REPORT OF THE VIRGINIA INFORMATION TECHNOLOGIES AGENCY

Ransomware Study Report (HJR 64, 2020)

TO THE GOVERNOR AND THE GENERAL ASSEMBLY OF VIRGINIA

HOUSE DOCUMENT NO. 4

COMMONWEALTH OF VIRGINIA
RICHMOND
2021

VIRGINIA IT AGENCY

RANSOMWARE STUDY REPORT (2020 HJ 64)

vita.virginia.gov

January 13, 2021

Ransomware Study Resolution

In its 2020 Session, the General Assembly recognized the threat that ransomware poses to the Commonwealth of Virginia by passing House Joint Resolution 64 (HJ64). The resolution directed the Virginia Information Technologies Agency (VITA) to study the Commonwealth's ransomware attack preparedness. The resolution specified that VITA shall:

(i) assess the Commonwealth's susceptibility to ransomware attacks at the state and local levels of government;
(ii) develop guidelines and best practices to prevent ransomware attacks;
(iii) evaluate current data encryption and backup strategies;
(iv) evaluate the availability of tools to monitor unusual access requests, viruses, and network traffic;
(v) develop guidance for state agencies and localities on responding in the event of a ransomware attack;
(vi) develop a coordinated law-enforcement response strategy that utilizes forensic investigative techniques to identify the source of ransomware attacks; and
(vii) provide recommendations on legislative or regulatory changes to better protect state and local government entities from ransomware.

This report provides the information that VITA was directed to study in the resolution.

Table of Contents

Ransomware Study Resolution 1
Table of Contents 2
Table of Figures 3
Executive Summary 5
Key takeaways and recommendations 5
Susceptibility to ransomware attacks in Virginia 7
The National Cybersecurity Review (NCSR) 8
The Virginia National Cybersecurity Review (NCSR) Results 10
Ransomware survey results and analysis: The threat of ransomware 12
Ransomware survey results and analysis: Top challenges 15
Guidance on preparing for ransomware 16
Ransomware Preparedness and Prevention 18
Cybersecurity insurance 18
Ransomware survey results and analysis: Cybersecurity insurance 19
Security training 20
Ransomware survey results and analysis: Security training 21
Ransomware prevention strategies 24
Ransomware survey results and analysis: Authentication and other security measures 24
Data encryption strategies 25
Ransomware Detection 27
Network monitoring 27
Ransomware survey results and analysis: Network monitoring 28
Forensic investigative techniques 30
Ransomware survey results and analysis: Forensics 30
Ransomware Recovery 32
Data Backup Strategies 33
Ransomware survey results and analysis: Backups 33
Ransomware Response 34
Security incident response 35
Ransomware survey results and analysis: Security incident Response 39
Evaluating Paying the Ransom 42
Commonwealth Ransomware Response Strategies 43

Existing Security Incident Response Framework 43
Leverage Department of Homeland Security tools 45
Law enforcement response strategies 46
Legislative and regulatory recommendations 47
Administrative law recommendations 47
Current Virginia criminal laws 47
Criminal law recommendations 48
Regulatory recommendations 48
Conclusion 49
Appendix – Report Methodology and Further Resources 51
Report methodology 51
Decryption Tools 52
Ransomware prevention advice 52
Ransomware Response and Prevention 52
MS-ISAC Ransomware Guide 2020 52
Backup Options 52
Protecting and Planning 52
Einstein Project 52
Cyber Insurance Cyberscoop 53
Ransomware Survey 53
Security Checklist for implementing ransomware best practices 54
Types of ransomware 55
Ransomware study committee members 57

Table of Figures

Figure 1: NCSR score for COV agencies compared to other states' agencies 11
Figure 2: Commonwealth localities compared to peer localities in other states 11
Figure 3: COV agencies compared to COV localities 12
Figure 4: Threat of ransomware 13
Figure 5: Ransomware threat by type of entity 13
Figure 6: Reported ransomware attacks 14
Figure 7: Reported ransomware attacks by entity type 15
Figure 8: Use of cyber insurance 15
Figure 9: Cyber insurance by entity type 20
Figure 10: Right type and amount of cyberinsurance 20
Figure 11: IT security awareness training 22

Figure 12: IT security awareness training by entity type 22
Figure 13: IT security awareness training for contractors 23
Figure 14: IT security awareness training for contractors by entity type 23
Figure 15: Is two-factor authentication in use in your organization 25
Figure 16: Unauthorized access prevention for remote access by entity type 25
Figure 17: Data encryption strategies in use 26
Figure 18: Continuous monitoring 28
Figure 19: Continuous monitoring by entity type 29
Figure 20: Reporting on exploits & vulnerabilities 29
Figure 21: Exploits & vulnerabilities reporting by entity type 30
Figure 22: Cybersecurity & forensic capabilities 31
Figure 23: Cybersecurity & forensic capabilities by entity type 31
Figure 24: Frequency of backups 34
Figure 25: Frequency of backups by entity type 34
Figure 26: IT security incident response plans 39
Figure 27: Security incident response plans by entity type 40
Figure 28: Percentage of organizations with law enforcement reporting policy 41
Figure 29: Percentage of organizations with law enforcement reporting policy by entity type 42

Executive Summary

Ransomware is a type of malicious software that infects a system or device and denies the owner or administrator access until a ransom is paid. Infections typically occur via phishing emails, poorly-secured network and services or vulnerabilities in infected websites.

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.

Key takeaways and recommendations

- Improve cybersecurity programs to target the reduction of ransomware risk. The data and analysis indicates that work needs to be done both at the state and local levels to reach program maturity levels to avoid and mitigate the effects of infection.

- Establish reporting requirements and accountability for the effectiveness of information security programs for all government entities. The data collected shows an extremely concerning lack of maturity in cybersecurity programs in localities and other organizations. The dramatic increase in ransomware infections at the local and school level reflect the large number of insufficient security programs. The analysis of the data indicates that cybersecurity programs and the resources needed to address deficiencies in those programs are not prioritized.

- Establish formal security incident reporting requirements for all government entities. In order to understand and identify how to respond to security incidents it is necessary to know that incidents are occurring. Requiring the reporting of security incidents will help to identify what steps are necessary to mitigate cyber threats such as ransomware.

- Increase cybersecurity resources (human and financial). Unsurprisingly, the biggest challenge for organizations is funding and personnel for preparedness and response. Introducing options for cost-sharing services and funding to implement security programs is essential. If possible, tying funding to maturity, sustainment of a program, and reporting to an independent party would help the programs progress. For several years now, Commonwealth policymakers have recognized the challenge of growing and developing Virginia's cybersecurity workforce. This year, the Governor's introduced budget adds three security positions at VITA to support state cybersecurity, two security incident personnel and a cloud security architect. Efforts to increase the number and capabilities of cybersecurity personnel must continue, and state and local government must be able to hire and retain capable and qualified personnel.

- Establish a designated body to handle cybersecurity incident reports for all government entities. When an organization is compromised the Commonwealth is often not informed

about the event. This results in the state not being aware of the impact to critical infrastructure, state technology or other connected systems associated with a compromise. Establishing a reporting body will allow stakeholders to have insight about incidents involving government systems and improve the incident response outcome.

- Increase cybersecurity training for all personnel. It is essential to establish a culture of cybersecurity and preparedness. Doing so will drive awareness of foundational cybersecurity concepts, common cyber threats, and how to respond appropriately, suspicious activity. Training that is reinforced frequently and engages personnel on an ongoing basis is effective at developing a culture of cybersecurity awareness. For example, a program that simulates phishing and tests employee responses regularly will be more effective than a once-a-year webinar.

- Invest in current, manageable cybersecurity technology and practices. Achieving and maintaining current technology is an ongoing challenge for state and local government, but key security measures and technology are critical in preventing and responding to ransomware. Continuous network monitoring, regular vulnerability assessments, tested backups, and good authentication and permissions practices contribute to a strong cybersecurity program. In this complex, interconnected age, cybersecurity cannot be achieved by simply installing anti-malware software.

- Improve the sharing of information and resources available to localities. Local governments and school systems need assistance when preparing and responding to ransomware. Providing them information on state, federal and industry resources available can ease the burden and improve security. Educating local governments and school systems will provide knowledge necessary to prevent attacks as well as shorten the time frame for recovery if compromised. State and local governments can make a more secure environment by working together.

Susceptibility to ransomware attacks in Virginia

Ransomware is a widespread and increasing threat. *Government Technology* magazine called the surge in successful, targeted ransomware attacks against governments and hospitals the top 2019 cybersecurity story,[1] and Virginia's experience bears that out. After seeing only a few ransomware incidents in 2017 and 2018, there were 13 attempted ransomware attacks in the first six months of 2019.

According to a study released by Deloitte's Center for Government Insights, there is rising trend in ransomware attacks on state and local governments generally.[2] The report indicates that in 2019 alone, governments reported 163 ransomware attacks with more than $1.8 million dollars in ransoms paid and tens of millions of dollars spent on recovery costs, a nearly 150% increase in reported attacks from 2018.

As the increase in the numbers of ransomware attacks over the last two years suggests, the perpetrators have discovered that attacking government entities is a successful enterprise. *StateScoop* reports that two-thirds of all publicly known and successful ransomware attacks have targeted state or local governments.[3]

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.[4] As Deloitte's report mentions, refusing to pay ransom demands may be good in principle, but it also may be far more expensive. For example, the City of Baltimore refused a $76,000 ransom demand, only to suffer over $18 million in recovery costs and lost revenues. The perpetrators of ransomware are aware of and exploit that difficult choice, sometimes describing their attacks as a business and customizing the amount of the ransom to fit the target and incentivize payment.

---

[1] "2019: The Year Ransomware Targeted State & Local Governments," by Dan Lohrmann, *Government Technology*, at https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2019-the-year-ransomware-targeted-state--local-governments.html (Dec. 23, 2019).
[2] "Ransoming Government," Deloitte Center for Government Insights, at https://www2.deloitte.com/us/en/insights/industry/public-sector/government-ransomware-attacks.html (March 11, 2020).
[3] "Report: Two-thirds of ransomware attacks in 2019 targeted state and local governments," *StateScoop*, at https://statescoop.com/report-70-percent-of-ransomware-attacks-in-2019-hit-state-and-local-governments/ (August 28, 2019).
[4] "Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase," CoveWare, at https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report (August 3, 2020).

Ransomware can be a particularly powerful weapon against governments, which must provide public services and cannot afford, financially or civically, to have data compromised to the point of governance paralysis.[5]

Multiple factors contribute to ransomware's growing threat.[6] 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 of information technology (IT) security talent. A CyberEdge Group report found that 85% of organizations are experiencing a shortfall of skilled IT security personnel,[7] 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 and local governments due to fiscal restraints.

The **National Cybersecurity Review (NCSR)**

The NCSR is an annual survey sponsored by the Department of Homeland Security (DHS) and the Multi-State Information Sharing and Analysis Center (MS-ISAC) designed to determine the maturity level of a cybersecurity program of state, local and tribal territory government participants. The survey is built on the National Institute of Standards and Technology (NIST) cybersecurity framework (CSF). The results of the survey show the strengths and weaknesses of a cybersecurity program.

The NIST Cybersecurity Framework is grouped into areas of focus to understand the maturity of the processes and technologies in place supporting an information security program. Each area has an objective ranging from preparation activities to recovery from a successful attack. Scoring in each of the five categories helps understand deficiencies in a program and the likely risks to an organization. The recommended maturity level for each of these areas is a five. This level should be adequate, in most situations, to both prevent and recover from a ransomware attack.

[5] "The State of Ransomware In the US: Report and Statistics 2019," Emsisoft, https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/ (updated December 31, 2019).
[6] "Ransoming Government," Deloitte Center for Government Insights, at https://www2.deloitte.com/us/en/insights/industry/public-sector/government-ransomware-attacks.html (March 11, 2020).
[7] "2020 Cyberthreat Defense Report," CyberEdge Group, at https://cyber-edge.com/wp-content/uploads/2020/03/CyberEdge-2020-CDR-Report-v1.0.pdf (March 2020).

The five main cybersecurity functional areas surveyed in the NCSR are:

- Identify

  "Identify" tends to be one of the lowest-rated functions. Immature capabilities in the "Identify" function may hinder an entity's ability to effectively apply risk management principles for cybersecurity. By incorporating sound risk management principles into cybersecurity programs, entities will be able to continuously align their efforts toward protecting their most valuable assets against the targeted risks, such as ransomware attacks.

- Protect

  The activities under the "Protect" function pertain to different methods and activities that reduce the likelihood of cybersecurity events and ensure that the appropriate controls are in place to deliver critical services. These controls prevent cybersecurity events from occurring through common attack vectors, including attacks targeting users and attacks leveraging inherent weakness in applications and network communication.

- Detect

  The quicker an entity is able to detect a cybersecurity incident, the better positioned it is to remediate the problem and reduce the consequences of the event. Activities found within the "Detect" function pertain to an entity's ability to identify incidents. These controls are becoming vitally important as the quantity of events occurring within an environment can be overwhelming to handle. In reviewing logs for evidence of a successful attack, it is imperative that the cybersecurity team understands the entity's normal operating baseline. This baseline knowledge is the foundation to being able to successfully identify key concerns. Through rapid detection, the cybersecurity team can implement additional controls to protect devices from being impacted by the ransomware attack.

- Respond

  An entity'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 entity plans, analyzes, communicates, mitigates, and improves its response capabilities. For many entities, integration and cooperation with other partners is key. Locality entities in particular do not appear to have sufficient internal resources to handle all components of incident response.

- Recover

  Activities within the "Recover" function pertain to an agency's ability to return to normal operations 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 cycles.

NCSR survey participants respond to a series of questions related to each of these five functional areas. The survey utilizes a "maturity" scale to assess how an organization addresses the different activities supporting these functions. The table below provides a breakdown of the NCSR maturity level scale along with the scores associated with each maturity level.

Score	Maturity Level *The recommended maturity level is set at a score of 5 and higher.*
7	**Optimized**: The organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	**Tested and Verified**: The organization has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	**Implementation in Process**: The organization has formally documented policies, standards, and procedures and are in the process of implementation.
5	**Risk Formally Accepted:** The organization has chosen not to implement based on a risk assessment.
4	**Partially Documented Standards and/or Procedures:** The organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy.
3	**Documented Policy:** The organization has a formal policy in place.
2	**Informally Performed:** Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.
1	**Not Performed**: Activities, processes and technologies are not in place to achieve the referenced objective.

The Virginia National Cybersecurity Review (NCSR) Results

VITA requires executive branch agencies to participate in the survey each year. The individual agency results are provided in the Commonwealth of Virginia Annual Security Report (https://www.vita.virginia.gov/commonwealth-security/annual-reports/). This analysis includes information from the executive branch NCSR, combined with locality NCSR data provided by the MS-ISAC. The 2019 NCSR survey included participation from 212 total organizations in the Commonwealth of Virginia. Of these participants, 70 were state agencies, 141 were local governments and one was a higher education facility. The local government participation represented 67% of all local governments within the Commonwealth.

