Virginia Information Technologies Agency

Fiscal Year 2019 Commonwealth of Virginia Report on Cybersecurity Policies

www.vita.virginia.gov

Prepared and Published by:

Virginia Information Technologies Agency

VITA - Powering the commowealth's digital government

Comments on the

Fiscal Year 2019 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

Virginia Information Technologies Agency

Contents

FY19 Annual Report

Contents

TABLE OF FIGURES

Executive Summary

The Fiscal Year 2019 Commonwealth of Virginia (COV) Comprehensive Cybersecurity Policies Review is the first such report by the chief information officer (CIO) of the commonwealth. As directed by § 2.2-2009(C) of the *Code of Virginia,* effective 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 chief information security officer (CISO) to address cybersecurity issues in the commonwealth. In addition, 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.

Based on research for this report, we have determined that effective cybersecurity policies significantly help the commonwealth's security posture. Effective policies lead to fewer security incidents. Fewer incidents result in more up time for applications and agency business as issues are pre-emptively avoided.

Effective policies implemented at the agencies help to better prepare staff for auditing and compliance requirements. Remediation after the fact is more difficult, expensive and time-consuming than addressing the issue correctly from the outset. Auditors in the commonwealth routinely review and assess whether agencies have and are maintaining required cybersecurity documentation. Auditors have often cited audit issues that relate to policy deficiencies over the last two years.

CSRM monitors (through reporting, corrective actions and governance) all IT audit issues, and most agencies can remediate these in a timely fashion. In addition, various IT security metrics for each agency are continually measured and monitored. Agencies that do not effectively remediate audit issues, do not perform required audits, or fail to adequately meet CSRM's audit and risk management requirements pose a greater risk to the commonwealth overall.

One issue identified by CSRM is the use of hardware and software that is not supported by the manufacturer because it is out-of-date or end-of-life. Agencies may be using out-of-date IT components to support a "legacy" application for which a newer, updated and more secure application has not been developed or procured. The use of outdated hardware and software is a major IT security vulnerability. It is a common practice for malicious third parties to attempt to attack weaknesses in unsupported or outdated systems because technical weaknesses are well-known and therefore easier to exploit. When CSRM identifies these issues, we require agencies to present a plan to address the problem in a timely and complete manner.

VITA uses its governance authority over agency IT budgets and IT acquisitions to ensure that agencies are adhering to information security standards. IT budget requests from agencies that are underperforming in the IT security area could be rejected by VITA until acceptable and actionable remediation steps have been taken.

The Code of Virginia requires all executive branch agencies to report cybersecurity incidents to VITA. A cybersecurity incident is any event or activity that could do harm or threatens to do harm to commonwealth IT systems or data.

An incident response team is on-call around the clock and works to immediately contain, identify, prioritize and mitigate any threat. All incidents are recorded into our enterprise governance and compliance database for tracking purposes.

Each incident is also categorized according to type. The most frequently tracked incident in the commonwealth is for malware. Malware can infect or damage a computer and may be used as a means to gain unauthorized access to a network.

Malware and other incidents have occasionally led to data breaches. In the last two years, all such breaches have been quickly identified and contained, so that minimal data was lost or exposed. All breaches are analyzed extensively after the fact to assure that all underlying issues have been identified and corrected to prevent it from reoccurring.

Attacks on the commonwealth's cybersecurity occur on a minute-by-minute basis. CSRM aggressively takes measures to prevent, counter and investigate all cybersecurity incidents. Although CSRM has been able to prevent and mitigate most attacks and breaches, we are acutely aware of the rising number of cyberattacks we are seeing. In particular, we have documented an increase in "ransomware" attacks and are taking focused efforts to identify and prevent them.

Key takeaways:

- Effective policies are an important component of a comprehensive cybersecurity program. Each agency must develop policies that take into account how the agency conducts business, the types of data that it handles and the laws and regulations that govern it.

- VITA uses its governance position to develop overall policies and standards to manage cybersecurity in the commonwealth and protect commonwealth data assets and IT services. VITA is constantly identifying and reviewing cybersecurity issues and adjusting policies, procedures and processes to address cybersecurity priorities.

- Audits, training and working with agencies are key steps that VITA CSRM utilize to understanding the threat landscape and strengthen cybersecurity in the commonwealth.

- The commonwealth's new multi-vendor IT service provider model has had a significant and positive impact on cybersecurity effectiveness and flexibility.

- VITA's investment in a shared cybersecurity model has improved cybersecurity for the agencies that participate in the model, as well as the overall cybersecurity posture of the commonwealth.

- VITA expects the new cybersecurity implementation within the multi-vendor model to provide increased transparency, effectiveness, and understanding for commonwealth systems.

- The commonwealth's reliance on technology continues to grow, increasing the critical nature of service and data availability. The material impact of a loss of those services is expected to increase as our technology footprint continues to grow by approximately 8% each year.

- New technology introduced with the multi-supplier model will help to improve cyber hygiene for data protection. More than 10 new services are now available with data encryption capabilities to enable secure hosting on cloud platforms.

- Centralized services continue to be an integral part of our IT strategy. Incorporating centralized security program and security audit services has resulted in a continued upward trend in the progress of commonwealth security programs. Compliance scores for security programs of participating agencies increased 19% for audit compliance and 22% for risk management compliance over the previous three years showing marked improvement in the programs.

- VITA continues to evaluate both the infrastructure and security programs for enhancements. Additional focus is needed on commonwealth partners such as localities and third party partners as they will be the primary source of risk to the Commonwealth in the future.

Report

CSRM's governance program over cybersecurity was used as a starting point to address the § 2.2-2009(C) requirement. CSRM uses laws, policies, standards and processes to help govern cybersecurity across the commonwealth with particular focuses on strategy, budgeting, risk management and incident response.

To establish a governance program for cybersecurity in the commonwealth, CSRM has developed and maintained an 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, but are not limited to, any regulatory requirements an agency is subject to, information security best practices and specific requirements defined in each of the eight standards.

The CSRM standards define the minimum acceptable level of information security and risk management activities that COV agencies must implement for their information security program.

In 2012, CSRM modified the commonwealth IT security standards to mirror the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 rev. 4, *Recommended Security Controls for Federal Information Systems and*

Organizations, as a framework for IT security in the commonwealth (https://nvd.nist.gov/800-53/Rev4). Compliance with the NIST SP 800-53 framework 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 as well as private sector buyers and suppliers.

NIST SP 800-53 provides a catalog of controls that support the development of secure and resilient information systems. These controls are the operational, technical and management 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. The NIST control families and their two letter abbreviations are:

- Access control (AC)
- Awareness and training (AT)
- Audit and accountability (AU)
- Security assessment and authorization (CA)
- Configuration management (CM)
- Contingency planning (CP)
- Identification and authentication (IA)
- Incident response (IR)
- Maintenance (MA)
- Media protection (MP)
- Physical and environmental protection (PE)
- Planning (PL)
- Personnel security (PS)
- Risk assessment (RA)
- Systems and services acquisition (SA)
- System and communications protection (SC)
- System and information integrity (SI)

Commonwealth Cybersecurity Risk Mitigation Strategies

CSRM uses several strategies to identify and manage cybersecurity risks in the commonwealth.

Commonwealth of Virginia Information Security Annual Report

Annually, CSRM issues a report on the state of IT security in the commonwealth (https://www.vita.virginia.gov/commonwealth-security/annual-reports/). We measure and grade each agency in two key areas: Risk management compliance and audit compliance.

Risk Management Compliance

Grades for risk management compliance measure the effectiveness of each

agency's risk management program. Risk management assures that an agency is working to identify and mitigate the IT security risks that could occur. Agencies must be continually evaluating the threats that could affect their IT environment and data. Threats can exploit vulnerabilities and weaknesses in IT systems. Agencies need to measure the likelihood of these threats occurring and also the impact to agency business and confidential data if they were to occur. Then the agency must develop a system security plan for each of its systems to identify and plan for the implementation of IT security controls to mitigate the issues.

Overall, the percentage of agencies receiving an A or B score on its risk management program has shown an increase in each year (Figure 1).

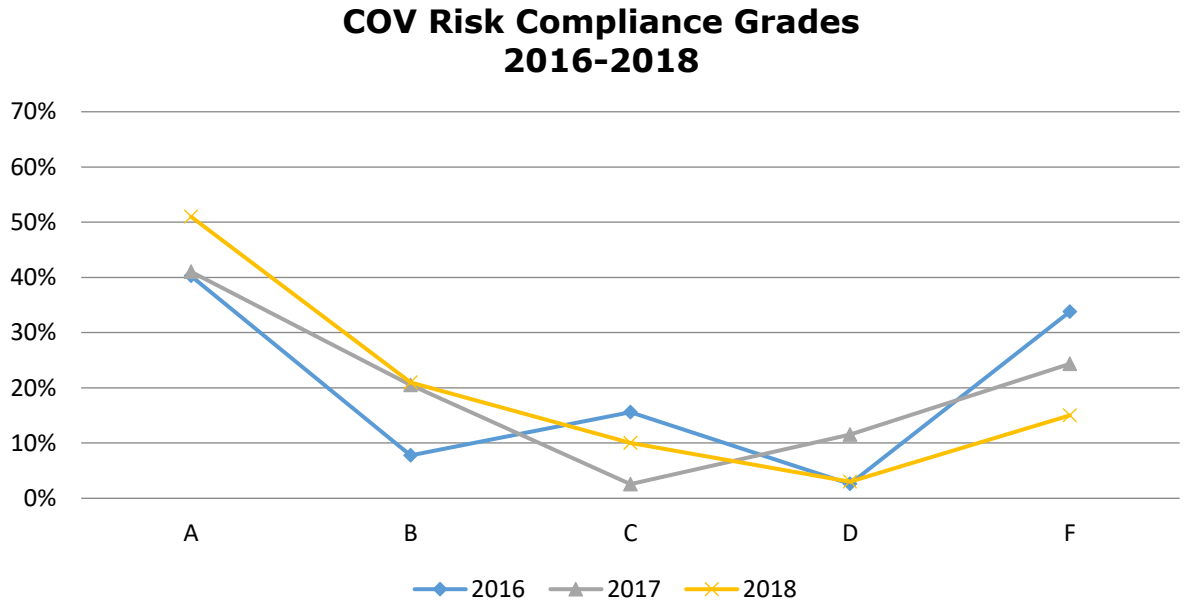

Figure 1: Agency Risk Compliance Grades

Audit Program Compliance

CSRM also grades each agency on the effectiveness of its IT auditing program. Metrics are gathered to determine whether agencies are meeting the requirement to audit each sensitive system within a proscribed frequency. In addition, CSRM reviews and monitors the remediation steps that agencies are making to correct deficiencies identified during audits.

