assets essential to meet the public sector demands.