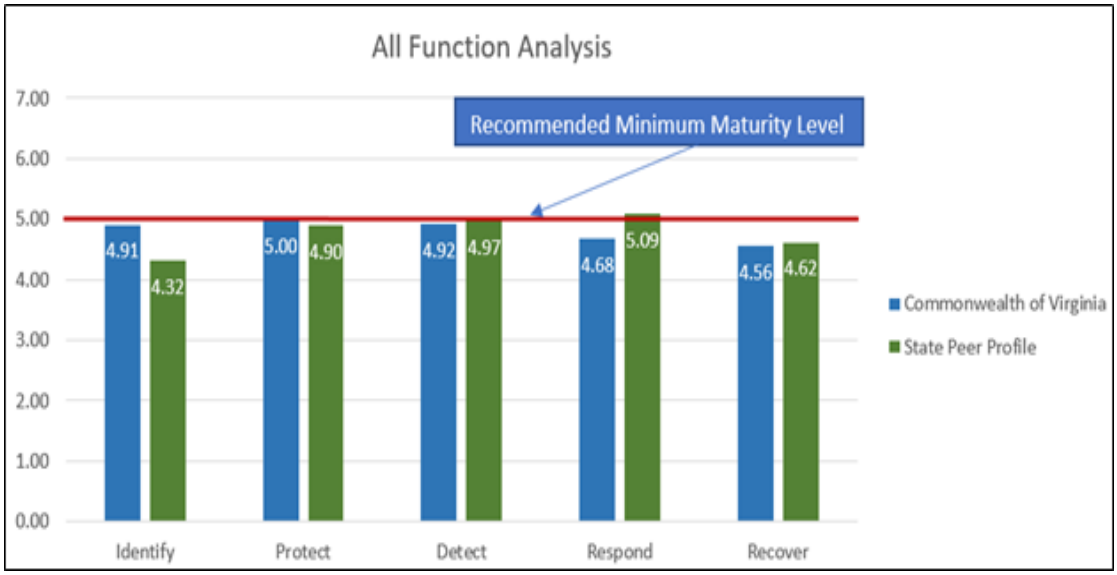


Figure 1: NCSR score for COV agencies compared to other states' Agencies

Virginia's state agency cybersecurity framework performance compared to other states is shown in Figure 1. All areas except "Respond" are ahead of or close to the maturity level in other states. Three of the five categories are approaching the target recommended maturity level, and the remaining two areas have been identified as areas needing additional resources for progress.

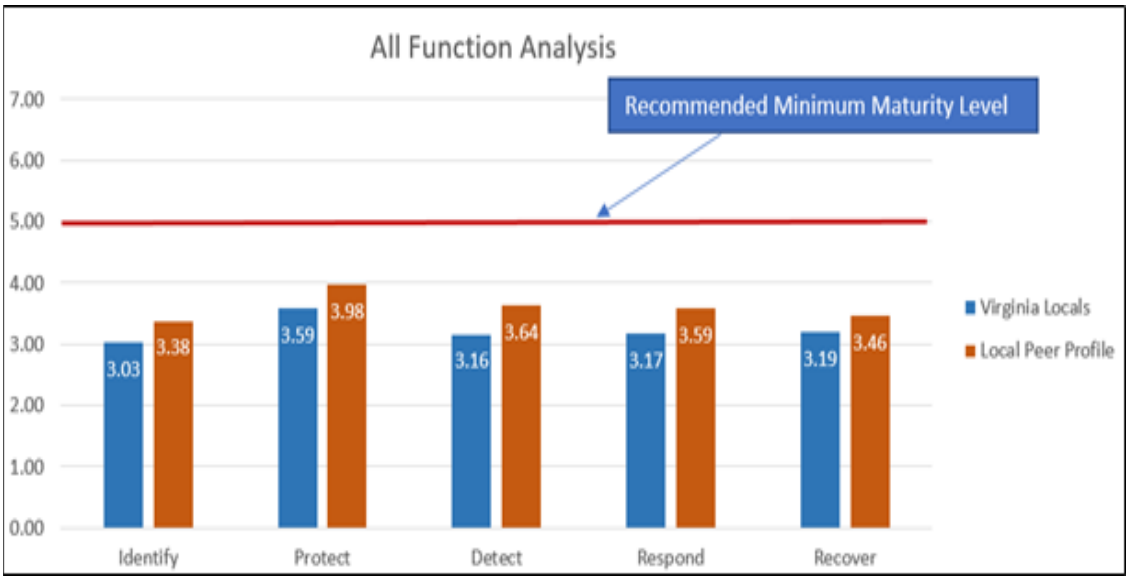


Figure 2: Commonwealth localities compared to peer localities in other states

The scores at the locality levels are significantly more concerning. Virginia localities are not only behind their peers they are also very far below the recommend maturity level. Virginia local governments scored approximately 10% lower than the 3.61 average for other local government participants. According to the review, most Virginia local governments have formal policies in place but have not made much progress in implementing the tools and processes needed to support those policies. Effectively, most organizations are indicating a desire for an information

security program but do not have the controls in place to actually protect their environment. Based on this information a majority of the localities surveyed are likely at significant risk of, not only infection by ransomware, but also would be unable to respond or recover in a timely manner from a compromise.

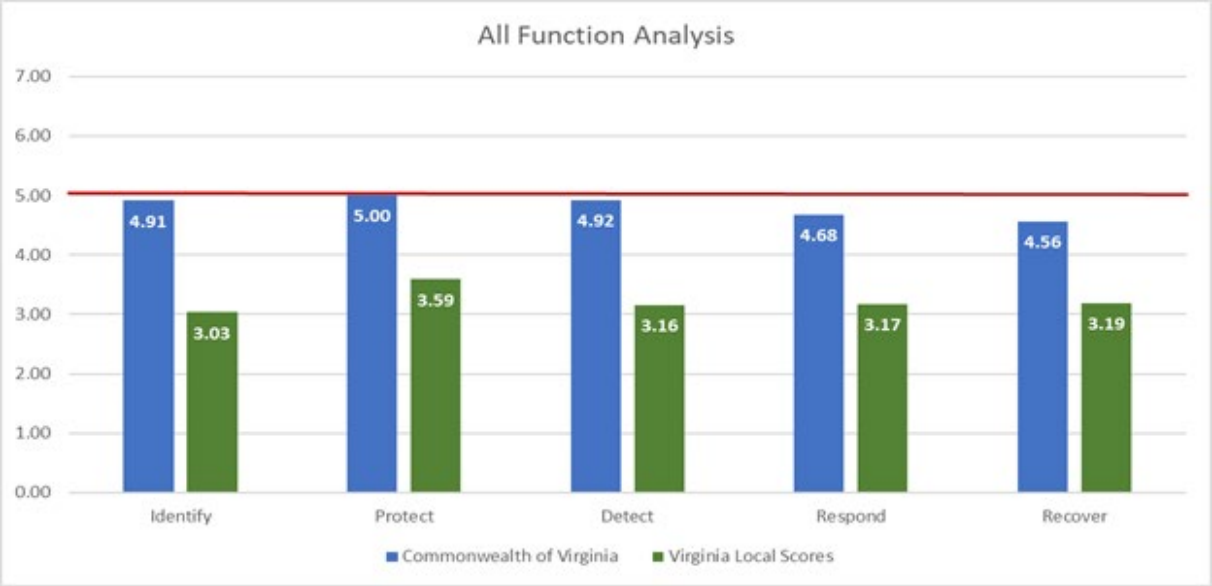


Figure 3: COV Agencies compared to COV Localities

In summary, the NCSR results are alarming and indicate a high probability of significant impact if a locality experiences a ransomware attack. The combined lack of ransomware preparedness, detection and ability to recover could prevent impacted locality government services from functioning for extended periods of time. The lack of information security program maturity means a ransomware attack could result in the affected entity electing to pay the ransom in order to recover data. Not only would this broadcast to bad actors that Virginia's data can be held hostage, but it would also erode citizen confidence in the organization's ability to perform its duties.

The Commonwealth's state government appears to be faring better than localities. The state is approaching the recommended minimum maturity level, however there are some areas that need improvement. Both "Respond" and "Recover" will need further analysis to identify what will bring the scores up to the recommended level. VITA will perform that review for the 2020 annual security report.

Ransomware survey results and analysis: The threat of ransomware

To obtain insight into how each organization perceived their susceptibility to ransomware, the team asked organizations to rate the perceived level of threat that ransomware is to their environment. The answer should represent how prepared the organization perceives it is in the case it experiences a ransomware attack. More than 75% of respondents indicated that

ransomware was very much a real threat to their organization. This number reinforces the results from the NCSR which indicated that many feel unprepared for a ransomware attack.

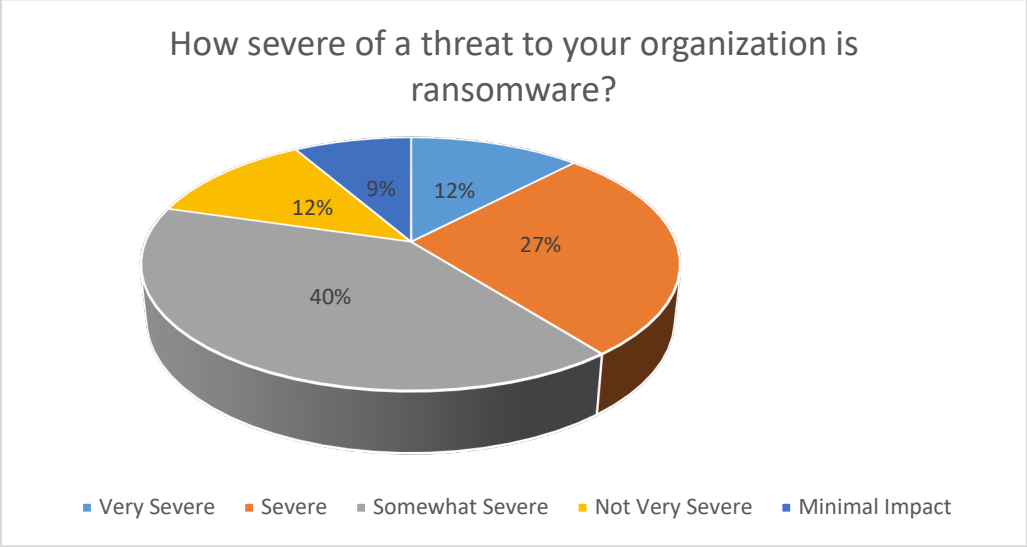


Figure 4: Threat of ransomware

Further analysis provides a breakout of the response by the type of government entity. The institutions of higher learning and the public school systems rated the threat of ransomware higher than state and local governments did.

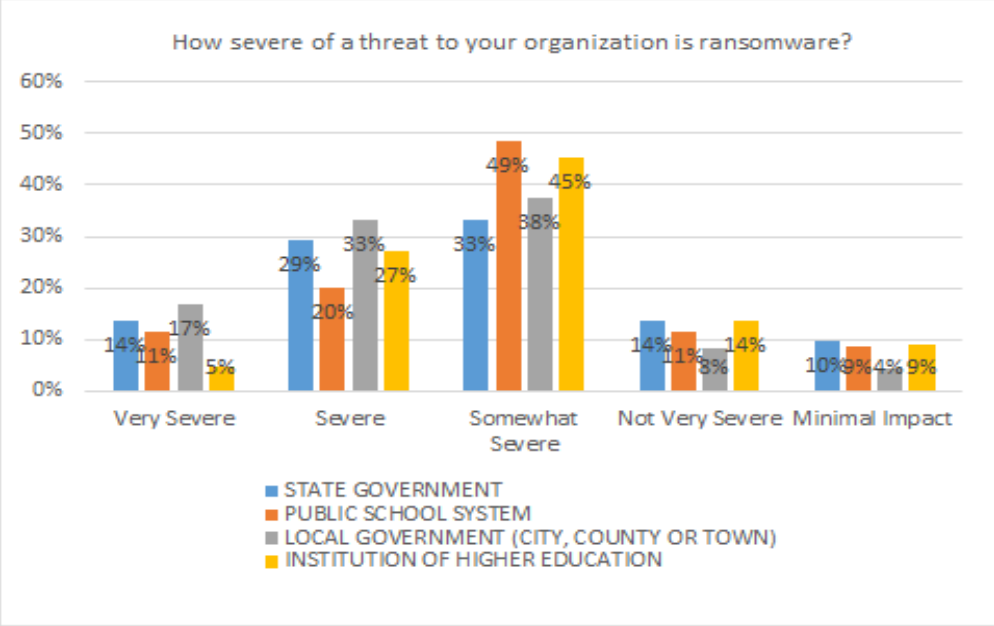


Figure 5: Ransomware Threat by Type of Entity

The survey also asked respondents about their experience with actual ransomware attacks. At the time of the survey, fewer than 20% had experienced an attack resulting in a significant compromise of the environment. Organizations experiencing the highest percentage of significant compromises were institutions of higher learning and public school systems.

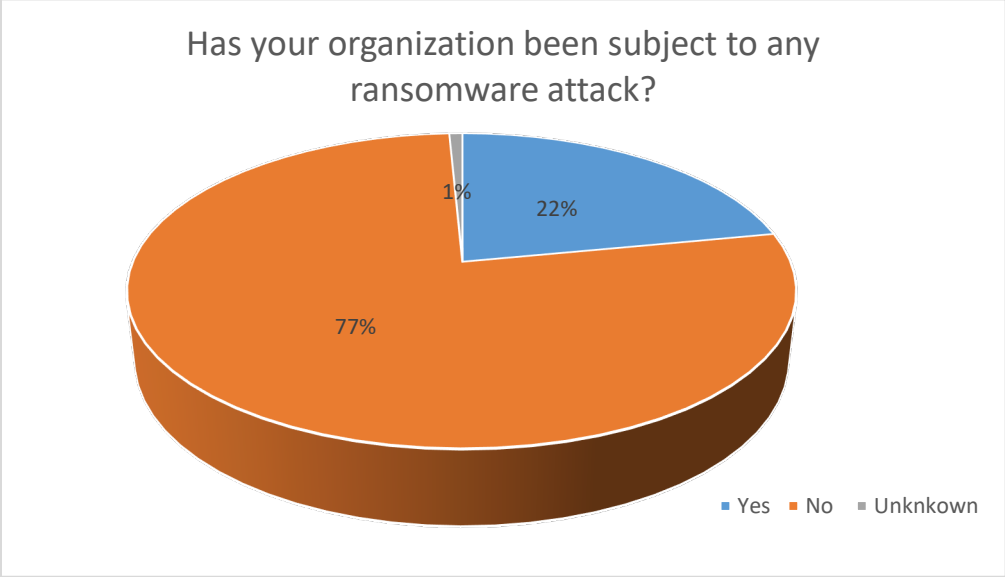


Figure 6: Reported ransomware attacks

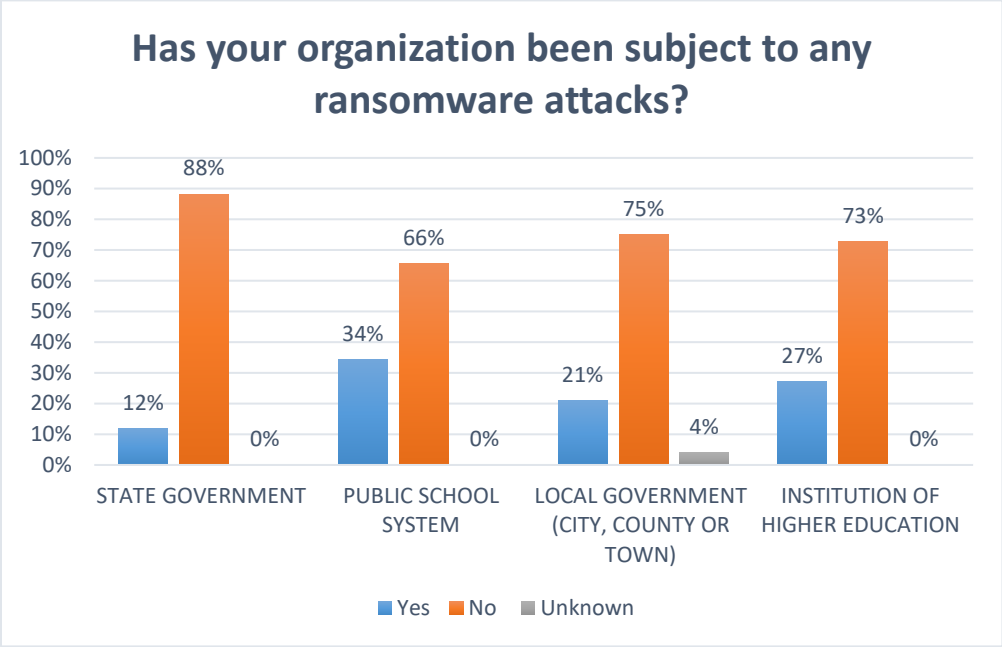


Figure 7: Reported ransomware attacks by entity type

Ransomware survey results and analysis: Top challenges

In addition to directed questions, the ransomware survey posed the following open-ended questions in order to solicit information about how to help improve the protection of state and local governments against ransomware:

- What is your organization's biggest challenge to improving your IT security program?
- What is your organization's top priority for improving your IT security program?
- How could the Commonwealth assist your organization with strengthening your IT security?