Overall, the percentage of agencies receiving an A or B score on its audit compliance program has also shown a slight increase in each year (Figure 2).

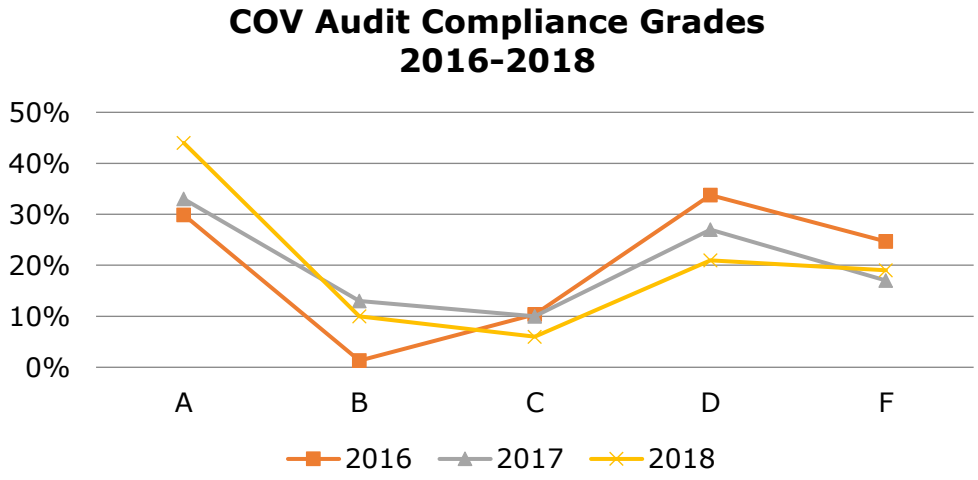

Figure 2: Agency Audit Compliance Grades

Shared IT Risk Management and IT Security Auditing Services

In 2017, with the assistance of the Department of Planning and Budget, VITA established a new division to improve the IT security posture of agencies in the commonwealth. The division specializes in providing IT risk management services and IT security auditing services. These 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 now over 30 agencies participating in the services.

Starting in fiscal year 2017, the Department of Planning and Budget (DPB), approved appropriations to improve cybersecurity in the commonwealth. The appropriations were allocated to 77 executive agencies that are subject to VITA governance. The funding model, developed jointly by VITA and DPB, was based largely on the number of "sensitive" IT systems that had been reported by the agencies. Funding was allocated to each agency for "IT auditing" services, and for "IT security management services".

Agencies that used the funding to participate in VITA's shared cybersecurity services showed significant improvements. Audits of sensitive systems increased from approximately 20% to nearly 60% in just over 2 years (Figure 3). In addition, participating agencies saw the number of Risk Assessments performed increase from 12% to almost 90% (Figure 4). Audits and Risk Assessments are two extremely important cybersecurity tools that provide assurance that sensitive systems have been assessed for proper implementation of required IT security controls. These tools provide agencies with the means to identify gaps in security so that they can be prioritized and corrected.

In addition, compliance scores for agencies using the shared cybersecurity services also increased significantly in just over three years. For agencies participating in the shared audit service, the percentage of agencies scoring an "A" increased by

19% (from eight to 14 A's), while the percentage of agencies receiving a failing grade of "F" decreased by 17% (from seven to only two F's).

Compliance scores for agencies using the shared IT security management services also faired very well in the same three year period. Agencies receiving an "A" score for compliance in this area improved by 22% (from 16 agencies receiving an A to 23). Agencies receiving a failing grade of "F" decreased over three years from seven agencies to only one.

As the shared cybersecurity services continues to grow and mature, we expect that all participating agencies will have passing compliance scores in these areas in the near term.

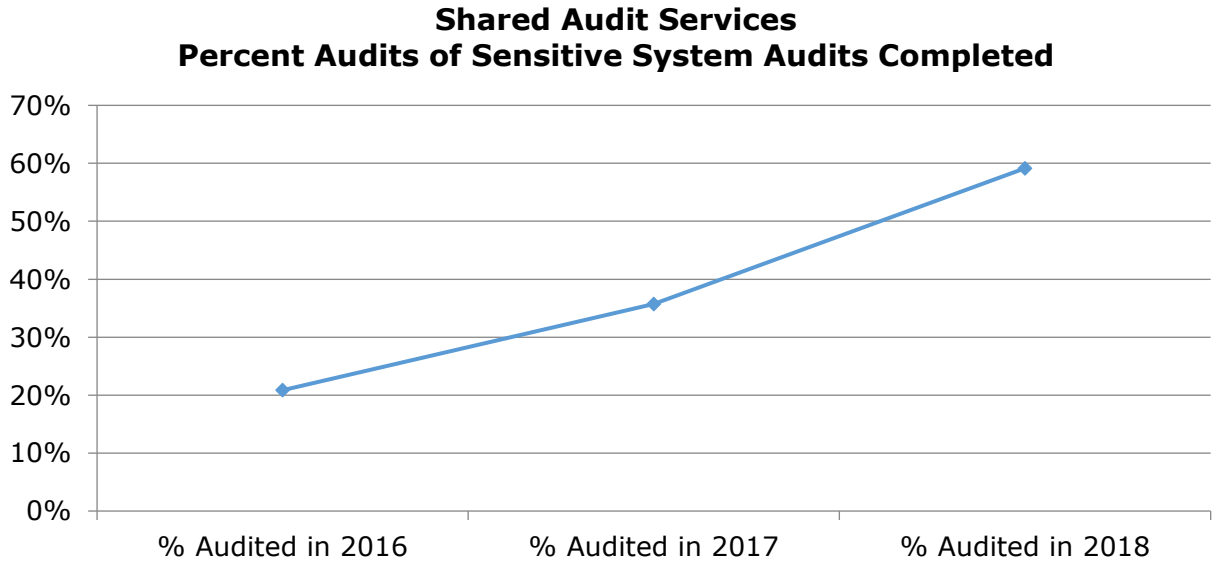

Figure 3: Audits Completed by Shared Audit Services

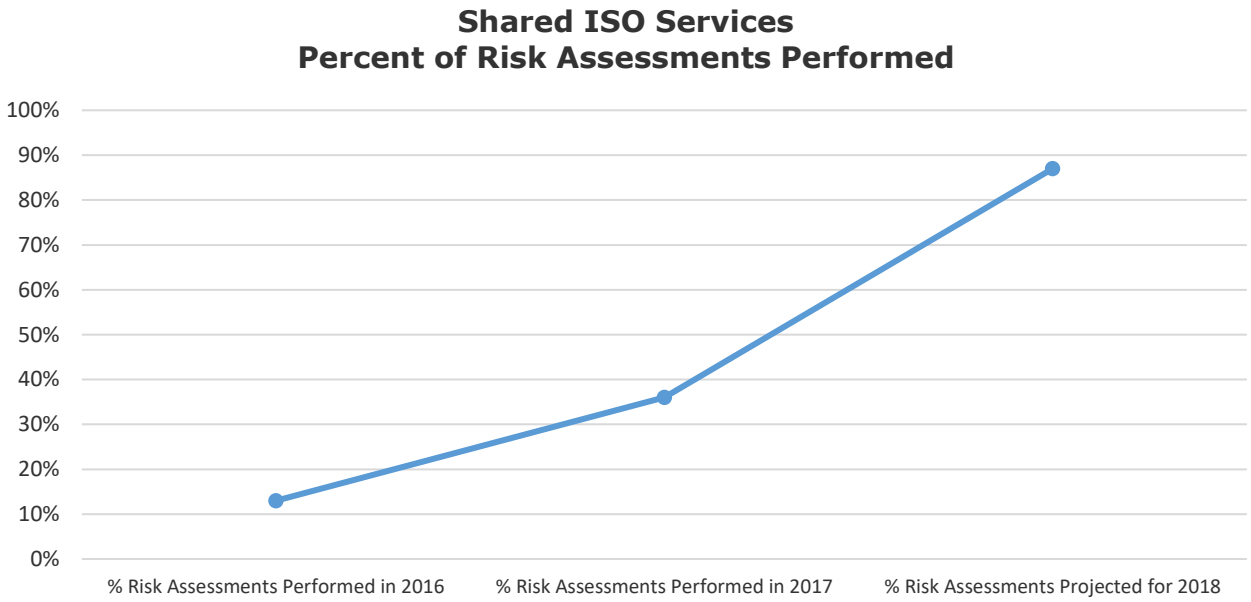

Figure 4: Risk Assessments Performed by Shared ISO Service

ISO Certification and Training

VITA requires all executive branch agencies to appoint an information security officer (ISO) to manage the agency's security program. In addition, each ISO must complete baseline IT security training. VITA monitors and "certifies" this training. In calendar year 2013, the first year of the ISO certification program, 59% of executive branch agencies had a certified ISO who had completed the baseline IT security training. In calendar year 2018, 95% of executive branch agencies had a certified ISO. CSRM believes that a better-trained ISO community in the executive branch leads to improved IT security for the commonwealth. CSRM also strongly encourages all ISOs to obtain additional training. One of the requirements to maintaining the ISO certification is to demonstrate that the ISO has obtained at least 20 additional hours of IT security training each year.