When asked to identify the organization's biggest challenge, the runaway leading answers were personnel and money. Smaller organizations reported wanting at least one person dedicated full-time to IT security, and respondents across-the-board noted concern about inadequate staffing. Respondents also worried about hiring and retaining qualified security personnel, particularly when competing for talented personnel in a market where IT security skills are in high demand.

Respondents reported that they lacked sufficient financial resources for cybersecurity. Some responses noted that IT security has insufficient funding priority and that one-time funding sources such as grants, are inadequate to maintain the required sustained investment of an IT security program. Whether an organization wishes to increase staffing, create or obtain training for staff, or acquire technology and tools, sustained funding was identified as the most critical need.

Awareness and cybersecurity culture were also identified as challenges. Respondents report a need to improve users' IT security awareness and knowledge throughout the organization. This was identified as a need both at the employee and executive levels. Responses expressed a need for leadership to recognize the importance of IT security to achieving organizational objectives.

Unsurprisingly, responses to what the Commonwealth could do to assist with strengthening IT security included providing more human and financial resources. Respondents also sought more information of various types, such as best practices, templates and examples, training and more information on who to contact for help.

Guidance on preparing for ransomware

Preparation is the most effective way to prevent ransomware infections from gaining a foothold in an environment. It requires education to recognize ransomware attempts, containment to prevent ransomware from spreading, and data protection to ensure backup information is adequately separated. The state has adopted the NIST cybersecurity framework and aligned applicable security controls. While the framework is detailed and comprehensive, alternative best practices are available for organizations without an established information security program. The Center for Information Security (CIS) has suggested several best practices for prioritizing the security controls that ransomware commonly exploits. Organizations often fail to adequately implement security controls in the included areas. The list of controls below is not comprehensive but will limit the effects of ransomware.[8] Additional information about these practices and strategies follows this list.

Maintain backups – thoughtfully

- Backing up important data is the single most effective way of recovering from a ransomware infection. Files should be appropriately protected and stored offline or out-of-band so they can't be targeted by attackers. Using cloud services can help mitigate a ransomware infection, because previous versions of files are retained, allowing users to roll back to an uninfected version. Backups should be tested regularly for efficacy. In the case of an attack, verify backups are not infected before rolling back.

Review exposed services and ports

- Many ransomware variants take advantage of exposed network ports. Determine if these ports need to be open, and limit connections to only trusted hosts. Be sure to

[8] "7 Steps to Help Prevent & Limit the Impact of Ransomware," Center for Internet Security, at https://www.cisecurity.org/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware/

review these settings for both on-premise and cloud environments.

Harden endpoints

- Ensure systems are configured with security in mind. Secure configuration settings can help limit the threat surface and close security gaps left over from default configurations. The CIS benchmarks are a great, no-cost choice for organizations looking to implement industry-leading, consensus-developed configurations.

Keep systems up-to-date

- Make sure all operating systems, applications and software are updated regularly. Applying the latest updates will help close the security gaps that attackers are looking to exploit. Where possible, enable auto-updating to automatically receive the latest security patches.

Train the team

- Everyone plays a part in protecting the organization; security awareness training is key to stopping ransomware in its tracks. . Security awareness training can teach team members what to look for in an email before they click on a link or download an attachment.

Implement an intrusion detection system (IDS)

- An IDS looks for malicious activity by comparing network traffic logs to signatures. A robust IDS will update signatures often and provide an alert quickly if it detects potential malicious activity.

Develop plans and policies

- Create an incident response plan so the IT security team knows what to do during a ransomware event. The plan should define roles and include communications to be shared during an attack. A list of contacts to notify, such as any partners or vendors, should be included. Consider creating a “suspicious email” policy that trains employees how to handle email that does not seem legitimate.

Ransomware Preparedness and Prevention

Cybersecurity insurance

When cyber attacks like ransomware and data breaches occur, they can result in devastating operational damage and exfiltration of sensitive information. Agencies have to contend with business disruptions, lost revenue and litigation. No organization is immune to the impact of cyber crime. As a result, cyber liability insurance has become an essential component to any risk management program.

Cyber liability insurance policies should be tailored to meet an organization's specific needs and can offer a number of important benefits, including: data breach coverage, cyber extortion defense, forensic support and data asset protection.

Under the 2020 Appropriations Act (Chapter 1289, Item 285 H), the Department of Treasury purchased cyber insurance for executive branch agencies. Treasury worked closely with VITA and Marsh & McClellan to develop a program that will cover the needs of the Commonwealth. Coverage will include:

- 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 that are levied against the agency.

- 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 protecting 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.

Links to additional information on cyber insurance can be found in the appendix.

Ransomware survey results and analysis: Cybersecurity insurance

The survey found that, although cyber insurance coverage is widespread, most government entities have not had the experience of making a claim under their cyber insurance policy, and there is substantial uncertainty whether they have the right type and amount of coverage. Most local governments (92%) and higher education entities (95%) indicated that they have cybersecurity insurance, but only 16% of state agencies indicated that they had insurance at the time of this survey. In addition, most respondents were not certain if they have the right type and amount of cyber insurance.

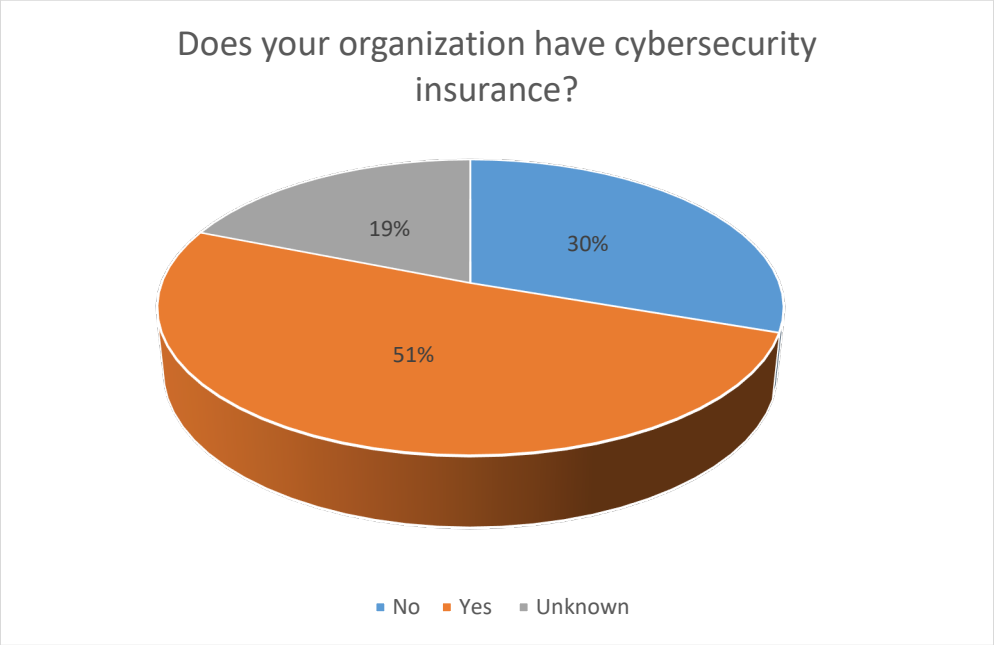


Figure 8: Use of cyber insurance

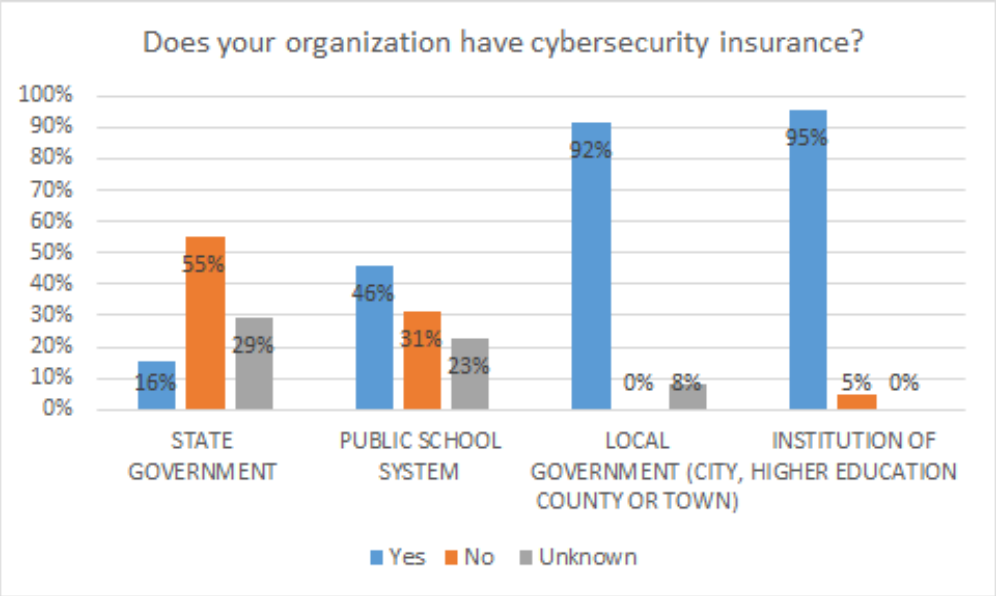


Figure 9: Cyber insurance by entity type

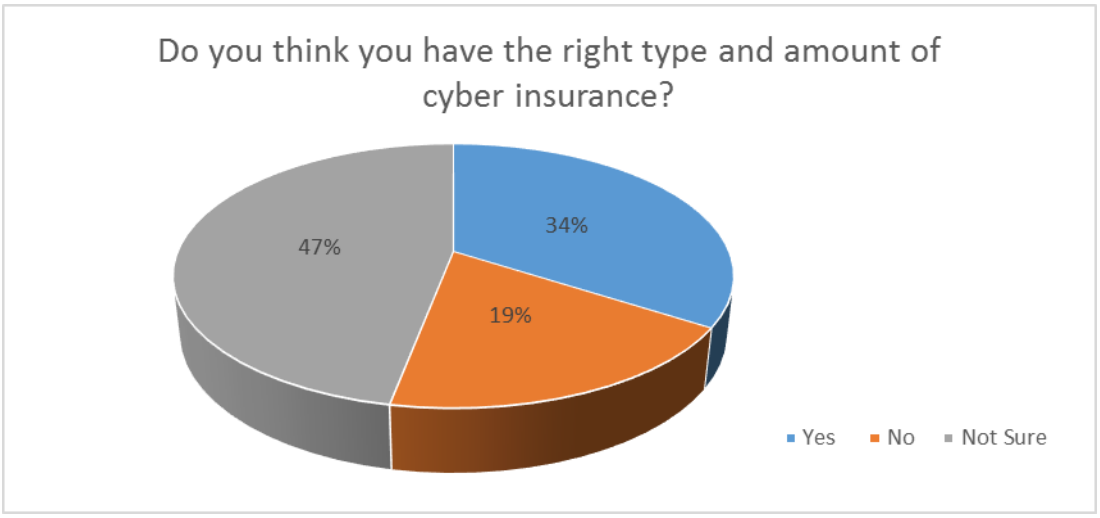


Figure 10: Right type and amount of cyber insurance

Security training

Like other cyberattacks, ransomware often enters an organization's network or systems by exploiting users. Attackers often enter an organization by tricking an employee or contractor into disclosing credentials or executing a malicious email attachment. Since end users are targets, employees and contractors should be made aware of the threat of ransomware and how it is delivered. Comprehensive and ongoing security awareness training must be provided to each employee and contractor regarding their responsibilities in protecting Commonwealth data. Security training is an essential ransomware prevention measure.

The General Assembly recognized the importance of security training in 2020 and passed House Bill 852. *See* 2020 Va. Acts ch. 717. This legislation requires the Chief Information Officer (CIO) of the Commonwealth, who is VITA's agency head, to develop by Nov. 30, 2020, a curriculum and materials for training all state employees in information security awareness and in proper procedures for detecting, assessing, reporting and addressing information security threats. The curriculum must be updated annually. Beginning in January 2021, the Commonwealth's executive, legislative and judicial branches and independent agencies will be required to provide annual information security training for all employees in accordance with the curriculum and materials developed by the CIO.

VITA has derived the curriculum topics from requirements set forth in the Commonwealth Information Security Standard (ITRM SEC 501 Information Security Standard).[9] The education program will help ensure that Commonwealth IT system users are able to:

- Demonstrate the safe and secure use of IT system resources
- Understand the need for protection of IT information
- Assure the privacy and confidentiality of personal information to which they've been entrusted
- Maximize operational effectiveness and increase productivity
- Minimize agency and Commonwealth liability
- Identify potential cyber threats
- Report potential cyber threats in a timely and efficient manner
- Stay compliant with all Commonwealth, regulatory and contractual requirements

Once the framework of the curriculum and materials are formally established, localities are encouraged to use curriculum to enhance their security awareness program.

Although employees are an organization's primary training audience, anyone who accesses an organization's network –including contractors and vendors– should be conducting security awareness training. Organizations should also vet their IT vendors' own security programs, given growing interconnectedness of systems and the increased exposure that accompanies such connections.[10]

Ransomware survey results and analysis: Security training

Respondents indicated that more than 75% of all state and local employees are currently receiving IT security awareness training. 92% of state agencies and 100% of institutions of higher education reported that they conduct security awareness training. However, only 46% of the

[9] SEC-501 and other security policies, standards, and guidelines are available on VITA's website at: https://www.vita.virginia.gov/it-governance/itrm-policies-standards/.

[10] Large data breaches have occurred through exploits of vendors. For example, the 2014 Target data breach occurred after credentials were stolen from a HVAC contractor. *See, e.g.*, "Target Hackers Broke in Via HVAC Company," Krebs on Security, https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/ (Feb. 5, 2014).

employees at public schools are receiving training. This indicates a need for improvement and assistance with training at public schools in the Commonwealth.