IT Acquisitions and Procurement

VITA uses its goverance over IT acqusition and procurement to ensure cybersecurity standards are properly prioritized across the commonwealth.

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 and with cybersecurity policies and standards.

Agencies that have not implemented acceptable IT risk management and IT audit compliance programs are in jeopardy of having their IT projects or IT budget rejected or delayed. Agencies must present VITA with reasonable and obtainable plans for correcting their programs before acquisitions will be approved.

Multi-Supplier IT Model

VITA has adopted a new model for providing IT services to the commonwealth. Virginia has moved away from a single-supplier long-term contract for information technology to a multi-supplier environment with shorter, more flexible contracts. The new model has been in place for less than a year. The increased flexibility will allow the commonwealth to more quickly and easily incorporate new and changing technologies. These changes will also better position us as we continue our efforts to move to the cloud.

IT security is one of eight different areas of IT that are now outsourced to specialized suppliers. The IT security supplier is solely devoted to analyzing, monitoring and implementing advanced cybersecurity tools and practices under the direction of VITA.

VITA has made a long-term commitment to ensuring that this new model for IT service delivery will be effective and successful for the commonwealth.

Methodology

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

- *CSRM's enterprise governance, risk and compliance application (eGRC):* CSRM uses the eGRC application to understand the policies, regulations, processes and technologies that affect each executive branch agency in order to better manage IT security risk and compliance for the commonwealth.

  The eGRC also allows CSRM to track IT security issues reported to us. CSRM requires each agency to have independently conducted audits performed. Any IT security related issues that are determined by audits are documented in the eGRC system for tracking. In addition, CSRM monitors IT audits of agencies performed by the auditor of public accounts (APA), the Office of State Inspector General as well as by other entities. For this report, we particularly focused on any issues that related to a deficiency in a cybersecurity policy or regulatory requirement.

- *Results of the National Cyber Security Review (NCSR):* The Department of Homeland Security sponsors the annual Nationwide Cyber Security Review (NCSR). The NCSR is a self-assessment survey designed to measure gaps and capabilities of participating state and local governments. Executive branch agencies subject to VITA governance completed the self-assessment. The NCSR evaluates cybersecurity maturity and allow us to compare commonwealth metrics to respondents across the US from other states and local governments.

- *The 2018 Commonwealth of Virginia Information Security Report:* As required by the Code of Virginia, CSRM 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.

- CSRM requires that agencies report IT security incidents. CSRM defines an IT security incident as any event that threatens to do harm, attempts to do harm, or does harm to a system or network. Incidents are logged in the eGRC database and categorized as to type and priority. In this report, a particular focus was made on incident types that may have caused or did cause sensitive information to be breached.

Policy Importance

A cybersecurity policy identifies the rules and procedures that all individuals accessing and using an organization's IT assets and resources must follow. The goal of these policies is to address security threats and implement strategies to mitigate IT security vulnerabilities, as well as defining how to recover when a network intrusion occurs. In addition, cybersecurity policies provide guidelines to employees on what to do and what not to do. They also define who gets access to what, and what the consequences are for not following the rules.

Cybersecurity policies are important to help agencies ensure the success of their cybersecurity strategies. An effective policy sets expectations for management and employees. It provides guidance for mitigating risks, for protecting against malicious activities, outlines measurements and promotes compliance with commonwealth and regulatory requirements.

The lack of effective cybersecurity policies can result from many reasons, but typically include limited resources to devote to developing policies, slow adoption by agency management, or sometimes a lack of awareness of the importance of having effective cybersecurity policies in place.

Regardless of size, it is important for every agency to have documented cybersecurity policies, to help protect commonwealth data and other valuable assets. It is also often a legal or regulatory requirement for our agencies that must comply with various regulations such as PCI, HIPAA, IRS federal tax information safeguards and privacy laws. The key factor is to have "documented" cybersecurity policies that clearly defines the agency's position on security. This can be of critical importance in the event of a data breach and/or litigation discovery.

There are three core objectives of cybersecurity policies:

- **Confidentiality**: The protection of IT assets and networks from unauthorized users.
- **Integrity:** Ensuring that the modification of IT assets is handled in a specific and authorized manner.
- **Availability:** Ensuring continuous access to IT assets and networks by authorized users.

In general, cybersecurity policies should be developed with a multi-layered approach. Each agency is required to have a cybersecurity policy for each family of IT security controls. The policies below identify the core set of policies that every agency should have

- 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 is needed to identify the minimum logical access control measures that are needed for systems, programs, processes, and information.
- 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 identifies the steps to be taken in case of an incident; ensuring that the incident is handled and communicated; allowing the quick recovery of affected systems; determining the cause of the incident; and how to determine 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.

Policy Deficiencies

Each of the 17 control families contains a list of specifically required IT security controls. An agency must review, analyze and implement each control in each control family according to 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. Policy and procedures 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 understand or effectively implement the IT security controls needed to maintain the security of commonwealth systems and data.

As part of its oversight responsibilities, CSRM requires the 78 executive branch agencies under its governance, to submit the results of all IT security audits and IT risk assessments for analysis and monitoring. CSRM utilizes eGRC software to track and categorize any issues identified and to monitor remediation progress. These

issues are associated in the eGRC to the specific IT security family and control where deficiencies were noted.

CSRM analyzed the eGRC database in order to review issues associated with cybersecurity policies. All issues reported to CSRM in calendar years 2017 and 2018 were analyzed.

Of the 5,103 issues reported to CSRM over the two-year period, 627 (12%) specifically identified the lack of or a deficiency in required cybersecurity policies (Figure 5).

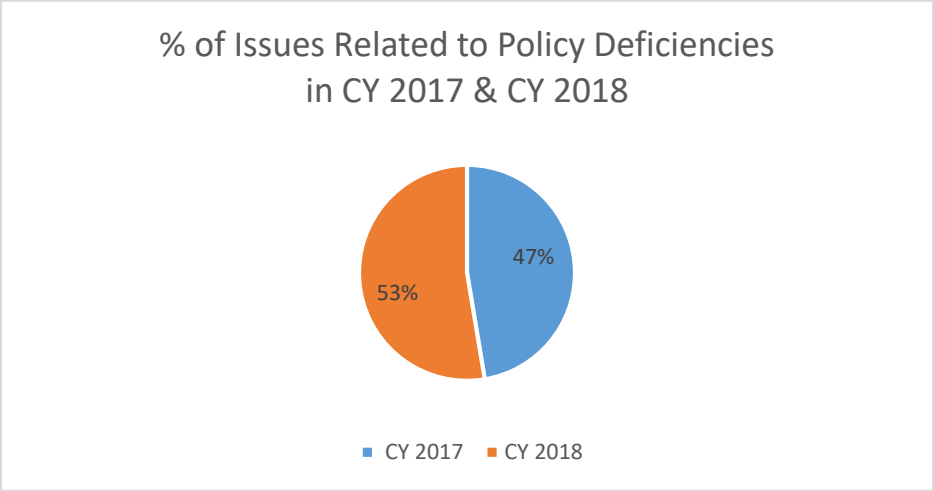

Figure 5: Issues Related to Policy Deficiencies

Additional analysis (Figure 6) shows the IT security control families most frequently identified as having policy deficiencies. The access control family had the most policy related audit and risk assessment issues. Access control is a security technique that regulates who or what can view or use resources in a computing environment.

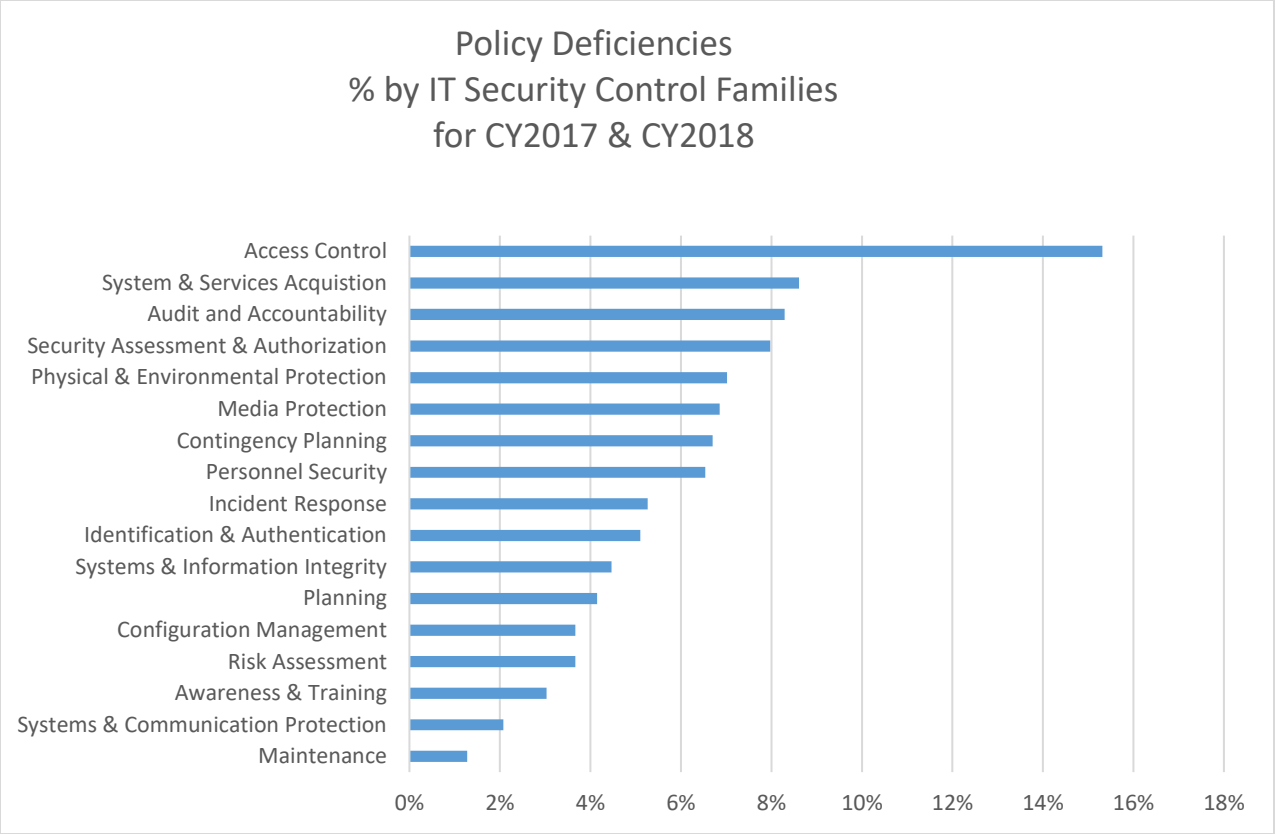

Figure 6: Policy Deficiency Issues by IT Control Family Group

Next, VITA reviewed the frequency in which policy deficiencies determined by audits and risk assessments occurred at agencies (Figure 7). It should be noted that even though an agency may have reported more such issues than other agencies, that could also mean particular agencies do a more thorough job in identifying weaknesses that need remediation. In most cases, the policy deficiencies reported by these agencies have been remediated.