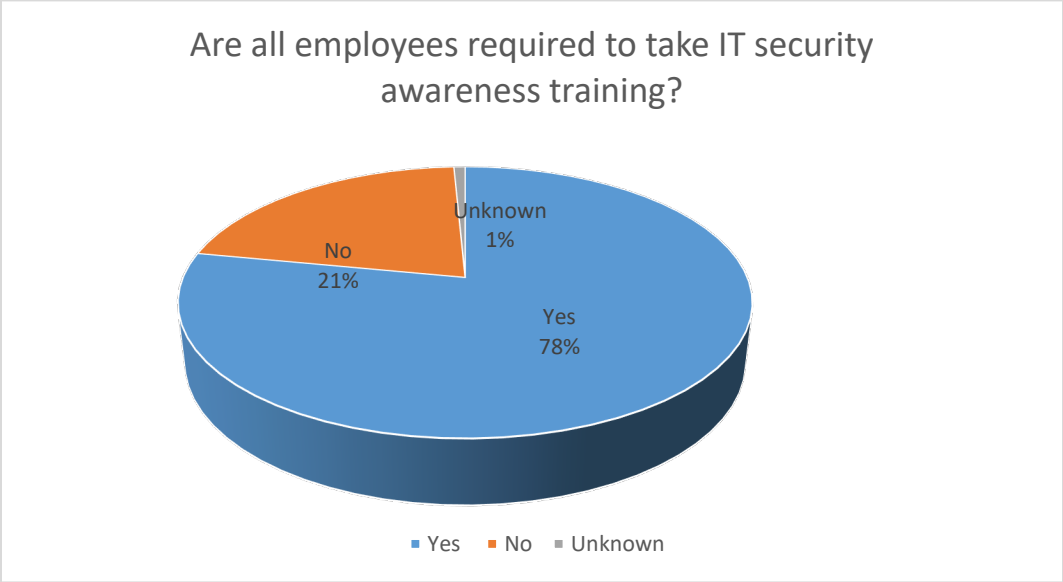


Figure 11: IT Security awareness training

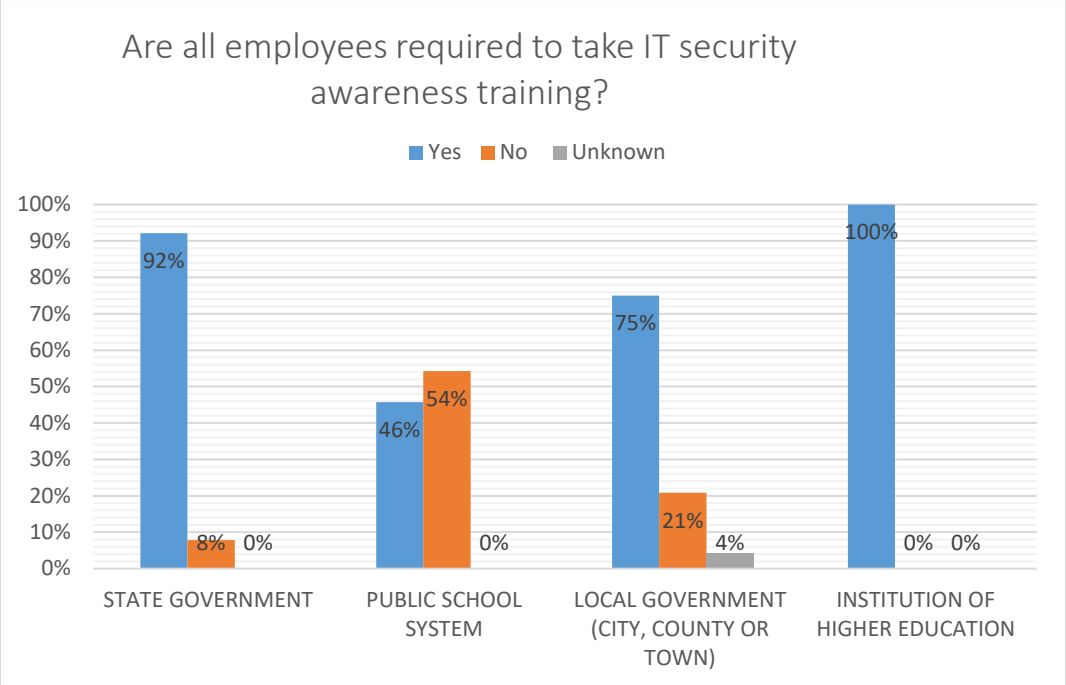


Figure 9: IT security awareness training by entity type

Figure 10: IT Security awareness training for contractors

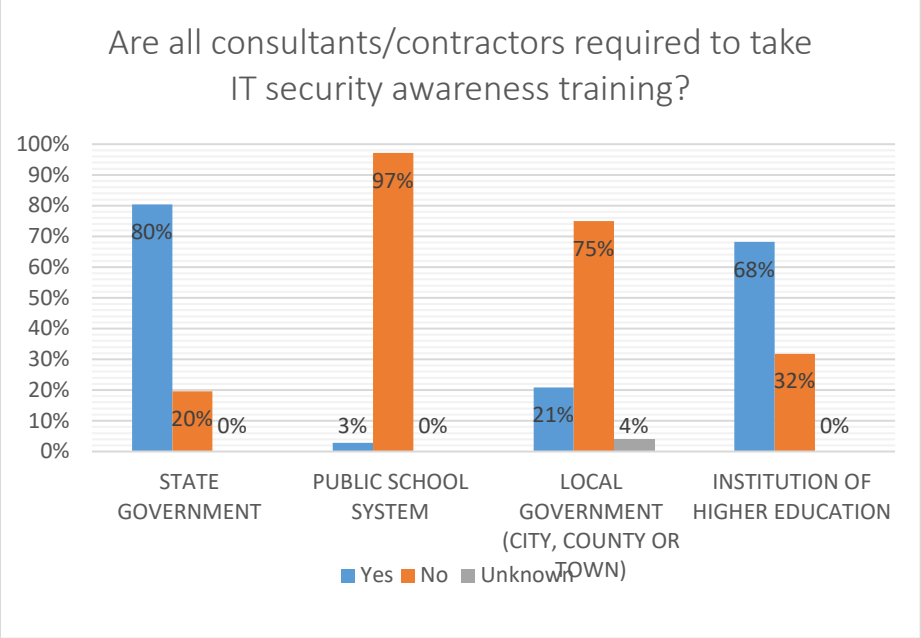


Figure 11: IT security awareness training for contractors by entity type

The percentage of consultants and contractors receiving IT security training is less than 50% overall. This is a major area of concern. Contractors and consultants may be assigned projects involving sensitive or confidential data. Understanding how to handle and protect this information is vitally important to ensuring the safety of Commonwealth data.

Ransomware prevention strategies

The FBI recommends the following to mitigate ransomware attacks.[11]

- Audit user accounts regularly, particularly remote monitoring and managing (RMM) accounts that are publicly accessible.
- Patch operating systems, software, firmware, and endpoints.
- Ensure backups are secure and are disconnected from the network at the conclusion of each backup session.
- Monitor inbound and outbound network traffic; set alerts for data exfiltration.
- Implement least privilege for file, directory, and network share permission.
- Educate employees about ransomware tactics, including preventative strategies, such as how to identify phishing emails and how to respond to suspected compromises.
- Apply two-factor authentication to user login credentials, receiving responses by text rather than email as actors may be in control of victim email accounts.
- Categorize data as to sensitivity and value using risk assessments.

Additional mitigation steps include incident response training, network and device segmentation; disabling macros, obtaining cyber insurance, service account management, network segmentation, the use of anti-malware and overall good cyber hygiene.

Ransomware survey results and analysis: Authentication and other security measures

Sixty-seven percent of surveyed organizations are using two-factor authentication and other security measures to prevent unauthorized access. The breakout by organization reveals almost a 50% difference between the local government and schools and state and higher institution monitoring scores.

[11] FBI, Private Industry Notification, April 1, 2020

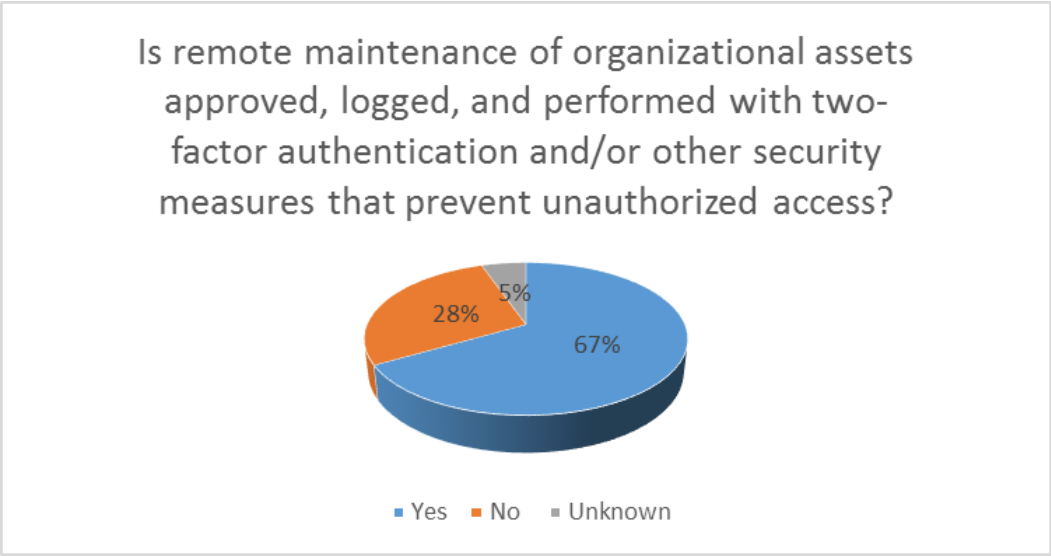


Figure 15: Is two-factor authentication in use in your organization?

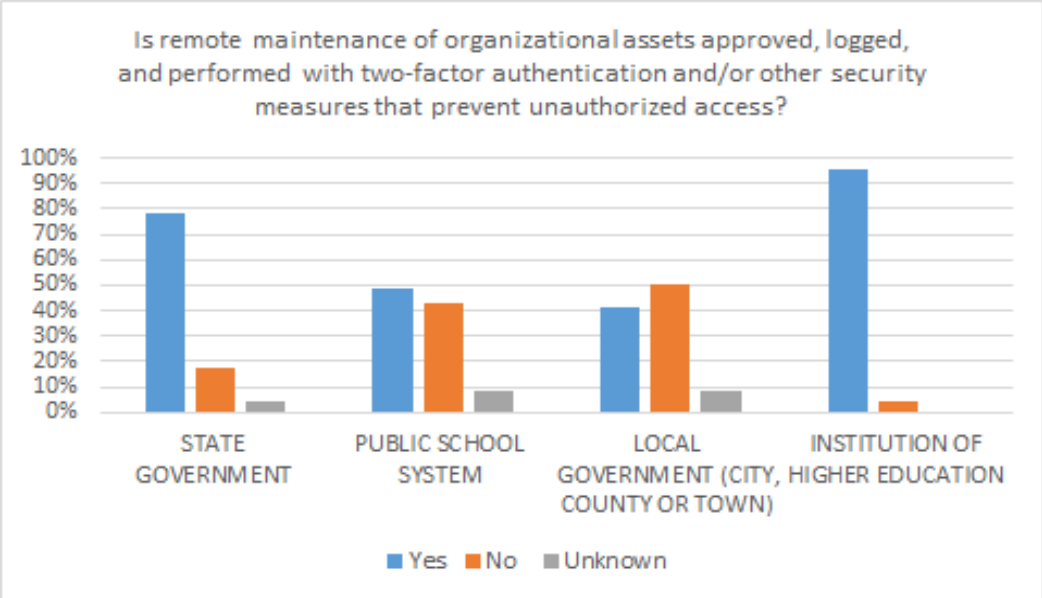


Figure 16: Unauthorized access prevention for remote access by entity type

Data encryption strategies

Encryption is the process of taking plain text, like a text message or email, and scrambling it into an unreadable format — called “cipher text.” This helps protect the confidentiality of digital data either stored on computer systems or transmitted across a network. When the intended recipient accesses the message, the information is translated back to its original clear text form. This is called decryption.

Data “in motion” refers to data traversing a network. For example, a user on a laptop connects to a file server. As the data moves back and forth between the laptop and server, it is “in motion.” Data “in motion” is often considered less secure.

A virtual private network (VPN), is a technology that is able to extend a private network across a public network like the internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across a VPN may therefore benefit from the functionality, security and management of the private network. Encryption is a common part of a VPN connection and is one of the ways in which data “in motion” is protected. Most organizations surveyed use VPN as a method to ensure secure encrypted and protected connectivity to their data.

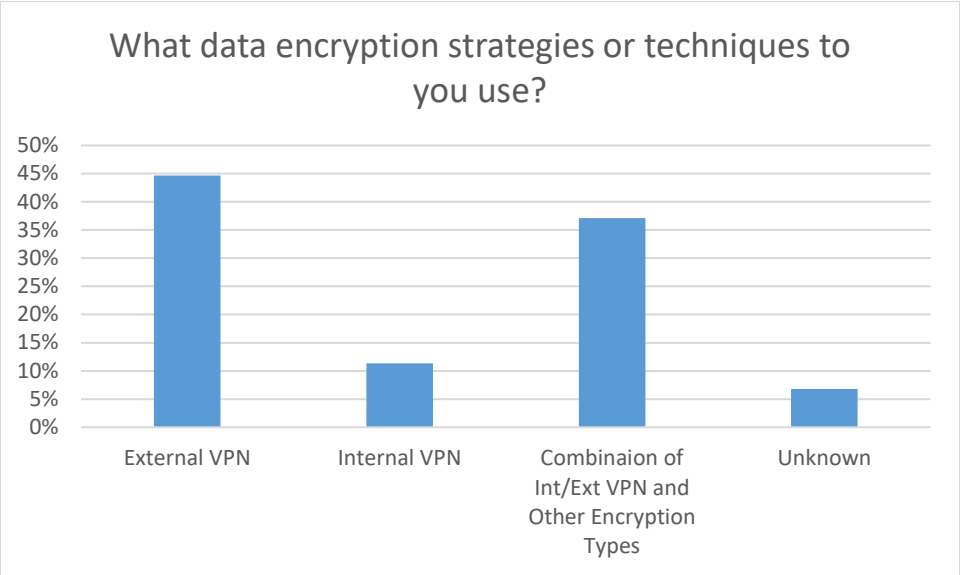


Figure 12: Data encryption strategies in use

Additionally, data can also be encrypted “at rest.” This means that the data is not actively moving within the system or network and is not interacting with hard drives, mobile devices, laptops, etc. To protect data “at rest,” encryption can also be used as a way to secure data that is stored on any device or network. Data “at rest,” particularly if it is not encrypted, is considered to be a valuable target to an attacker.

Protecting sensitive data both “in motion” and “at rest” is imperative for modern enterprises as attackers find increasingly innovative ways to compromise systems and steal data. Encryption alone may not protect an organization from a ransomware attack, but it can make data more difficult to access and less desirable to an attacker. Although encrypted data could still be compromised in a ransomware attack, encryption rendering it unusable would limit an attacker’s ability to use or disclose the encrypted data.

Ransomware Detection

Network monitoring

The most common cyber defense tools found in entities today are anti-virus products and email spam/virus filters. When configured properly across an enterprise, these two products offer a bare minimum level of defense against today's advanced threats. Organizations, however, need to do more by implementing network monitoring systems and tools that help analyze and make sense of system data.

Types of network monitoring systems

Several types of network monitoring systems are available. As noted above, an intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. The IDS system compares the current network traffic to a known threat database to detect several kinds of behaviors like security policy violations, malware and port scanners.

An intrusion prevention system (IPS) is a technology that monitors a network for any malicious activities attempting to exploit a known vulnerability. IPSs proactively deny network traffic if the security profile represents a known security threat.

Both IDS/IPS read network traffic and compare the contents to a database of known threats. The primary difference between the two is that an IDS is primarily a detection and monitoring tool that does not take action on its own. An IPS is a control system that takes action by accepting or rejecting network traffic based on the ruleset. However, as more encrypted traffic traverses the network, the efficacy of these devices is diminished unless full network traffic decryption is performed.

Endpoint detection and response (EDR), also known as endpoint threat detection and response (ETDR), offers continuous monitoring and collection of data that enhances rule-based detection and automated response capabilities. This type of tool offers the best environment visibility, which can greatly decrease time needed to uncover indicators of compromise during an incident response.

Log data

Entities often already have tools available, but may not be using them to their full potential. Logging data from the systems in the environment and retaining for at least 30 days can make or break an investigation. Even if an entity’s team does not know how to parse, interpret or monitor these logs, having them available to incident responders is critical in answering initial questions in an investigation.

Log sources that are likely already present in an environment:

- Router/switch - provides Netflow connection logs
- Firewall - provide syslog logs on connections and data
- Windows system event logs – Host-based logs that can be enhanced further by turning on additional audit logging such as process tracking and object access.
- Web servers - HTTP/S access and error logs
- Database servers – audit logs
- Web proxy - HTTP/HTTPS web connection logs from internal clients
- Domain name system (DNS) server - DNS logs
- Remote connections – Secure Shell (SSH), File Transfer Protocol (FTP) and logs from services that provide connections to remote clients

Ransomware survey results and analysis: Network monitoring

The results of the survey reveal that more than half of the organizations surveyed performed some type of "continuous monitoring." Continuous monitoring is the process and technology used to rapidly detect compliance and risk issues associated with an organization's IT infrastructure.