Additionally, some agencies did not perform required audits and risk assessments and subsequently there were no issues of any kind identified or reported to CSRM. Of the 78 agencies monitored by CSRM for the CY2018 Annual IT Security Report, eight were determined to have inadequate audit programs and inadequate risk programs. An inadequate audit or risk program means that those agencies are not sufficiently and independently monitoring their cybersecurity responsibilities as required by § 2.2-2009(A). The lack of monitoring does not provide us with any assurance that those agencies have developed and implemented effective cybersecurity policies.

These agencies were determined in calendar year 2018 to have inadequate IT security audit and risk programs: Department of Military Affairs; Office of Attorney General; Southwest Virginia Higher Education Council; Virginia Center for the Arts; Virginia Department of Emergency Management; Virginia Economic Development Council; Virginia Foundation for Healthy Youth and the Virginia Resource Authority.

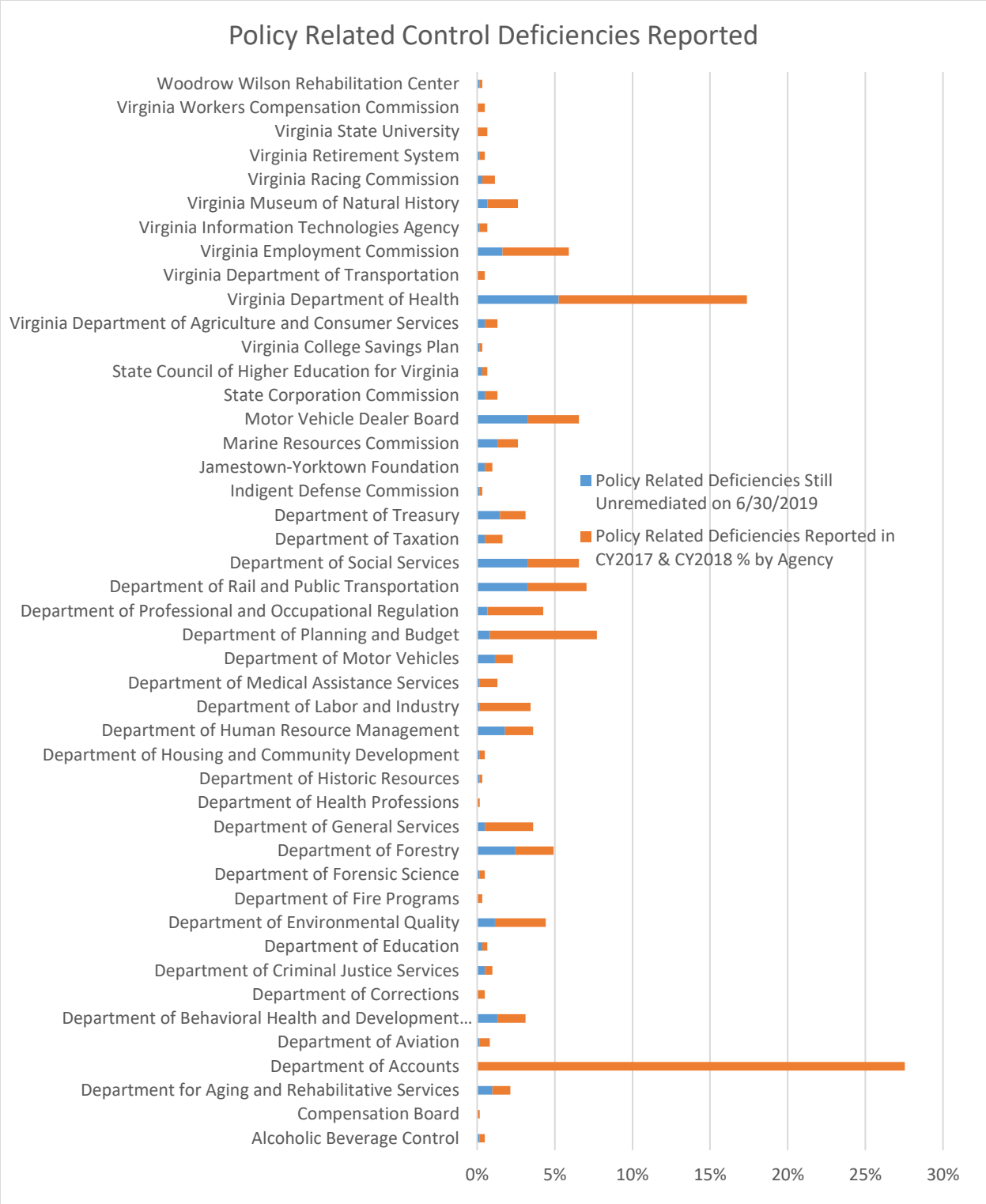

Figure 7: Policy Issues Reported by Agency

Technical Review Issues

CSRM also monitors when continued uncorrected issues exist that could operationally imperil 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 out-of-date and unsupported hardware or software that has reached its end-of-life. Often, the hardware or software is not updated because an agency is using a "legacy" or custom-developed application that will not function correctly on newer supported systems. Unsupported hardware or software that cannot be updated to operate securely poses a greater risk of being exploited and attacked (Figures 8 and 9).