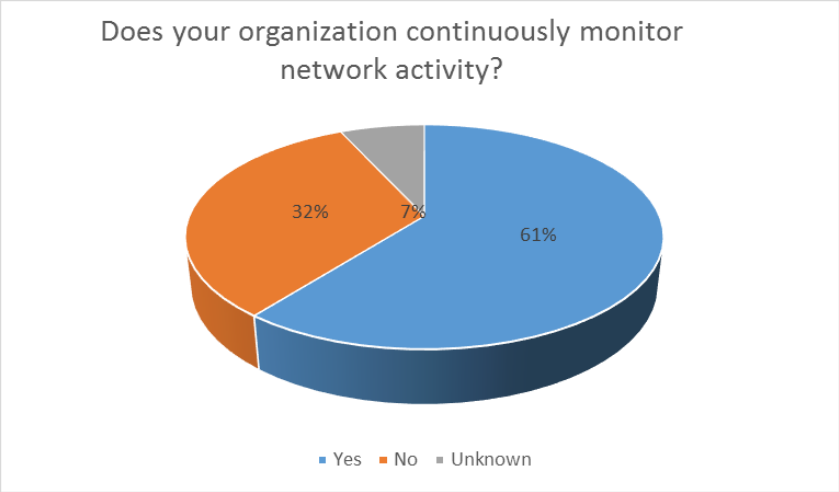


Figure 13: Continuous monitoring

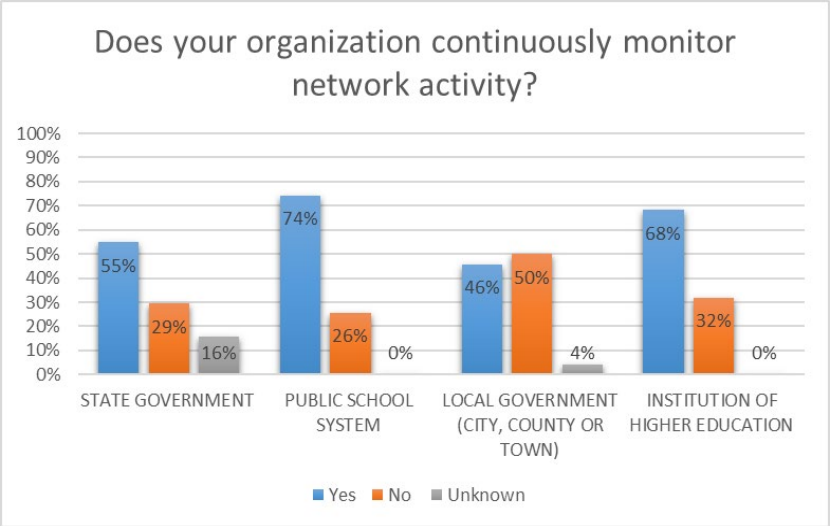


Figure 14: Continuous monitoring by entity type

The use of continuous monitoring reported by public schools (74%) and higher education institutions (68%) were significantly higher than state (55%) and local governments (46%).

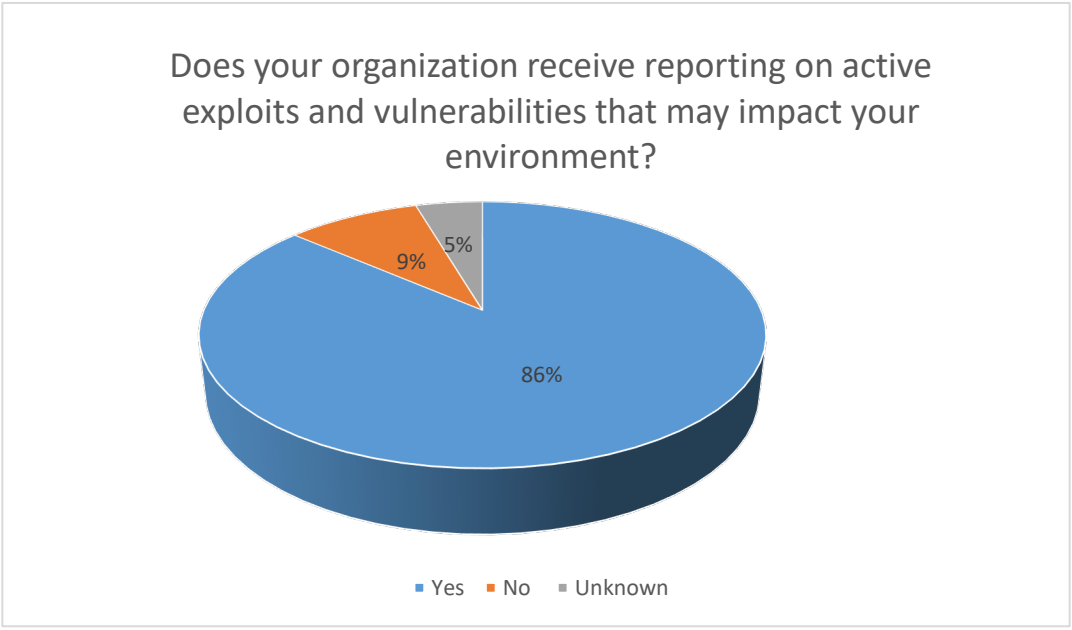


Figure 15: Reporting on exploits & vulnerabilities

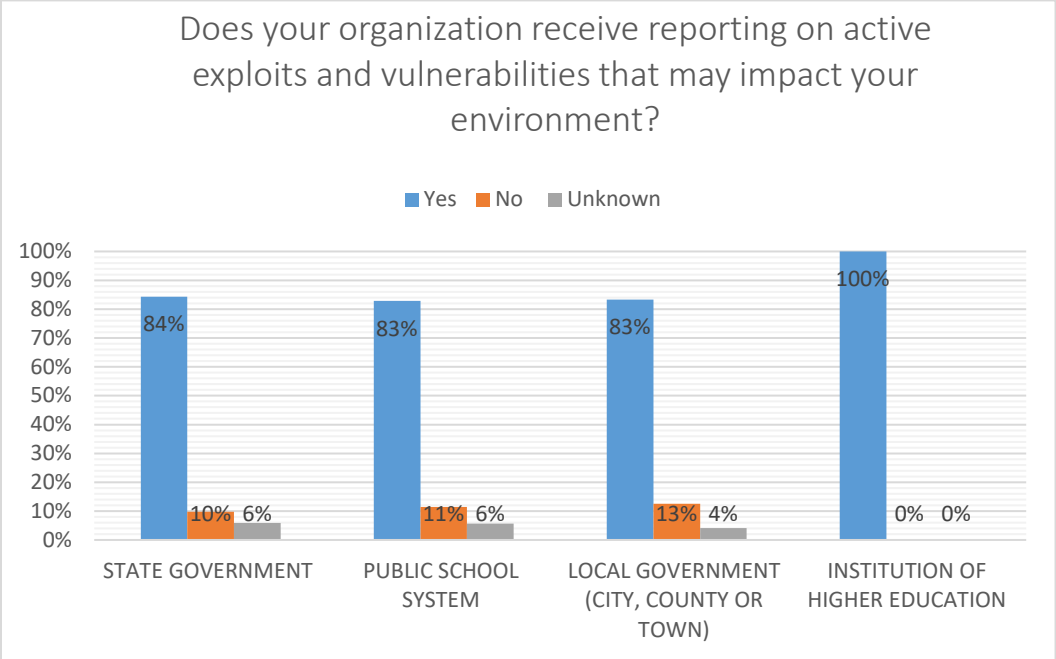


Figure 16: Exploit & vulnerabilities reporting by entity type

Receiving notification on active exploits and vulnerabilities helps organizations to keep their software and operating systems patched and less vulnerable to attack. Presently, 86% are receiving this valuable information. Increasing access to active exploits and vulnerabilities can enable organizations to keep their employees informed and alert incident responders of possible system vulnerabilities. In the survey, 100% of higher education institutions reported that they are receiving such notifications.

Forensic investigative techniques

Forensic investigative techniques use the indicators generated by event detection in the enterprise to discover the source and effects of the malware event. Implementing the indicators of compromise (IOC) back into security tooling is an effective way to prevent similar events in the future.

These techniques allow an organization to analyze malware or artifacts related to the malware's execution and produce information, including the servers that the malware communicates with or the executable's signature, which can help limit the spread of ransomware or improve detection of the malware in the future.

Ransomware survey results and analysis: Forensics

Sixty-five percent of the survey respondents' organizations have knowledge of or access to cybersecurity and forensic investigative capabilities. The combined percentages of no and

unknown responses (35%) are an area of concern that indicates the need for additional training or assistance.

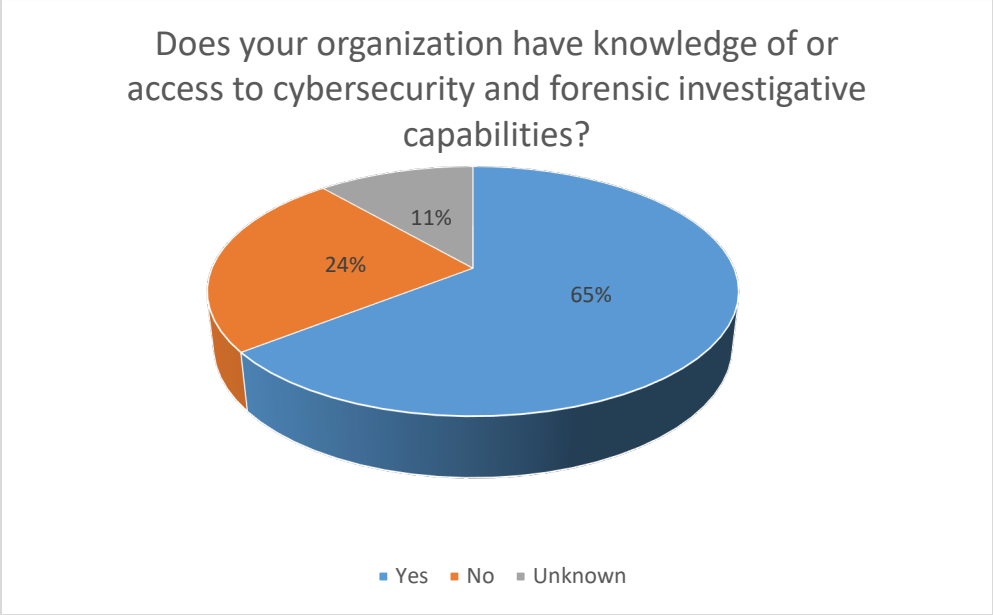


Figure 17: Cybersecurity & forensic capabilities

Figure 18: Cybersecurity & forensic capabilities by entity type

The availability of forensic resources can be a particular challenge. Computer forensic examiners are present across Virginia in various law enforcement departments. The three biggest statewide

forensic units are at the Office of the Attorney General (OAG), the Virginia State Police (VSP) and the Department of Forensic Science. OAG and VSP can be very responsive and flexible in responding to situations on scene during an event (both have mobile forensic labs). All three of those units regularly communicate and coordinate with each other.

State and local government agencies should also determine whether their local law enforcement has a forensic unit. Larger jurisdictions, like the City of Virginia Beach and Fairfax County, often have access to forensic units that can assist. Other jurisdictions often need to call an outside agency to help.

The Commonwealth would improve its ransomware response capabilities by increasing the availability of forensic resources and by improving access to existing resources. For example, Virginia could create a forensic listserv or portal to which main forensic response units are tied and distribute that to Commonwealth government entities.

Ransomware Recovery

In the unfortunate scenario where ransomware infects an environment, organizations depend on their disaster recovery and continuity of operations plans, and data backups to restore. The recovery and backup strategy is typically where organizations impacted by ransomware struggle the most. In order to have an effective disaster recovery effort, data backups must be reliable and include all the files needed to recover.

Data backups should be tested frequently to ensure data stored is viable. Users accidentally deleting their files often provide IT staff with a natural reason to restore individual files. If standard operations do not result in frequent tests, organizations should schedule, at a minimum, monthly restoration tests as part of a disaster recovery.

Planning to restore from a backup means that all the work between the time of the backup and the ransomware infection will be lost. This span of time is referred to as the recovery point objective (RPO). Organizations should ensure their disaster recovery plan identifies the RPO acceptable to the business for each system included in the plan. The shorter RPO, the more frequent backups will be needed.

Restore time is at the center of the business impact of a ransomware infection. The recovery time objective (RTO) is the time it takes from when an event stops work until work can resume. Like RPO, there will likely be different RTOs for different applications. Organizations must identify the amount of time they can tolerate a system being offline in the event of a disaster such as ransomware. The resulting target RTO should then incorporate any additional time required to physically move or transfer backups to the restoration site to ensure the full timeframe a system will be unavailable is included.

Data Backup Strategies

In order to have a successful backup strategy, a full copy of an organization's data must be verified as functioning and must be available. One of the most widely used industry backup strategies to accomplish this objective is the 3-2-1 rule. This rule is named based on the recommended backup steps: create at least three copies of the data, on two different storage media, with at least one copy located off-site. For example, organizations can store a copy of the information on an internal hard drive and two copies in an external device. The third copy would be kept off-site at a different physical or cloud location. This practice prevents losing copies of the information in case of an event such as a natural disaster.[12]

It is important to note in order for a data backup strategy to be effective against ransomware a full logical separation between the off-site backup must be maintained. Often times the off-site backup is moved to a device at a separate physical location but is accessible with the same administrator account as on-site backup copies. Ransomware attacks seek out backup copies and backup systems in order to prevent restoration of data and services. The simplest approach is to maintain an offline physical copy. If a backup is going to be connected to a network it must remain logically separated from the rest of the environment and accessible via two factor authentication only.

Additional links pertaining to backups are listed in the report's appendix.

Ransomware survey results and analysis: Backups

In order to understand the effectiveness of backup strategies employed in the Commonwealth the ransomware survey included information about organization backup plans. Overall the responses indicated most organizations maintain a disaster recovery and backup plan. The data was not able to indicate whether sufficient compliance with the 3-2-1 approach and logical access separation was included in the disaster recovery planning.

The team asked survey respondents how frequently they performed backups. More than 80% perform backups daily and only 4% were not sure whether backups were being performed. Additionally, 96% of local governments indicated that they perform backups daily.

[12] US-CERT Data Backup Options," at https://us-cert.cisa.gov/sites/default/files/publications/data_backup_options.pdf (2012).

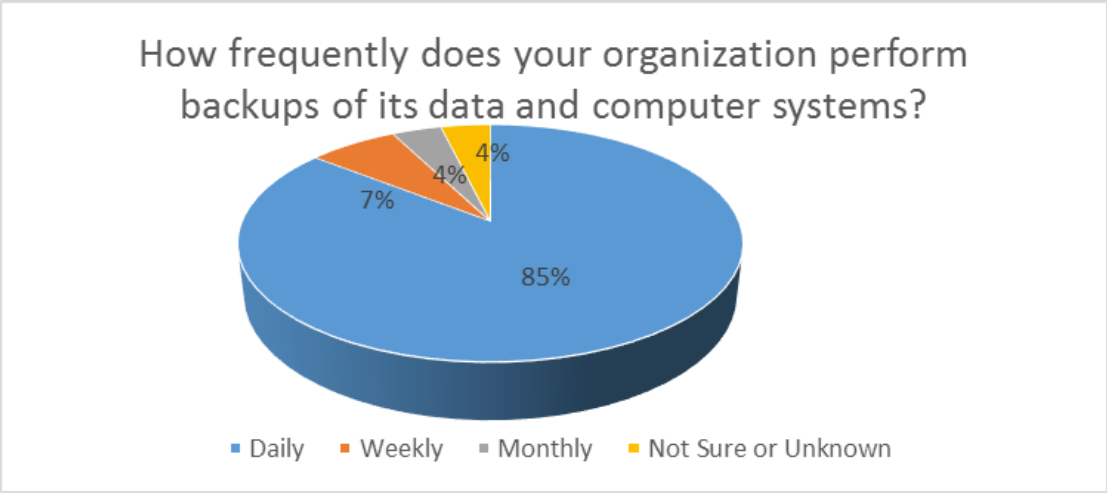


Figure 19: Frequency of backups

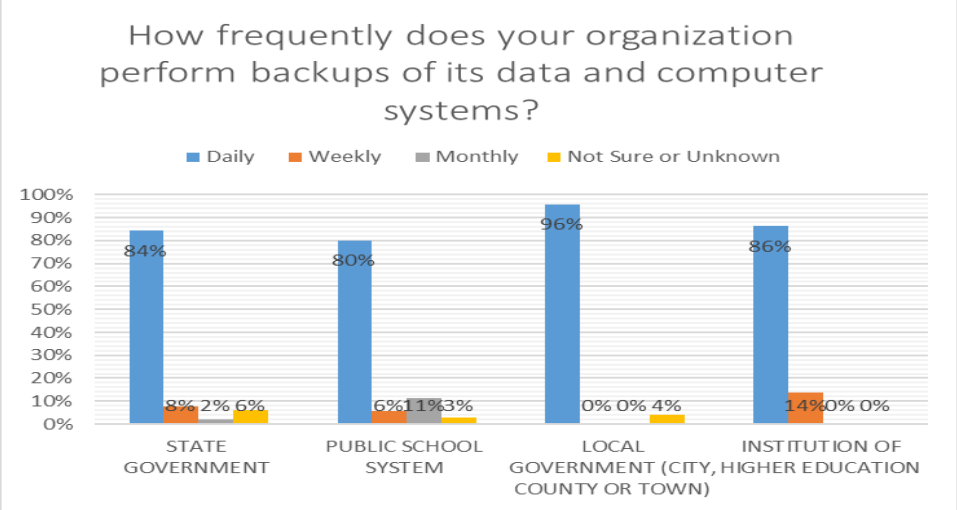


Figure 20: Frequency of backups by organization type

Ransomware Response

Ransomware attacks have the ability to strike even the most prepared state or locality. Planning can help ensure that the organization is ready to respond quickly and without confusion. Early detection and mitigation can reduce the potential impact of the event, which can include damage to our enterprise files, applications and systems. Prompt reporting to law enforcement and application of forensic investigative techniques also will assist with mitigation and response.

Should an organization be a victim of ransomware, the Cybersecurity and Infrastructure Security Agency (CISA) strongly recommends responding by using the following checklist.[13] (The list below is an abbreviated version. A link to the entire document is listed below and in the appendix.)

Security incident response

An organization's response to ransomware will be more effective if the organization has engaged in appropriate planning. Having a plan can reduce the effectiveness of an attack and might even stop the attack entirely.

Planning for a ransomware attack can involve training an organization's IT response personnel and employees and instituting some of the practices listed below:

- An incident response plan should contain information specifically related to responding to a ransomware attack
- Exercises should be conducted to determine the effectiveness of the ransomware response
- Train, test and re-train employees – employees should know how to identify malicious emails, how to avoid being hacked, and how to report suspicious emails.
- Beware of email – install anti-malware scanners and advanced threat prevention
- Conduct regular network risk assessments
- Keep software and systems up-to-date with all patches and updates
- Back up, back up, back up: regularly back up data
- Limit privileged administrator accounts and review quarterly
- Implement multifactor authentication (MFA) for remote access and privileged administrators' access
- Prohibit local storage of data

A plan that is implemented, communicated and exercised can greatly reduce the time required to handle the attack and reduce the costs associated with the attack. An additional link on ransomware protection planning is listed in the appendix.

Security incident recovery and post-incident activity

- Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services. Take care not to re-infect clean systems during recovery.

- Document lessons learned from the incident and associated response activities to inform updates to—and refine—organizational policies, plans, and procedures and guide future

[13] "Ransomware Guide, September 2020." Cybersecurity and Infrastructure Security Agency (CISA) (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (2020).

exercises of the same.

- Consider sharing lessons learned and relevant indicators of compromise with CISA or your sector's Information Sharing and Analysis Center (ISAC)/Information Sharing and Analysis Organization (ISAO) for further sharing and to benefit others within the community.

A ransomware "playbook" developed for each entity's specific needs and requirements would be valuable. Playbooks serve as a step-by-step guide for responding to incidents and keep incident response moving when the stress of an actual incident can cloud judgement. These playbooks should ideally be tested as revised, incorporating tabletop exercises into the preparation phase of incident response.

Detection and analysis

- Determine which systems were impacted and immediately isolate them.
- Only when you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.
- Triage affected systems for restoration and recovery. Prioritize critical systems for restoration and recovery.
- Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis.
- Engage your internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident. Consider requesting assistance from CISA, MS-ISAC and local, state, or federal law enforcement. As appropriate, coordinate with communication and public information personnel to ensure accurate information is shared internally with your organization and externally with the public.

Reporting to IT security

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. The longer the discovery time, the more damaging the breach can be and the costlier it will be to correct and contain.

Under current law, when a cyber incident occurs, directors of agencies in the executive branch are required to report them to VITA within 24 hours of discovery. *See Va. Code § 2.2-603(G).* Incidents can be reported 24 hours a day, seven days a week using an online incident reporting

form[14] or by contacting the Commonwealth's help desk service. More information is available on VITA's security incident reporting site at https://www.vita.virginia.gov/commonwealth-security/incident-reporting/.

Containment and eradication

Assess the situation and prevent spread

When unusual activity on the network is detected, following the suggested steps will assist in slowing the spread of the attack:

- Disconnect system from the network to prevent the spread of the infection and turn off any wireless functionality.
- Do not turn off the infected asset, if possible. Many times the decryption key or routine is still in memory and powering off the asset might make recovery hopeless.
- If the asset must be shut down, preserve the hard disk to be used in identifying the indicators of compromise.
- Perform a memory dump of the asset (free open source tools are available).
- Determine the scope of infection – shared drives/folders, external hard drives, storage devices.
- If possible, obtain a copy of the ransom note to assist in determining what type of ransomware is attacking.
- Contact/coordinate with law enforcement.
- Determine responses to the attack
    - Locate backups, ensure their integrity, and work to restore.
    - Consider trying to decrypt using a decryption tool, such as those made available through the No More Ransom! Project, which is an initiative developed by the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre, Kaspersky, and McAfee, with the goal of helping victims of ransomware retrieve their encrypted data without having to pay the criminals.
    - Assess whether the loss is acceptable. If the value of the data is less than the amount of ransom requested, the decision might be made not to pay.
    - Consider whether to negotiate or pay the ransom. Some digital forensics groups offer professional negotiation with ransomware perpetrators, which (as with real life kidnap or hostage negotiation) can offer significant advantages over attempting to deal with the criminals yourself.

[14] VITA Commonwealth Security incident Reporting Form: https://www.vita.virginia.gov/commonwealth-security/incident-reporting/incident-reporting-form/

Contain and mitigate the incident:

- Research the trusted guidance (i.e., published by sources such as government, MS-ISAC, reputable security vendor, etc.) for the particular ransomware variant and follow any additional recommended steps to identify and contain systems or networks that are confirmed to be impacted.

- Identify the systems and accounts involved in the initial breach. This can include email accounts.

- Based on the breach or compromise details determined above, contain any associated systems that may be used for further or continued unauthorized access. Breaches often involve mass credential exfiltration.

- Conduct an examination of existing organizational detection or prevention systems (antivirus, endpoint detection & response, intrusion detection system, intrusion prevention system, etc.) and logs. Doing so can highlight evidence of additional systems or malware involved in earlier stages of the attack.

- Conduct extended analysis to identify outside-in and inside-out persistence mechanisms.

- Rebuild systems based on a prioritization of critical services (e.g., health and safety or revenue generating services), and using pre-configured standard images, if possible.

- Once the environment has been fully cleaned and rebuilt (including any associated impacted accounts and the removal or remediation of malicious persistence mechanisms), issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility. This can include applying patches, upgrading software, and taking other security precautions not previously taken.

- Based on established criteria, which may include taking the steps above or seeking outside assistance, the designated IT or IT security authority declares the ransomware incident has ended.

If mitigation actions do not appear possible:

- Take a system image and memory capture of a sample of affected devices (e.g., workstations and servers). Additionally, collect any relevant logs as well as samples of any “precursor” malware binaries and associated observables or indicators of compromise (e.g., suspected command and control internet protocol (IP) addresses, suspicious registry entries, or other relevant files detected).

- Consult federal law enforcement regarding possible decryption tools available, as security researchers have already broken the encryption algorithms for some ransomware variants.

Ransomware survey results and analysis: Security incident Response

Survey results show that 91% of higher education institutions and 73% of state agencies have an incident response plan. The survey, however, shows that less than half of local governments and public school systems currently have an incident response plan.

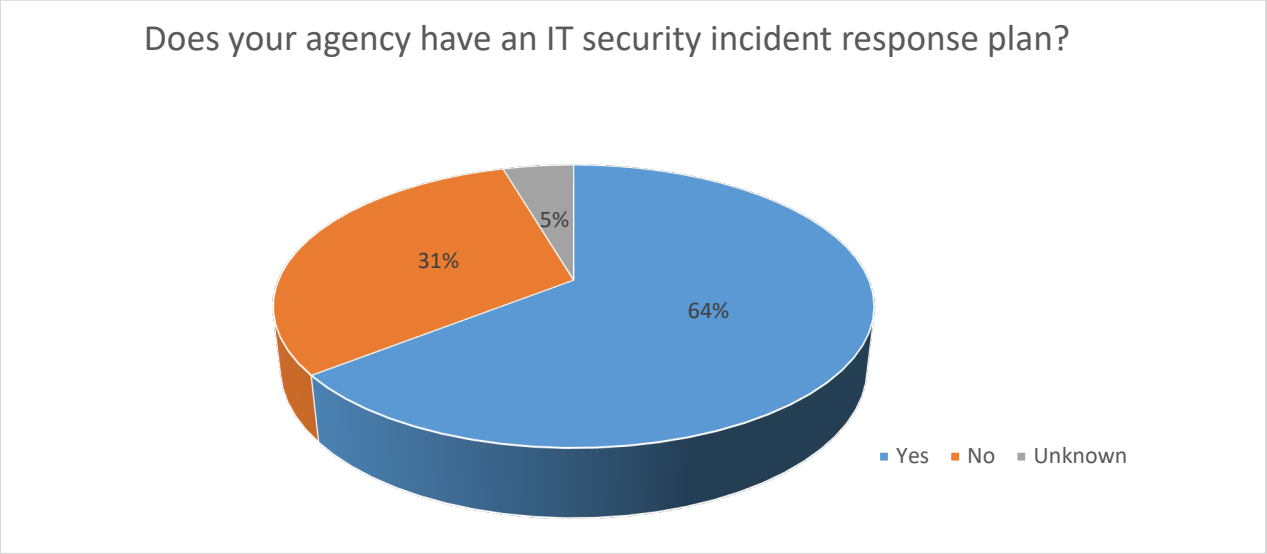


Figure 21: IT security incident response plans

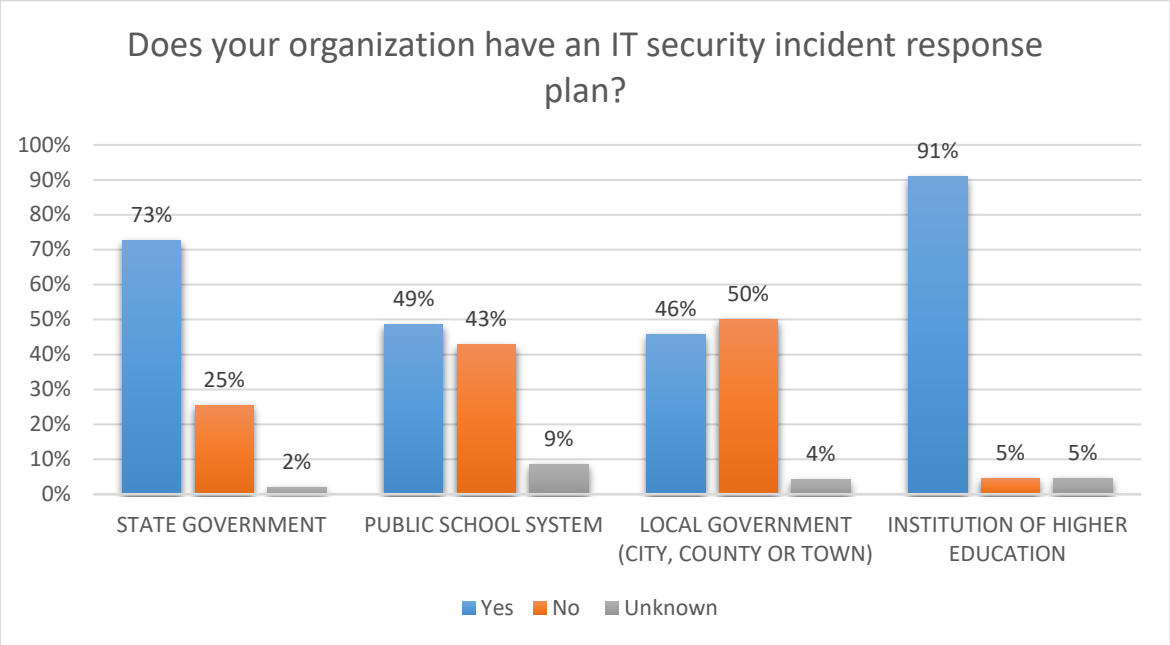


Figure 22: Security incident response plans by entity type

Reporting ransomware

Incident reporting to VITA within the executive branch is discussed above. Broadening prompt, consistent reporting outside of the executive branch and into local government would improve the overall security posture of the Commonwealth.

Contacting law enforcement is an important part of ransomware response. Law enforcement may be able to use legal authorities and tools that are unavailable to most organizations. Law enforcement can enlist the assistance of international law enforcement partners to try to locate the stolen or encrypted data or identify (and ideally charge and apprehend) the perpetrator.

Law enforcement should be contacted through designated individuals in a manner consistent with the requirements of the law and the organization's procedures.

When a ransomware attack is detected in Virginia, reports should be made to the Virginia Fusion Center (VFC) at vfc@vfc.vsp.virginia.gov and the High Tech Crimes Division (HTCD). The HTCD has right of first refusal for all investigations in Virginia. For the Commonwealth, the VFC is the central reporting mechanism in the State Cyber Emergency Operations Plan that engages the FBI, DHS, and National Guard, as necessary.

One reason that many security-related incidents do not result in convictions is that some organizations do not properly contact law enforcement. Under reporting can be due to potential

embarrassment, fines, or loss of customer confidence and in some cases, regulations do not require organizations to report attacks.[15]

Law enforcement reporting

Only 55% of respondents have a policy to report IT security incidents to law enforcement. Providing additional information on how to create a reporting policy and creating policy templates might be useful.