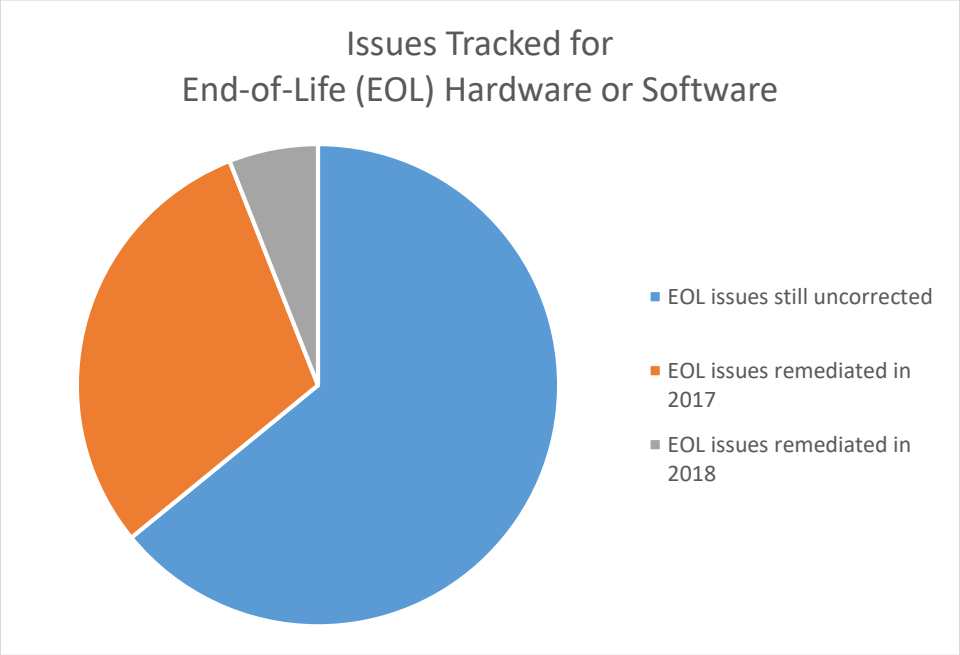

Figure 8: Issues Related to End-of-Life Hardware or Software

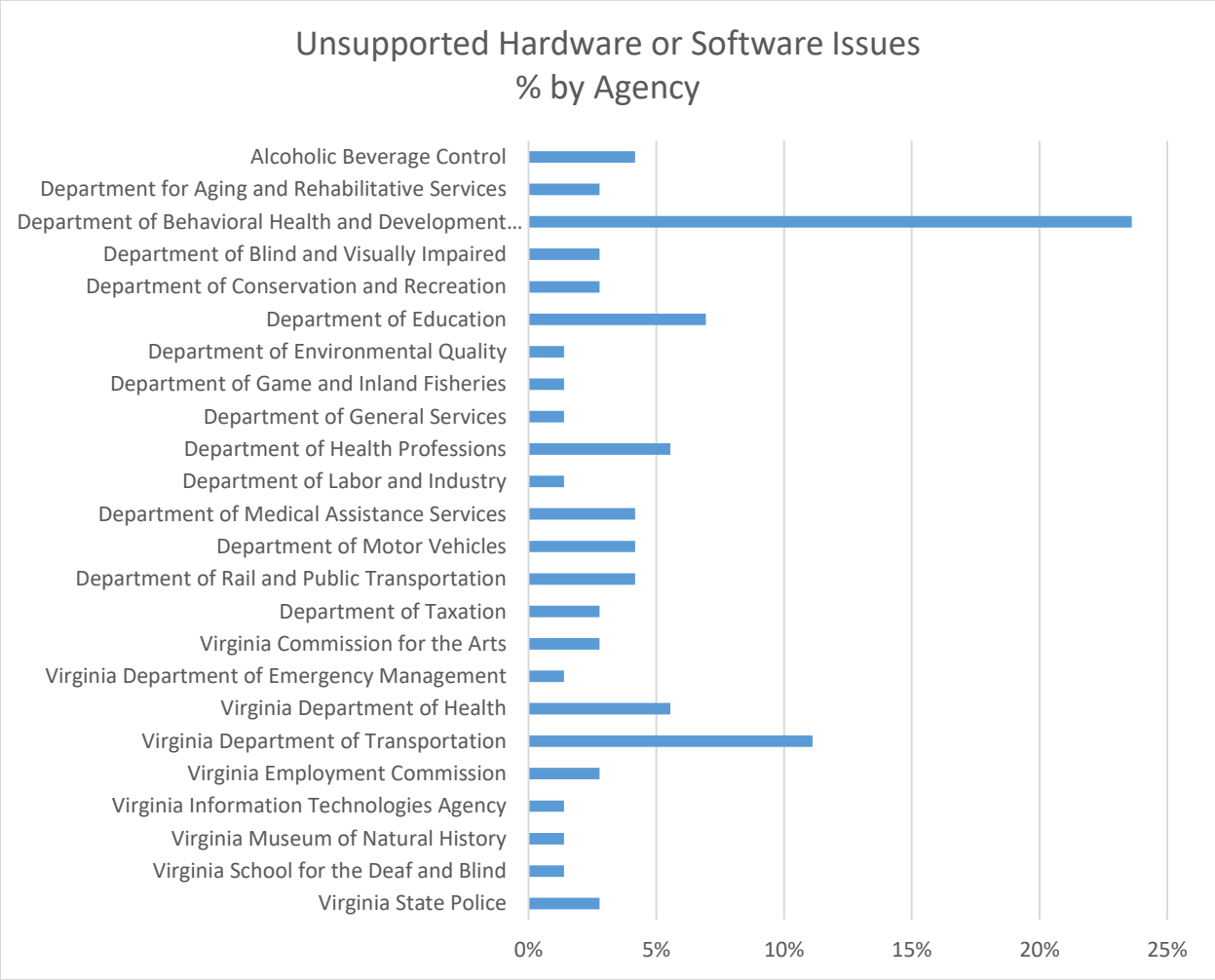

Figure 9: Chart depicts agencies that have had a significant percentage of unsupported hardware and software issues

National Cyber Security Review (NCSR) Analysis

Annually, the commonwealth participates in the NCSR, a self-assessment survey aligned within the NIST cybersecurity framework (CSF) to evaluate the commonwealth's cybersecurity posture and compare with other states. Each agency was asked to rank 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.

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.

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.

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.

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 lifecycle.

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 as slightly above or very close to the recommended minimum maturity level score of five in all five of the core cybersecurity functions. Commonwealth agency scores are also slightly above the score of other state agencies that participated in the survey (Figure 10).

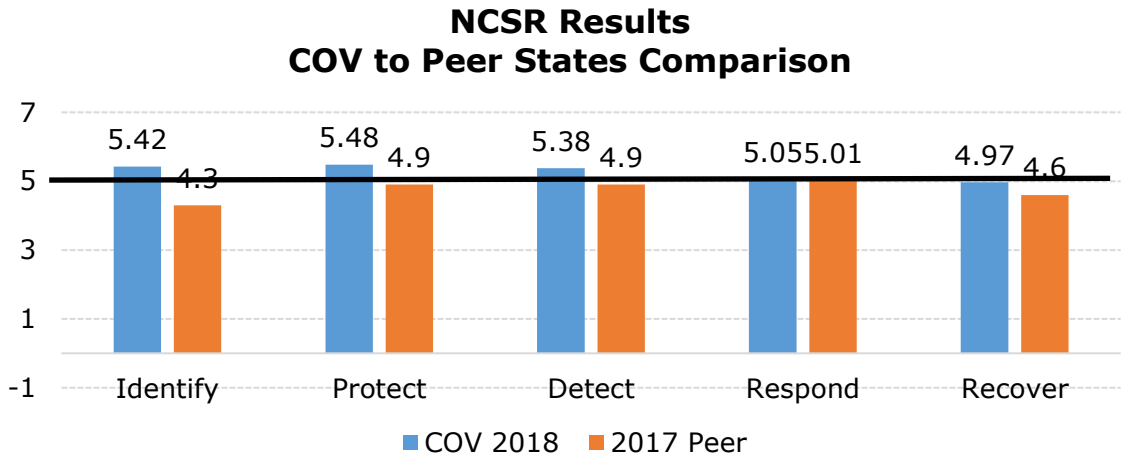

Figure 10: COV to Peer State Comparison for NCSR Results

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 were surveyed in the NCSR to determine if an organizational cybersecurity policy had been established and communicated. An organizational cybersecurity policy is a key component in assuring that an agency's cybersecurity culture, infrastructure and risk tolerance has been documented and is understood by its employees and contractors. Over half of the agencies indicated in their self-assessments that their organizational cybersecurity policy was either "optimized" (22%) or "tested and verified" (33%) (Figure 11a).

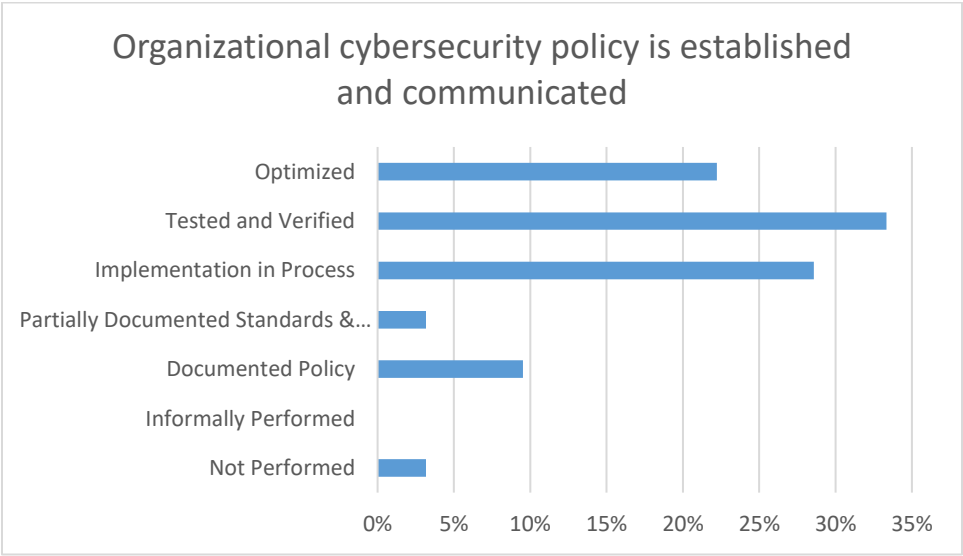

Figure 11: NCSR Results for Organizational Cybersecurity Policy

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. 16% of the agencies considered themselves "optimized" and 41% believe this area has been "tested and verified" (Figure 11b).

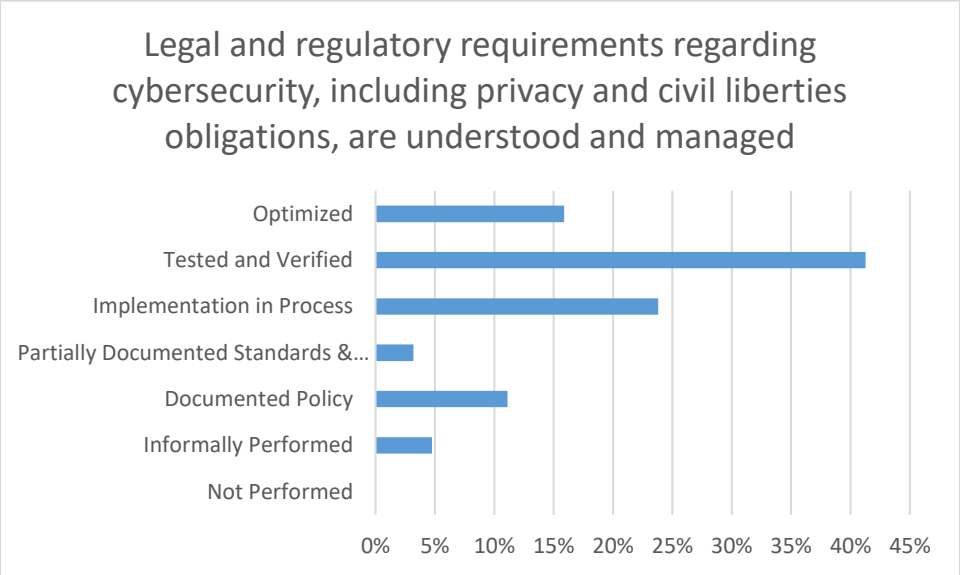

Figure 12: NCSR Results for Legal & Regulatory Requirements

Governance and risk management processes must address cybersecurity risks so that any potential issues or gaps in performance can be promptly identified and corrected. Overall, agencies scored themselves as performing well in this area (16% optimized and 37% tested and verified). In addition, 29% indicate that these processes are currently being implemented (Figure 11c).