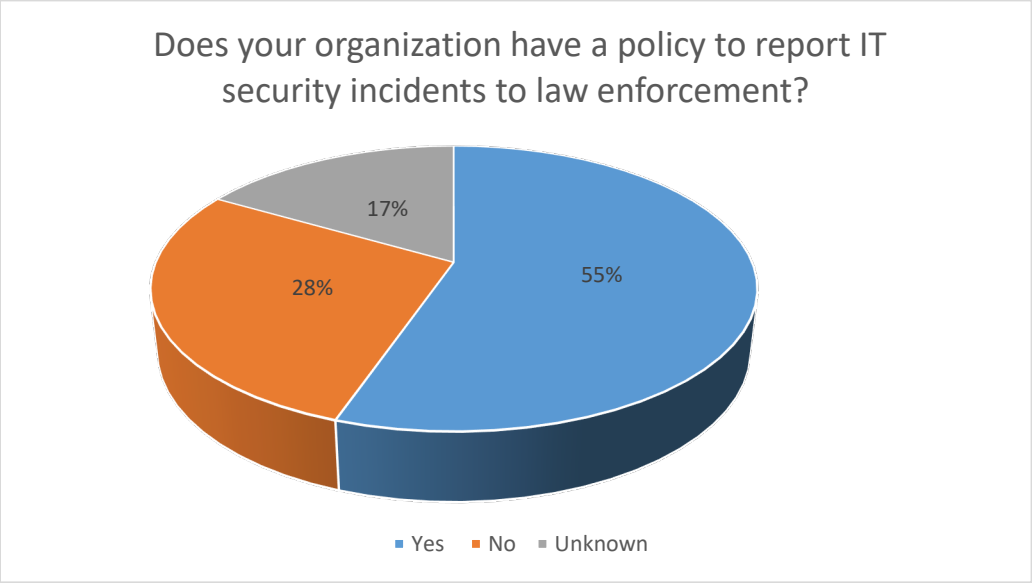


Figure 28: Percentage of organizations with law enforcement reporting policy

[15] "Enterprise Cybersecurity: Investigating and Detecting Ransomware Infections Using Digital Forensic Techniques," Jason E. Thomas, 2008-2019.

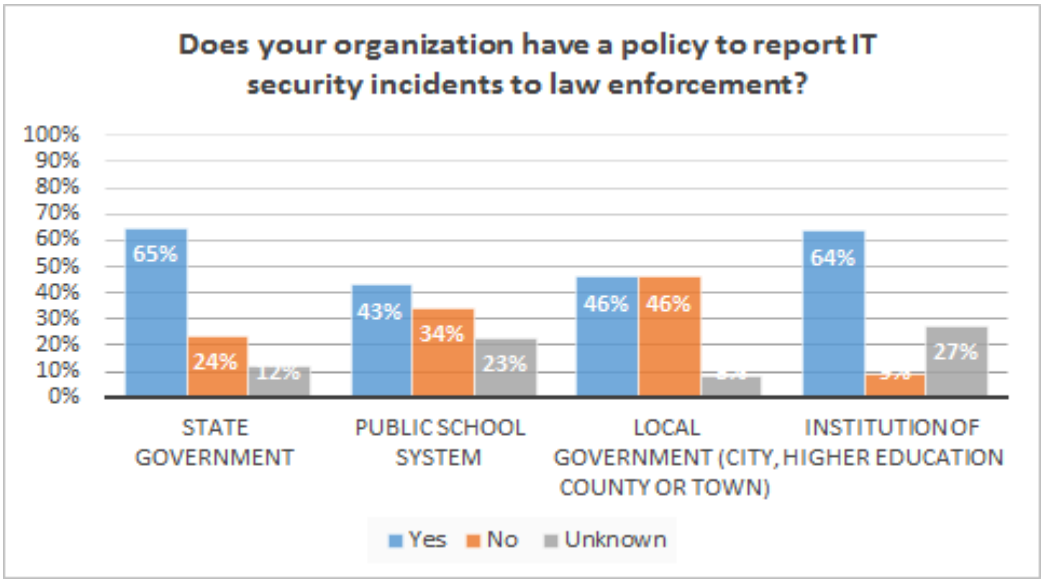


Figure 23: Percentage of organizations with law enforcement reporting policy by entity type

Contacting law enforcement is essential, but expectations should be realistic. As ransomware rapidly increases in complexity and scale, it can be challenging for law enforcement agencies to respond. Even with law enforcement involvement, it can be difficult to recover a victim's data and nearly impossible to find the cybercriminals responsible for a ransomware attack.

Evaluating Paying the Ransom

Once infected by ransomware, the choices are not good: pay the ransom, restore from unencrypted backups, or wipe the network and start over. Starting over without data often means the inability to effectively operate for an extended period of time. Usually this is longer than stakeholders deem acceptable. Restoring from backups can also require considerable time and resources and may encounter problems along the way. Often times at least portions of the data in large scale recovery won't be available. When evaluating these factors against the possibility of a quick recovery by paying the ransom it can be tempting, to believe that the best choice is to pay. This approach is not recommended.

Paying the ransom poses serious risks. The following should be considered before deciding whether to pay:

- Paying a ransom does not guarantee an agency will regain access to their data. Decryption can fail, or in some cases, some individuals or organizations were never provided with decryption keys after paying a ransom. Experienced negotiators will often engage in a process that involves testing the perpetrator's capability to restore access to the data.
- Some victims who paid the demand have reported being targeted again by cyber actors.

- After paying the originally-demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- Paying supports the perpetrators' "business" and could encourage more ransomware attacks.

On October 1, 2020, the US Department of Treasury's Office of Foreign Assets Control (OFAC) issued an advisory to highlight sanctions and risks involved with paying ransomware actors. Facilitating payments to a sanctioned malicious actor or to comprehensively sanctioned jurisdictions could violate U.S. law, which may incur fines or other penalties assessed by OFAC. OFAC encourages victims to contact OFAC should they choose to pursue making a ransomware payment.[16]

If possible, an organization should seek assistance when it comes to communicating or negotiating with, and possibly paying, ransomware perpetrators. Agencies should contact law enforcement to coordinate activities.

Commonwealth Ransomware Response Strategies

Existing Security Incident Response Framework

Due to the different organization types and authorities, the response framework within the Commonwealth has several different paths. Fortunately, the teams involved have an excellent working relationship. That said, one of the areas that would likely be helpful is to create a formal structure for an incident response process for all entities in the state.

The incident response process executes in one of two paths depending on whether a state or local entity or school district is involved. Each path has a defined process for the reporting of incidents, however the actual steps for containment are different depending on the type of entity involved. For the executive branch VITA infrastructure customers, security incident containment is handled as a joint effort between VITA Commonwealth Security and Risk Management, the VITA infrastructure program, and the impacted agency. In state agencies in other branches or in agencies that are in the executive branch but not part of the VITA infrastructure program, the incident coordination is performed through VITA and the containment is executed by the impacted agency. In all of these circumstances VITA partners with several other organizations to disseminate information other organizations can use to protect themselves. VITA also works with law enforcement at the state and federal level to provide any evidence needed to facilitate a criminal investigation.

[16] "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" Depart of the Treasury. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf (Oct. 1, 2020).

Localities and school districts do not have a formal reporting process to notify the state of a compromise such as ransomware. Practically though when the organizations are compromised they are either looking for help from a government entity or receive attention from the press resulting in public notice of the compromise. In most cases when an organization is looking for assistance they will either contact their local emergency manager or will reach out to the Virginia State Police. Either way the contact will result in engagement of the Virginia Fusion Center where they will coordinate resources to assist. The Virginia Fusion Center will advise the agency as to whether they need to contact the Virginia Department of Emergency Management to declare an incident.

State Security Incident Response

At the state level, the Chief Information Officer of the Commonwealth (CIO) and VITA have the lead role in information security. Additionally, each agency has responsibilities assigned by VITA in Commonwealth security standards and recognized in the Code. The primary objective of the requirements is to ensure security incidents are reported so stakeholders can be adequately briefed.

VITA responsibilities

The CIO of the Commonwealth is charged with leading the Commonwealth's information technology security and risk management program. *See* Va. Code §2.2-2009; Va. Code §2.2-603F. The CIO performs these duties through the Chief Information Security Officer (CISO) and the Commonwealth Security and Risk Management (CSRM) group within VITA.

Agency responsibilities

Agencies have requirements identified in several different areas. VITA establishes some of these responsibilities in the Commonwealth security standards and others are identified in code. The primary responsibility of an agency is to work with VITA to mitigate a compromise and determine the impact. Identifying the impact involves understanding the initial attack vector, containing the incident from causing further damage and identifying data that may have been impacted. VITA works with agencies to establish the parameters for meeting these objectives during an incident.

Emergency Operations Plan – Cyber Annex

To date state agencies have been fortunate enough not to experience an issue severe enough that it couldn't be mitigated through standard processes. If an incident this severe does happen, the Virginia emergency operations plan has steps included to engage the Virginia National Guard. The Department of Military Affairs/Virginia National Guard/Virginia Defense Force advise and assist with cyber response and recovery activities. The National Guard's cyber resources, including information assurance, applications, and network operations personnel, support incident response and recovery for affected state, local, and private sector partners.

Leverage Department of Homeland Security tools

There are significant, free, mature, open-source tools available that provide capabilities for collection and monitoring of network traffic. Some tools, for example, include: security incident and event management (SIEM), vulnerability scanning, network mapping, endpoint detection and response (EDR), intrusion detection (IDS), host- and network-based digital forensics, threat hunting, network mapping and documentation, and asset management. The amount of technical knowledge necessary to effectively configure, deploy, and monitor these tools can be prohibitive to entities adopting the technologies into their environments. DHS has taken some steps to help with this issue and has worked with the MS-ISAC to a few services leveraging these tools.

One tool recently introduced is a domain name query monitoring service called Malicious Domain Blocking and Reporting (MDBR). This technology prevents IT systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats. This capability can block the vast majority of ransomware infections just by preventing the initial outreach to a ransomware delivery domain. It is a very low impact service with a very high benefit. It is especially effective for organizations with minimal resources as it does not require a lot of technical changes or support.

Another tool available from MS-ISAC is a networking monitoring tool called "Albert." This tool is a cost-effective intrusion detection system (IDS), which uses open-source software combined with the expertise of the Center for Internet Security's (CIS) 24x7 Security Operations Center (SOC) to provide enhanced monitoring capabilities and notifications of malicious activity.[17] Albert is based on the U.S. Department of Homeland Security's (DHS) "Einstein" technology, which was designed to generate, collect and analyze network traffic. Albert is tailored to U.S. state, local, tribal, and territorial (SLTT) government organizations. The custom signature set utilized by Albert enables it to be very effective in detecting ransomware and other malicious traffic. The signatures on Albert are updated daily to ensure organizations receive the latest threat protection.

The true advantage to the Albert network monitoring is the ability to have a cost efficient and effective monitoring service for government organizations. Government organizations are able to maintain a clear picture of their network activity while keeping an "always-on" eye for malicious behavior. Typically this type of service is too costly for medium to small organizations, however the cost sharing arrangement makes it possible for even smaller organizations.

In the Commonwealth, Albert is in place for all executive branch agencies which are part of the VITA infrastructure program. It is recommended for all agencies and localities within the Commonwealth even if they have their own tools due to the intelligence provided to the monitoring team.

[17] The Center for Internet Security, "Albert Networking Monitoring and Management" https://www.cisecurity.org/services/albert-network-monitoring/ (2020).

Law enforcement response strategies

The Virginia State Police (VSP) is the lead state agency for criminal investigations and provide investigative support to other law enforcement organizations. The Virginia Fusion Center (VFC) serves as an initial point of contact and coordination for criminal response to cyber incidents impacting non-state agencies. The VFC functions in a role which coordinates the cyber investigation information flow between state entities. It also disseminates non-sensitive/non-identifying information to government and/or critical infrastructure partners so they can protect themselves. The VFC can also participate in incident handling, and collect and analyze law enforcement information following the incident's conclusion.

The OAG's Computer Crime Section assists in both the computer forensic examination and prosecution of criminal incidents involving ransomware and malware. The Computer Forensics Unit, contained within the Section, consists of three computer forensic examiners who can respond on-site during malware attacks to perform forensics on servers or to triage evidence, and will subsequently conduct full forensic analysis on evidence in support of the investigation. The Section's four attorneys have concurrent jurisdiction with Commonwealth's Attorneys under the Virginia Code to handle prosecutions in all Virginia courts stemming from ransomware/malware incidents where crimes under Virginia's Computer Crimes Act are implicated. The attorneys are also cross-designated as Special Assistant U.S. Attorneys and can potentially bring such cyber-based prosecutions into federal court, if appropriate.

One of the most frequent challenges faced in identifying the sources of ransomware and other compromises is the ability to identify and obtain information about the systems leveraged in the compromise. In most cases systems which are already compromised or belong to parties in other countries are leveraged to carry out the attack. For those systems in the United States, it is often necessary to coordinate with either a federal organization or another state's law enforcement organization to obtain the information needed. In addition, the resulting information doesn't typically yield the investigative data needed to track the source to the final destination.

While law enforcement strategies alone won't fix the inability to consistently find the source of ransomware attacks there may be some approaches to streamline some of the investigation process. One step would be to investigate the feasibility of streamlining requests for forensic information across states. For example, if Virginia is looking for information on a corporate system in Georgia used in a compromise, it would be useful to be able to obtain the information directly from Georgia, reducing the investigation time frame and increasing efficiency.

Legislative and regulatory recommendations

Administrative law recommendations

In 2020, the General Assembly took steps to strengthen the requirements for and coordination of state government cybersecurity training (through 2020 Va. Acts ch. 717). Additional legislation could establish training requirements for local government and provide for a statewide cybersecurity training and awareness plan to improve awareness and education among employees and other personnel with access to state and local government networks. It is important to note, however, that additional mandates may not be welcome without the resources to help organizations meet those requirements.

The Code of Virginia currently requires executive branch agencies to report cyber incidents promptly. *See* Va. Code § 2.2-603(F) & (G). Additional legislation could create a reporting framework for non-executive branch entities at the state level and for local government.

Agencies with current responsibilities do work to coordinate with each other, and that should be encouraged – state and local entities who are able to do so should be authorized to assist each other with cybersecurity. However, additional measures are recommended to embrace a cooperative approach, such as establishing and funding a cross-functional incident response team that would be able to call on state, local, and federal resources and that could be rapidly activated to respond to a cyber incident. Regional cooperation in cybersecurity could be encouraged, as well as highlighting and helping others learning from leading organizations among their peers.

Current Virginia criminal laws

Most ransomware incidents violate the Computer Trespass statute, Virginia Code § 18.2-152.4, a part of the Virginia Computer Crimes Act that specifically prohibits (among other things) altering, disrupting, disabling, removing, or halting computer data or programs. During the 2020 Session, the General Assembly broadened the scope of Computer Trespass to include acts committed using intentionally deceptive means and without authority, in addition to acts committed maliciously (which was the previous and only standard). *See* 2020 Va. Acts ch.821. A violation of Computer Trespass is a Class 1 Misdemeanor but rises to a Class 6 felony if the conduct affects a state or local government computer, affects a provider of utilities, causes damage of $1,000, or involves the installation of a keystroke logger.

Ransomware is also a form of extortion and most incidents will likely violate Virginia's extortion statute contained within Virginia Code § 18.2-59, which prohibits threatening injury to the property of another person in order to extort money. A violation of this statute is a Class 5 felony.

These existing laws mean that it is likely possible to charge a ransomware event.

Jurisdiction can pose a challenge to prosecuting a ransomware event, however. The long arm of Virginia's criminal jurisdictional reach is only but so long and can pose a significant challenge in many computer crimes including ransomware incidents. Virginia can obtain criminal jurisdiction over an incident if the bad actor resides in Virginia, if there is a victim of the crime in Virginia, or if any of the bad actor's conduct utilized computer networks in Virginia. However, actors in other countries, where Virginia's criminal statutes and associated subpoena/extradition power have no reach, commit many of these incidents. Virginia can indeed reach actors within the United States who commit such attacks through the extradition process between the states (which must be approved by the Governor's Office). Extradition would not be possible though if the only violations at issue are misdemeanors, which particularly narrows the impact of the Computer Trespass statute upon out-of-state actors.

Criminal law recommendations

Virginia's criminal laws do encompass ransomware, but it is possible to strengthen those laws to better target ransomware. Although Virginia's general extortion statute likely would apply in many ransomware incidents, it may not reach incidents where there is no specific "threat to injure" the network or computer data and the bad actor is simply holding it hostage. In addition, there is scant, if any, case law that has interpreted the "property" term within the extortion statute to include computer data, although that seems likely to be the conclusion if tested.