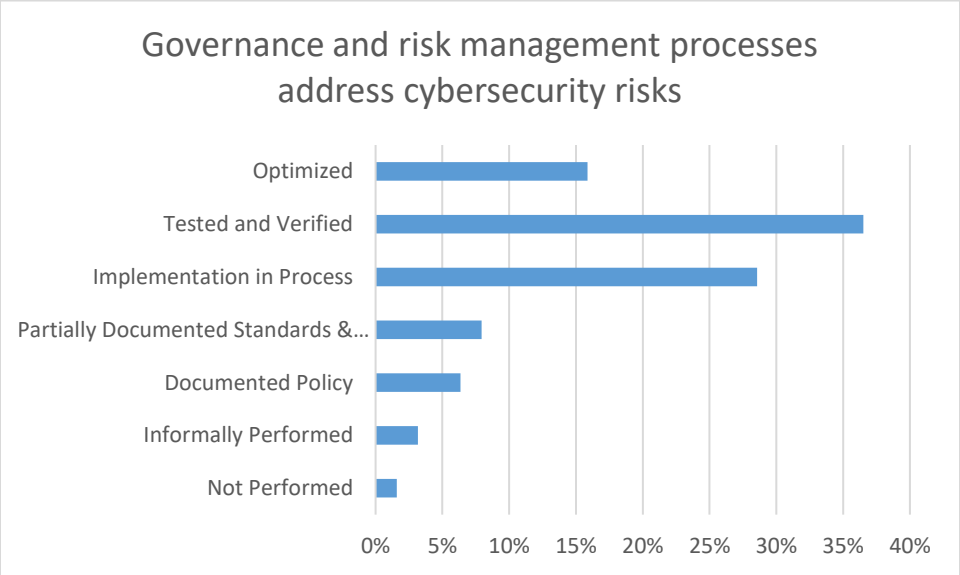

Figure 13: NCSR Results for Governance & Risk Management Processes

Agencies were also asked to scores themselves on how well they are complying with policies and regulations related to their physical operating environment. Maintaining adequate control over the operating environment provides assurance that organizational IT assets are protected and secured (Figure 11d).

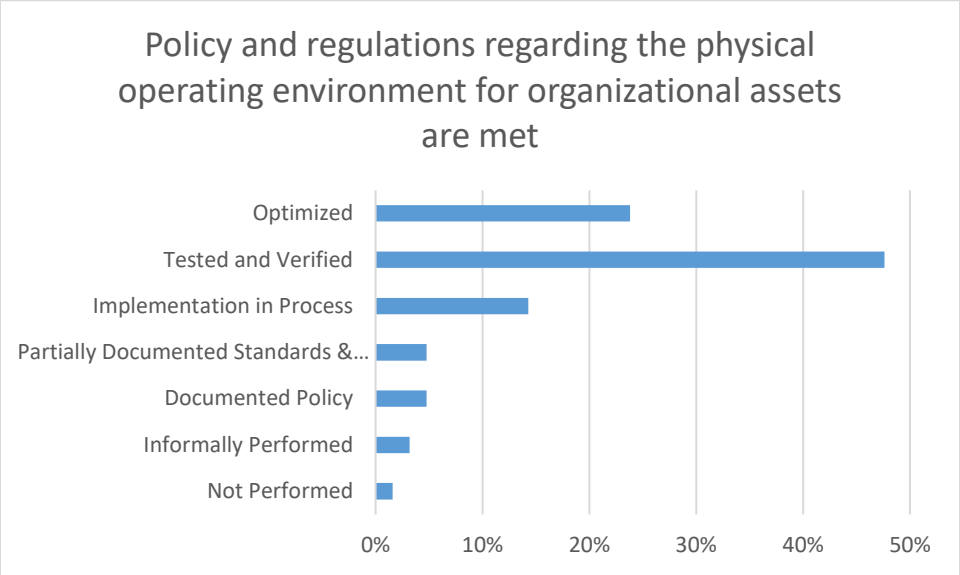

Figure 14: NCSR Results for Physical Access Policies

The majority of agencies measured their own performance for these particular policy-related activities as "optimized" or "tested and verified", indicating the two highest levels of maturity.

With some exceptions, the agency self-reported results on the NCSR generally aligns with the IT security risk ranking that CSRM is tracking for each agency. We compared the agencies that gave themselves the top overall scores on the NCSR survey with the report card results of VITA's most recent COV cybersecurity report (https://www.vita.virginia.gov/commonwealth-security/annual-reports/) (Figure 11e).

Agency	2018 NCSR Self-Assessment Score (highest to lowest)	COV 2018 Annual Cybersecurity Overall Report Card Score (average of Risk and Compliance scores)
Department of Small Business and Supplier Diversity	862	A
Department of Conservation and Recreation	842	A
Department of Accounts	840	A
Virginia State University	840	A
Virginia Information Technologies Agency	832	A

Department of Veterans Services	819	A
Department of Motor Vehicles	800	C
Office of State Inspector General	798	A
Virginia Retirement System	789	B
Department of Fire Programs	773	D
Virginia Department of Agriculture and Consumer Services	768	A
Department of Medical Assistance Services	764	C
Department of Treasury	764	A
Department of General Services	763	A
Department for Aging and Rehabilitative Services	756	A
Department for the Deaf and Hard of Hearing	756	A
Library of Virginia	748	C
Department of Health Professions	736	A
Department of Planning and Budget	736	A
Virginia Workers Compensation Commission	727	A
Department of Human Resource Management	722	B
Board of Accountancy	718	C
Gunston Hall	717	A
Department of Labor and Industry	703	A

Figure 15: Top 25 NCSR Agency Self-Assessment Scores compared to COV IT Security Annual Report Scores

Analysis of Cyber Incidents

CSRM identifies a cyber incident as an event that threatens to do harm, attempts to do harm, or does harm to the system or network. A cyber event is an observable occurrence in a system, network or workstation. Some example cyber events could be systems crashing and rebooting, unwanted emails bypassing firewalls or packets flooding the network. CSRM records these events to determine normal baseline activity. Activity aberrations that exceed norms are characterized as incidents for immediate incident response, investigation and remediating action.

CSRM records all incidents into its eGRC software. Within the eGRC, each incident is prioritized and categorized. Of particular concern for this report, were any incidents that caused or could have caused a breach of data or sensitive information. A data breach is the unauthorized access and acquisition of unredacted computerized data that compromises the security or confidentiality of personal information.

The chart below displays high priority IT security incidents reported in the last two calendar years by agency. Typically, large agencies, with lots of IT assets and more potential vulnerabilities that could be exploited had the most reported incidents (Figure 12).

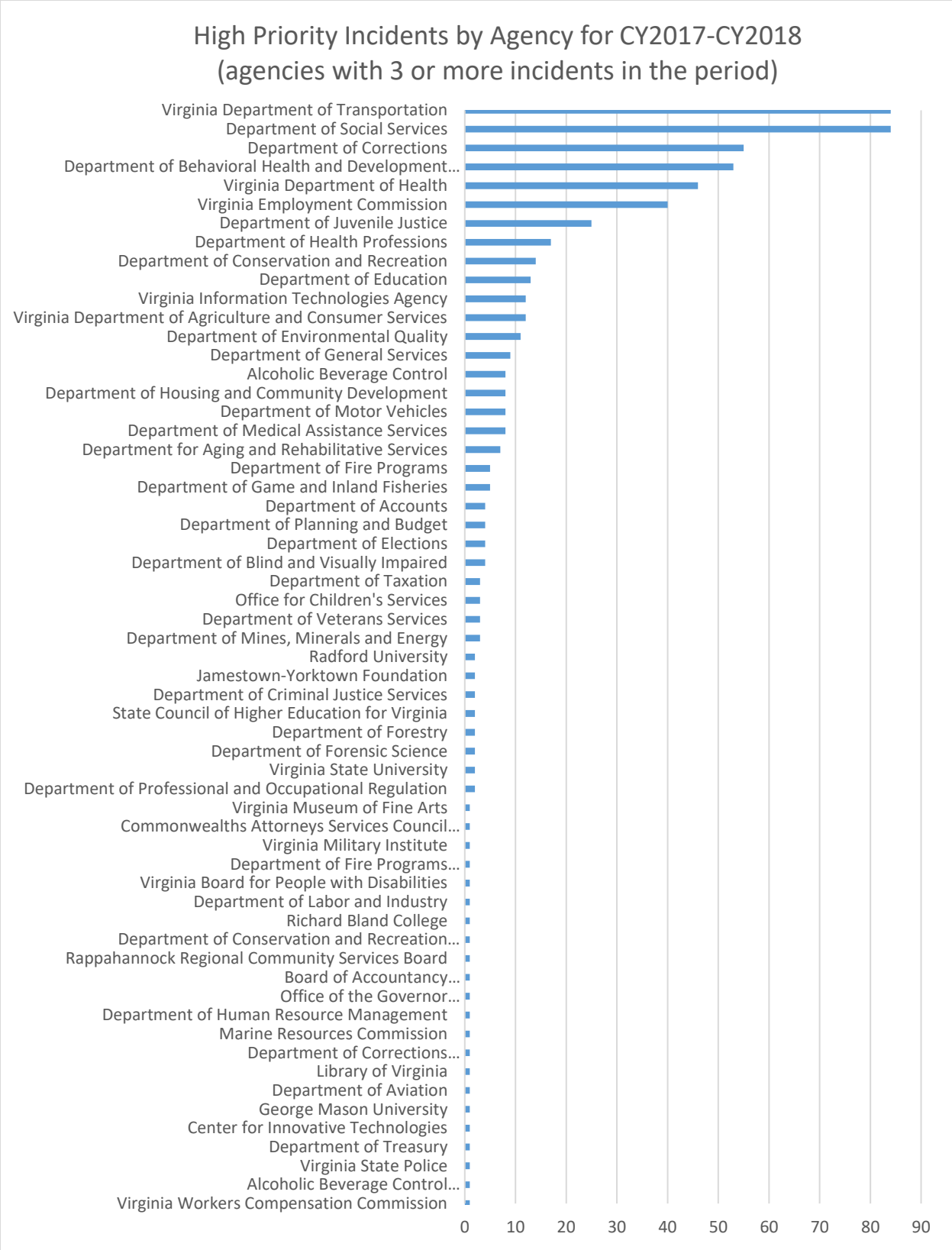

Figure 16: High Priority Cybersecurity Incidents by Agency

The top incident categories reported during the 2017-2018 period were analyzed. Malware, or malicious software, is the most reported type of IT security incident (Figure 13). Of major concern are any incidents that could lead to a breach of confidential commonwealth data.

The Ponemon Institute is a private research organization that conducts independent research on privacy, data protection and information security policy. In their 2018 annual report on the cost of a data breach, they estimate that that the **average total cost** of a data breach, the **average cost** for each lost or stolen record and the **average size** of data breaches have all increased beyond the 2017 report averages. In 2019, Ponemon estimated that each lost or stolen record from a public sector entity would cost that entity $75 per record. This could lead to a sizeable financial impact as well as negative publicity and a loss in confidence from citizens (https://www.ponemon.org/library).

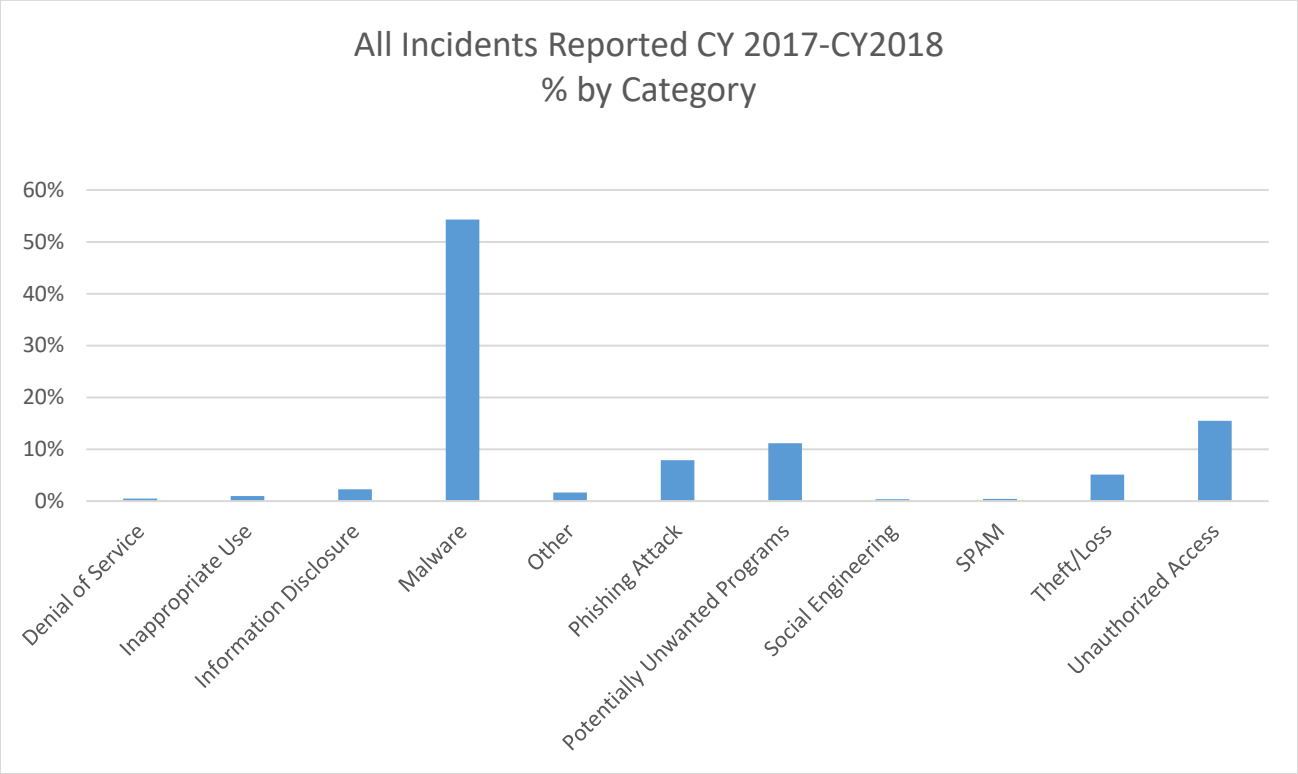

Figure 17: Cybersecurity Incidents by Category

Overall, the trend of incidents reported is showing a downward trend over the last two years (figure 14).

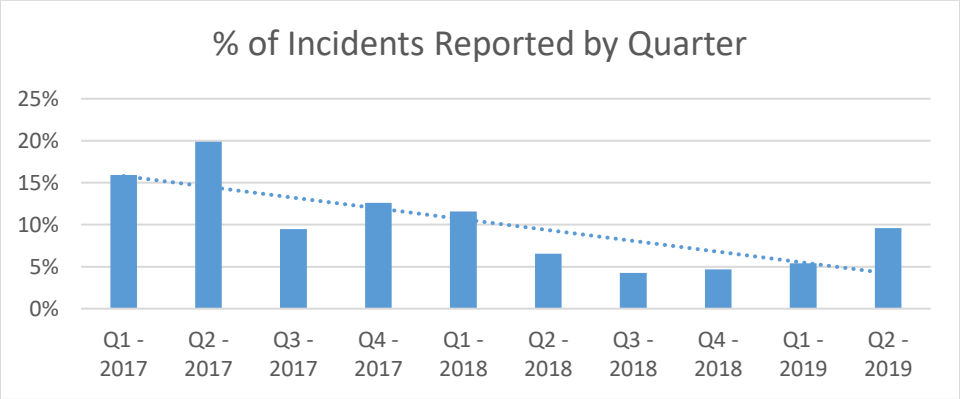

Figure 18: Cybersecurity Incidents by Quarter

Top Incident Categories

- Malware, or malicious software, is a serious threat and the most commonly identified incident. Malware can infect legitimate users' computers in order to damage the system or provide unauthorized access to sensitive data. Malware typically exploits known vulnerabilities in systems that are using unsupported hardware or software applications or systems that are not up to date or patched with the latest security updates.

- Incidents categorized as unauthorized access mean that someone gained or tried to gain access to system using someone else's account or by other methods. Unauthorized access also occurs when someone tries to gain access to an area of a system that they are not authorized to access or accesses data that they are not entitled to access or view.

- A potentially unwanted program (PUP) is a program that may be unwanted, even if the user consented to download and install it. PUPs may include spyware, adware, or dialers. PUPs can be implemented in a way that compromises privacy or weakens the computer's security.

- Theft/loss of a physical IT asset is a major concern, because a malicious party would have unlimited access and time to compromise the data contained on the system.

- Social engineering and phishing attacks are similar attacks in that they both use manipulation and deception to trick a user into divulging information, like passwords, or to take some other unauthorized action.

- "Unauthorized access: information disclosure" typically refers to the unintentional disclosure of confidential data. This could occur if sensitive information was sent unencrypted in email or by other means or stored in in an unsecured area in unencrypted format.

Category Analysis

Incident Categories: Malware and Unauthorized Access

The largest two incident categories are malware and unauthorized access. Commonwealth systems are frequently the targets of attackers who are trying to gain unauthorized access or install malware on our computers. Investigations show that they are often trying to exploit known software vulnerabilities using some type of malware attack. These vulnerabilities are often caused when systems are not configured correctly or are not updated or "patched" with the latest software and security updates. In November 2018, the commonwealth had five web servers compromised due to the attack exploiting a known vulnerability before the system was patched.

Cause: The primary driver for malware is poor cyber hygiene on systems. Cyber hygiene includes maintaining basic components of security that are mostly built into our processes today. Items such as maintaining strong passwords, keeping systems up to date, using least privilege, etc. A majority of the cyber hygiene issues in the commonwealth systems involve patching and updates. Patching is the process of keeping the hardware and software on a computer system updated to fix security vulnerabilities, bugs, or otherwise improve the system. Hackers are looking to exploit vulnerabilities in a system before vendors even have a chance to fix them. This is known as a "zero-day attack" and it's a very difficult exploit to prevent. So vendors frequently update their software, sometimes on a daily basis in order to stay ahead of the hackers. These patches in turn need to be installed on the affected systems in a timely and efficient fashion. Patches also need to be tested prior to installation to ensure that the update does not cause any undesired affect to the system or on the environment. The frequency of updates, the need to test updates and the urgency of many of these updates creates a cycle of near continuous patching across the commonwealth. The complication of the issue means that at times some agencies may not get all patches installed in a timely fashion. Often, it is a staffing issue when there is not enough trained IT staff available, often due to existing staff being stretched too thin. An un-patched system means that a vulnerability could exist that an attacker will try to exploit.

Policy requirement: The commonwealth's IT security standard has numerous requirements to manage IT systems by keeping software and hardware configured securely and updated timely. These requirements appear in several IT security control families, most notably in access control, configuration management,

planning, and systems information and integrity. In addition, IT security training, specifically "role-based" needed by IT administrators and developers, is required in the awareness and training family of controls.

Recommendations: Agencies need to review and update their policies to assure that these IT security control areas are addressed and communicated as well as ensure they are maintaining their systems to an adequate update level. Agencies must provide secure coding training to agency IT developers and staff so that agency developed applications can be better protected from unauthorized access.

In addition, patching for agency-specific applications should be included in the enterprise patch management system or agencies should have trained system administration staff and efficient patch management systems that will allow them to patch the agency specific applications in a secure and timely manner.

Finally, all systems must be routinely and continually monitored for vulnerabilities. VITA provides a vulnerability scanning service for all web application and our IT service providers are continually scanning the internal devices on our networks. These scans can identify when systems are not configured to secure baseline "norms" or are using hardware or software that is out of out of date and requires patching or replacement. Agencies should plan to replace end-of-life and non-supported systems as soon as possible.

Incident Categories – Theft/loss

Theft/loss of a physical IT asset is a major incident category. It is of particular concern because a malicious party often has unlimited access and time to compromise the data contained on a lost or stolen system.

Cause: Typically, theft or loss, involves a portable or movable devices such as a laptop or smartphone. Users can be careless and inattentive, leaving those devices unsecured and left behind in an area such as a car or public place.