Creating a separate statute within the Virginia Computer Crimes Act to specifically prohibit holding data hostage while demanding money and including a felony penalty (which is justified given the enormous damage ransomware inflicts on businesses, governments, organizations, and even individuals) would provide clarity in the prosecution realm and strengthen Virginia's reach to get to some of these bad actors. Specific statutory language could include (with the caveat that this could be amended in many ways to account for all contingencies): "any person who (i) disrupts the operation of a computer network of another person or organization, (ii) disables computer data or a computer network of another person or organization, or (iii) threatens injury to computer data or a computer network of another person or organization, and thereby extorts money, property, or pecuniary benefit or any note, bond, or other evidence of debt from him or the organization or any other person is guilty of a Class (5 or 6) felony."

Regulatory recommendations

Virginia has a regulatory and governance structure in place for state agencies and it has proven effective in ensuring the state has evolved the information security program. This continued prioritization has led to reasonable levels of protection within the Commonwealth state government and prioritization of protecting citizens, government services and Commonwealth data. While there is always room for improvement, the current structure has done a good job of positioning the Commonwealth to have protections against threats such as ransomware. The

framework is successful due to having a designated organization responsible for setting the security thresholds for the state and the ability to measure and report on those thresholds.

At the state level, the primary recommendation is to add reporting for the state of cybersecurity as a requirement for all branches and agencies of government. Right now, only the executive branch is required to produce a report for the state of security. That report has proved immensely helpful in prioritizing problem areas. Adding a reporting requirement for those agencies not subject to VITA governance, as well as judicial and legislative branches to the corresponding appropriate stakeholders, would be a good step in understanding what cybersecurity issues the Commonwealth may not be aware of. This requirement should also include higher education, which has been able to opt out of VITA governance and does not currently provide an analysis. Governing stakeholders of each public body needs analysis of cybersecurity, regardless of whether the additional reporting is submitted to VITA.

For localities and school districts, a similar approach to reporting should apply. Establishing the responsibility for maintaining an information security program is the first step in making progress. A report indicating how seriously an organization and its leadership is taking the issue helps drive resources and attention in the right direction.

Conclusion

After an in-depth analysis of the survey data, the NCSR and the notable increase in successful ransomware attacks throughout the state, it is clear there is significant susceptibility to, and lack of preparedness for, ransomware attacks within the Commonwealth. Unless action is taken it is likely government and school systems will continue to experience compromises. In order to prevent ransomware attacks from continuing to be successful VITA recommends a twofold approach: make cost-effective security technology and services available to localities and school systems; and, establish a formal response unit.

The need for technology and services was apparent in the survey results. Cybersecurity training and awareness plans are needed throughout state and local government. Technical strategies and tools can be effective preventative measures, but employees are a key line of defense to prevent attacks especially in ransomware attacks. In addition to a deficit in training, security measures such as continuous monitoring and vulnerability assessments are not widely performed. This indicates an organization is not able to identify where their environment is susceptible to ransomware and wouldn't be alerted once compromised. Additionally, slightly more than half of the respondents said they have the knowledge and skill sets to handle a ransomware incident if they were to become infected. Almost half of Virginia government entities surveyed indicated they aren't able to identify ransomware attacks with the resources they have available. This fact, combined with a minimal information security programs in a majority of locality governments, leads to a Commonwealth extremely susceptible to ransomware attacks.

Obtaining cost effective security technology and services is often a significant challenge for localities, especially the smaller ones. If each locality is responsible for obtaining their own set of security tools the cost will likely be insurmountable. One strategy to deal with this challenge is to implement a cost-sharing model for security services. For example, modifications to allow localities and school districts to leverage existing private sector contracts for security and infrastructure services. For those localities that do not have sufficient funding this would change would help eliminate the hefty upfront costs to establish some of the security services. An additional recommendation is to establish funding for localities to obtain the MS-ISAC Albert service. The service is an extremely cost-effective approach to identify malicious traffic in a network and share intelligence across networks. Though funds are necessary to set up and run the service it is an extremely reasonable rate. This step won't solve the full scope of technology needs but it will provide an affordable way of understanding what is happening in the case of a ransomware attack.

The second recommended component is introducing legislation establishing a Virginia Cybersecurity Incident Response Team (VA-CIRT). This team would be responsible for receiving reports and providing resources to help engage law enforcement, recommending remediation plans and connecting organizations to established contracts or services to address their needs. Additionally the team's primary goals would be to reduce recovery time due to ransomware, help law enforcement obtain information to identify the source of the intrusion and identify the impact to critical infrastructure within the Commonwealth. The team would require some limited funding for the tools and technology necessary to collaborate with impacted organizations. The recommended participants should include the existing multi-agency cyber response participants.

The final recommendation is to explicitly assign responsibilities for locality and school district cybersecurity programs to an appropriate stakeholder within the Code of Virginia. Some of the feedback we received from the survey, along with anecdotal conversations, expressed frustration that leadership did not seem to support or understand that cybersecurity is part of their job responsibilities. Including a specific assignment of ensuring cybersecurity risks are managed will help ensure there is some prioritization.

State and local governments' susceptibility to ransomware is elevated and ongoing, and there is not an "easy" button to solve the problem. Minimizing the Commonwealth's susceptibility to, and mitigating the effects of, ransomware will require a variety of measures including legislation and improved coordination between government entities. VITA thanks the General Assembly for highlighting this important issue and looks forward to working with policymakers and other state and local government stakeholders to better protect the Commonwealth by improving cybersecurity.

Appendix – Report Methodology and Further Resources

Report methodology

To assist with collecting information and to obtain broad statewide collaboration for this report, VITA requested the assistance of the Commonwealth Information Security Council. The council is composed of information security officers and other interested parties from numerous state agencies. The council formed a ransomware committee, whose names are listed at the end of this report, including personnel from VITA, several other state agencies, and one locality. Statewide, local and educational associations were consulted for guidance, collaboration and background data-gathering. The ISO council subcommittee met from April to November 2020 to generate an inclusive body of information and work on this report. The IS Council developed a methodology to support each section of the resolution.

To gain insight into the current state of ransomware preparedness within the Commonwealth, the ransomware committee and VITA decided a survey of agencies and organizations covered by the legislation was appropriate and an ideal way to understand the state of ransomware preparedness. The subcommittee created a survey instrument based on standard information security profiling and specific ransomware inquiries and sent it to security contacts at executive, legislative, judicial, and independent state agencies, as well as to localities, institutions of higher education, and public (K-12) schools. Statewide associations and VITA distribution lists were used to distribute the survey, which reached approximately 350 organizations. Survey responses were provided in August and September, and the results have been tabulated and analyzed. The survey received 122 responses for a response rate of 35%.

The ransomware committee thanks the Virginia Association of Counties (VACo), the Virginia Municipal League (VML), the Virginia Association of Local Government IT Employees (VALGITE) and the Department of Education for assistance in reaching targeted members and stakeholders. In discussing the legislation, this report and the aforementioned survey, members of localities and the K-12/higher education community expressed an interest in the results and having greater awareness of the issues they face among the legislative bodies governing Virginia.

The ransomware committee also thanks the Multi-State Information Sharing and Analysis Center (MS-ISAC) for its collaboration and information-sharing to strengthen this report. MS-ISAC is a voluntary and collaborative organization designated by the U.S. Department of Homeland Security as a key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal, and territorial governments. Virginia governmental entities work with MS-ISAC, and its parent organization the Center for Internet Security (CIS) to communicate potential data breaches and security threats to government entities.

Decryption Tools

Decryption tools for many known ransomware variants:
https://www.nomoreransom.org/en/decryption-tools.html

Ransomware prevention advice

https://www.nomoreransom.org/en/prevention-advice.html

National Institute of Standards and Technology (NIST):
https://www.nccoe.nist.gov/sites/default/files/library/supplemental-files/msp-protecting-data-extended.pdf

Ransomware Response and Prevention

MS-ISAC Ransomware Guide 2020
https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

Backup Options

US-CERT
https://us-cert.cisa.gov/sites/default/files/publications/data_backup_options.pdf

Computer Weekly
https://www.computerweekly.com/feature/Top-five-ways-backup-can-protect-against-ransomware

InfoSecurity Magazine
https://www.infosecurity-magazine.com/opinions/keeping-backups-ransomware/

Protecting and Planning
https://www.nccoe.nist.gov/sites/default/files/library/supplemental-files/msp-protecting-data-extended.pdf

Einstein Project
https://www.dhs.gov/publication/dhsnppdpia-001the-einstein-program

Cyber Insurance Cyberscoop
https://www.cyberscoop.com/ransomware-fbi-insurance-companies-data/

Ransomware Survey
The results of the survey conducted for this study can be referenced as a separate document.

Security Checklist for implementing ransomware best practices

Once a system is infected with ransomware, it will download the encryption keys and begin locking a victim's files. At this point advanced cybersecurity controls, such as Intrusion Detection Systems (IDS), can identify ransomware in its early stages and alert organizations to an impending disaster.

In addition to having an IDS in place, it is important to implement several information security best practices. Organizations should take a defense-in-depth approach to building a strategic security program. Implementing a multiple layered defense assists in succeeding at defending against modern, sophisticated threats.

Start with basic cyber hygiene such as the following CIS Sub-Controls from Version V7.1 Implementation Group 1:

- Keep all systems patched. Effective patching requires:
    - Know what systems are on the network.
    - Implement:
        - CIS Control 1.4: Maintain Detailed Asset Inventory
    - Know what software is running on the network.
    - Implement:
        - CIS Control 2.1: Maintain Inventory of authorized Software.
        - CIS Control 2.2: Ensure software is supported by vendor
        - CIS Control 2.6: Address unapproved software
    - Patch your systems.
    - Implement:
        - CIS Control 3.4: Deploy Automated Operating System Patch Management Tools
        - CIS Control 3.5: Deploy Automated Software Patch Management Tools

- Use anti-virus and anti-spam solutions.
    - Implement:
        - CIS Control 8.2: Ensure Anti-Malware Software and Signatures are Updated

- Protect sensitive data.
    - Implement:
        - CIS Control 13.1: Maintain an Inventory of Sensitive Information
        - CIS Control 13.2: Remove Sensitive Data or Systems Not Regularly Accessed by Organization
        - CIS Control 14.6: Protect Information through Access Control Lists

- Train all employees on how to identify and report suspicious activity and to not click on links or download files within any suspicious emails.
    - Implement:
        - CIS Control 17.3: Implement a Security Awareness Program
        - CIS Control 17.6: Train Workforce on Identifying Social Engineering Attacks

Types of ransomware

Research reveals that there are two main types of ransomware - Crypto and Locker ransomware.

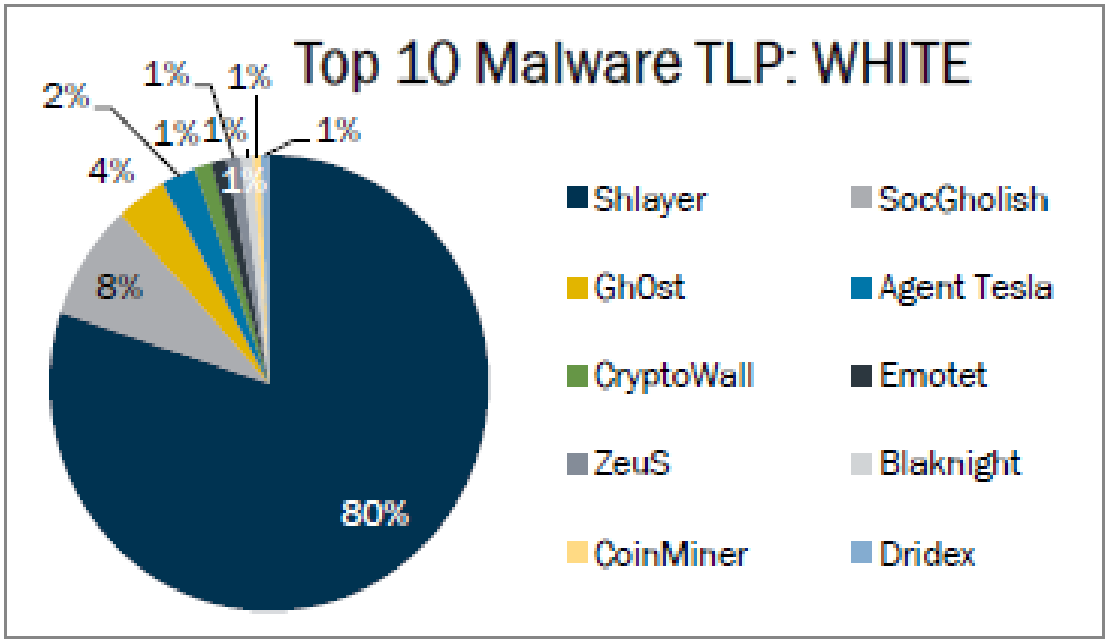
Crypto ransomware encrypts valuable files on a computer so the user cannot access them without the key know only to the attacker.

Locker ransomware is a form of malware that restricts login or file access while demanding payment to lift the restriction. It's typically deployed at the operating system (OS) level, meaning you won't be able to use an infected computer or device

Crypto ransomware is currently most attackers' preferred software. Some of the most common attacks in 2020 were:[18]

1. Shlayer is a downloader and dropper for MacOS malware. It is primarily distributed through malicious websites, hijacked domains, and malvertizing posing as a fake Adobe Flash updater.
2. SocGholish is a RAT and a banking trojan that uses fake Flash Updates to drop a NetSupport RAT payload. Recently, SocGholish has been used to drop WastedLocker ransomware, a new ransomware variant.
3. Gh0st is a RAT used to control infected endpoints. Gh0st is dropped by other malware to create a backdoor into a device that allows an attacker to fully control the infected device.
4. Agent Tesla is a RAT that exfiltrate credentials, log keystrokes, and capture screenshots from an infected computer.
5. CryptoWall is a ransomware commonly distributed through malspam with malicious ZIP attachments, Java Vulnerabilities, and malicious advertisements. Upon successful infection, CryptoWall will scan the system for drive letters, network shares, and removable drives.
6. Emotet is a modular infostealer that downloads or drops banking trojans. It can be delivered through either malicious download links or attachments, such as PDF or macro-enabled Word documents.
7. ZeuS is a modular banking trojan which uses keystroke logging to compromise victim credentials when the user visits a banking website.
8. Blaknight, also known as HawkEye, is an Infostealer known for its keylogging capabilities for credential and banking theft.
9. CoinMiner uses the WMI Standard Event Consumer scripting to execute scripts for persistence. CoinMiner spreads through malspam or is dropped by other malware
10. Dridex is a banking trojan that uses malicious macros in Microsoft Office with either malicious embedded links or attachments.

[18] Top 10 Malware September 2020, Multi-State Information Sharing and Analysis Center



In September 2020, malvertisement accounted for the greatest number of alerts. Malvertisement continues to increase and stay as the top initial infection vector due to Shlayer. Shlayer returned to the Top 10 Malware after new evidence resulted in it being reclassified as a Trojan Downloader compared to an Adware Dropper. Activity levels for all vectors, except malspam and network, increased. It is likely that malvertisement will remain the primary infection vector as the Shlayer campaign pans out.

Ransomware study committee members

Joseph Walton, Department of Behavioral Health and Development Services
Michael Wickham, Virginia Workers Compensation Commission
Kathy Bortle, Virginia Information Technologies Agency
Marlon Cole, Virginia Information Technologies Agency
Renea Dickerson, Virginia Information Technologies Agency
Joshua Heslinga, Virginia Information Technologies Agency
Dean Johnson, Virginia Information Technologies Agency
Edward Miller, Virginia Information Technologies Agency
Michael Watson, Virginia Information Technologies Agency
Gene Fishel, Office of Attorney General
Broadus Pettiford, Office of Attorney General
Daniel Persico, Department of Elections
Robert Reese, Virginia State Police
John Singleton, Virginia State Police
Mitchell Smith, Virginia State Police