Policy requirement: By policy, mobile devices must be encrypted. Encryption renders the data on the device unreadable and unusable to anyone but an authorized user. However, when a device is reported lost or stolen, there is always uncertainty that the encryption policy is being adequately enforced and other access controls on the device are implemented and working correctly.

Recommendations: Agencies must assure that they have policies in place that address physical protection of IT assets and employee responsibilities. Protection of devices and media in the possession of commonwealth users' needs to be addressed in IT security awareness training, so that users are fully aware of their responsibilities for protecting those assets. In addition, all users need training on other security controls related to their devices, such as access control, backup controls, and encryption controls. IT management at each agency needs to ensure that an accurate IT inventory is maintained, that users are trained, and that all policies are being followed.

Incident Categories – "Social engineering" and "phishing attacks"

Social engineering and phishing attacks are two methods which use manipulation and deception to trick users into divulging information to attackers.

Cause: Commonwealth users are frequently targeted by phishing attempts and social engineering attacks. Users, in general, can sometimes be too trusting, clicking on links and pop-ups without fully understanding the potential dangers. Successful phishing and social engineering ploys can allow malicious software to enter into our computers and networks.

Policy requirements: Per the commonwealth's IT security standard, each agency must have policies that specify provide training for employees and contractors on protecting passwords and data (Awareness and Training control family).

Recommendation: Policy requirements need to be routinely communicated to all staff. Comprehensive and reoccurring security awareness training must be provided to each commonwealth employee and contractor on their responsibilities.

Ransomware

Ransomware is one type of malicious software that we are seeing more frequently. Ransomware is designed to deny access to a computer system or data by making the data unusable by encrypting it until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.

Ransomware can be devastating to an organization and government entities are frequent targets. In addition, recovery after a successful ransomware attack can be a difficult process that may require the services of a data recovery specialist, and in some cases, victims have paid to recover their files. However, there is no guarantee that victims will recover their files if they pay the ransom.

In addition to an increase in the number of ransomware attacks over the last two years, the perpetrators have also discovered that attacking government entities has been successful. In particular, local governments are frequently attacked but there have also been successful attacks on agencies in other states.

It has been reported that two-thirds of all publicly known and successful ransomware attacks have targeted state or local governments. According to the U.S. Conference of Mayors, at least 22 such attacks have been noticed in the first half of 2019.

Some cities, like Washington, Pennsylvania, Lake City, Florida, and Riviera Beach, Florida, have agreed to pay nearly $1.1 million collectively to ransomware attackers.

Some victims have refused to pay. Baltimore refused to pay $75,000 in bitcoin to decrypt their data in May 2019. Atlanta also refused to pay $52,000 in bitcoin a year earlier. Both cities were able to recover their data from the incidents without

paying ransom but at an estimated cost of over $18 million for Baltimore and $17 million for Atlanta in recovery efforts.

After seeing only a few ransomware incidents in 2017 and 2018, we have so far seen 13 attempted ransomware attacks in the first six months of calendar year 2019 (Figure 15). CSRM has been scheduling training for agency ISOs that will simulate ransomware attacks and get them familiar with detecting and containing such attacks as early as possible.

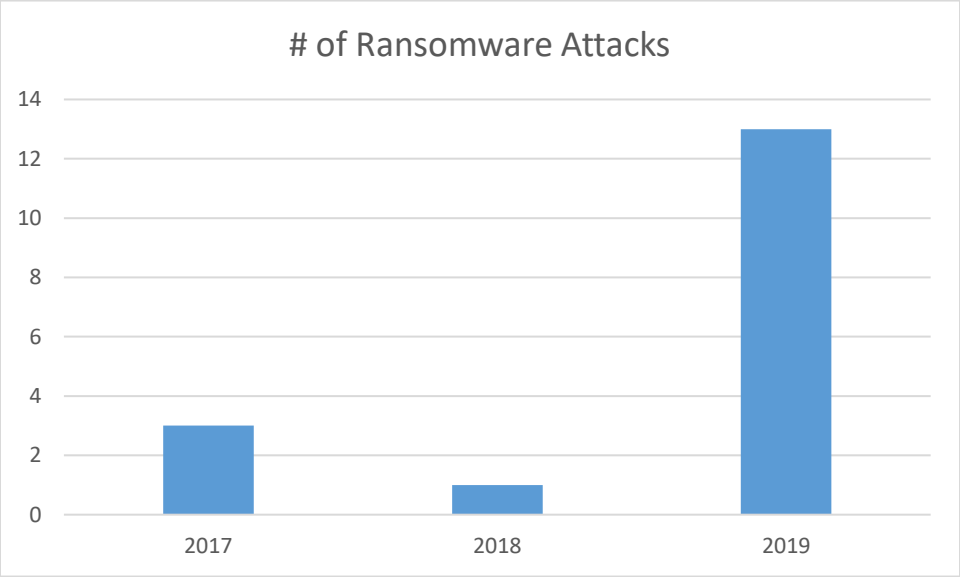

Figure 19: # of Ransomware Attacks on the COV

Investigations

Investigations are started when it's uncertain whether or not an actual IT security incident has occurred.

A frequent type of investigation is when an employee or contractor is suspected of using IT resources in an unauthorized manner. When this is suspected, CSRM will initiate an investigation to determine the merits of the complaint.

Other investigations are often started as a result of information provided to CSRM from other cooperating entities. Organizations such as the Multi-State Information Sharing and Analysis Center (MS-ISAC), the Spamhaus Project, the Center for Internet Security, and law enforcement agencies, provide CSRM with alerts related to new phishing, malware and hacking attempts that may be affecting the commonwealth or commonwealth employees. In addition, CSRM receives reports whenever any commonwealth employee's email address or other identifying credential or personal information is located in certain websites that are known to collect and share this type of information without authorization (Figure 16).

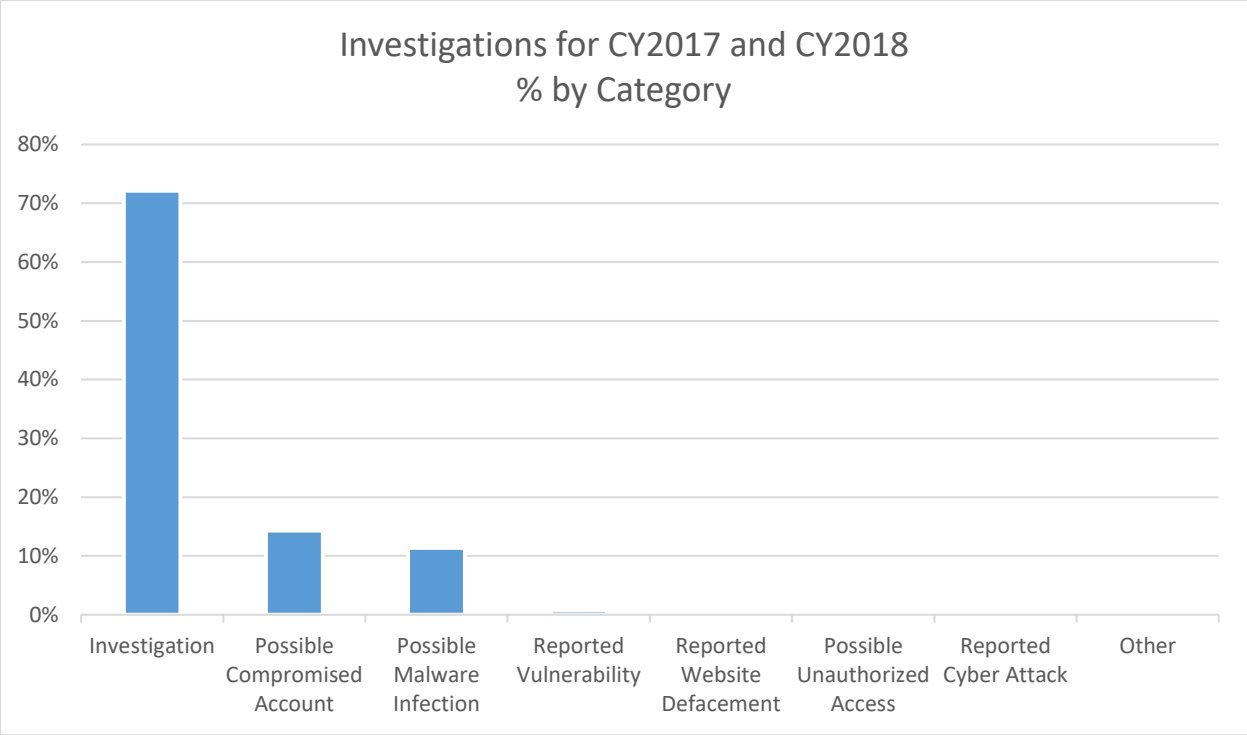

Figure 20: Cybersecurity Investigations by Category

Incident Response

The commonwealth utilizes laws and policies to describe what constitutes a cyber incident, what criteria is used to evaluate the severity of an incident and defines the roles and responsibilities of agencies tasked with responding to an incident.

When a cyber incident occurs, agency directors are required by §2.2-603 to report them to VITA within 24 hours of discovery. Incidents can be reported 24/7 using an online incident reporting form or by calling the commonwealth's help desk service (https://www.vita.virginia.gov/commonwealth-security/incident-reporting/). Timely reporting of cyber incidents is critically important. Studies have shown that the time it takes to compromise an asset can typically be measured in seconds or minutes. However, the discovery time is likelier to be in terms of weeks or months. The longer the discovery time, the more damaging the breach can be and the costlier it will be to correct and contain.

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

Conclusion

Cybersecurity in the commonwealth is a process that has no finish line. The ongoing process of mitigating IT security risks to the commonwealth takes place continually. Cybersecurity cuts across many issues and involves numerous stakeholders.

VITA uses its governance position over cybersecurity to continually monitor, manage and improve IT security. VITA is constantly identifying and reviewing cybersecurity issues and adjusting policies, procedures and processes to address cybersecurity priorities.

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