



Office of the City Auditor

Audit of Select Cybersecurity Controls

Report Date: January 18, 2019

Office of the City Auditor
2401 Courthouse Drive, Room 344
Virginia Beach, Virginia 23456
757.385.5870

"Promoting Accountability and Integrity in City Operations"



Office of the City Auditor

"Promoting Accountability and Integrity in City Operations"

Lyndon Remias, CPA

Gretchen Hudome, CIA, CRMA

City Auditor

Deputy City Auditor

www.vbgov.com/cityauditor

Office of the City Auditor

2401 Courthouse Drive, Room 344

Virginia Beach, VA 23456

Telephone: 757.385.5870

Fax: 757.385.5875

Fraud, Waste, and Abuse Hotline 757.468.3330



Office of the City Auditor Transmittal Letter

Date: January 18, 2019
To: David L. Hansen, City Manager
Subject: Audit of Select Cybersecurity Controls



I am pleased to present the report of our Audit of Select Cybersecurity Controls. The objective of our audit was to assess the adequacy of select cybersecurity controls to reasonably reduce the risk of service disruption, data loss and/or data corruption resulting from certain types of cyberattacks.

Findings considered to be of insignificant risk have been discussed with management. We completed our fieldwork on December 3, 2018.

The Office of the City Auditor reports to City Council through the City's Audit Committee and is organizationally independent of all other City Departments. This report is intended solely for the information and use of the Audit Committee, City Council, Department of Information Technology, and appropriate management. It is not intended to be and should not be used by anyone other than these specified parties. However, this report is a matter of public record and its distribution is not limited.

We would like to thank the management and staff of Information Technology, particularly the Information Security and Privacy Office, for their cooperation and responsiveness to our requests during our audit and their receptiveness to questions, recommendations and suggestions.

If you have any questions about this report, or any audit-related issue, I can be reached at 385-5872 or via email at lremias@vbgov.com.

Respectfully submitted,

Lyndon S. Remias, CPA
City Auditor

c: City Council Members
Audit Committee Members
Tom Leahy, Deputy City Manager
Pedro Wallace, Chief Information Officer
Ernie Forni, Information Security and Privacy Office



Office of the City Auditor Table of Contents

Transmittal Letter	i
Purpose	1
Scope	1
Methodology.....	1
Standards	1
Background	2
Findings and Recommendations	6
Conclusion.....	18
Acknowledgements.....	18
Management’s Response.....	Attachment A



Office of the City Auditor Audit of Select Cybersecurity Controls

Purpose

The audit addressed the adequacy of select cybersecurity controls to reasonably reduce the risk of service disruption, data loss and/or data corruption resulting from certain types of cyberattacks.

Scope

The audit covered Information Technology policies, processes and mechanisms in place at the time of the audit.

Methodology

To accomplish our objectives, we performed the following:

- Obtained and reviewed pertinent guidance, laws, regulations, policies and procedures regarding cybersecurity.
- Reviewed the City's policies and processes related to cybersecurity through inquiry and examination of documents and data.
- Met with appropriate staff to discuss policies, processes and procedures related to prevention, detection and response to cybersecurity threats.
- Assessed whether the design of the City's policies and processes are adequate to address prevention and detection of cybersecurity threats and reduce the risk of service disruption, data loss and/or data corruption to an acceptable level.
- Performed analysis and tests of data and processes designed to prevent and detect cyber threats (i.e., access controls, monitoring, logging, training, etc.)
- Investigated anomalies/irregularities.
- Made recommendations, as appropriate, to ensure compliance, improve processes, increase efficiency and reduce the City's risk of service disruption, data loss and/or data corruption.

Standards

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained during this audit provides a reasonable basis for our findings and conclusions based on our audit objectives.

The Office of the City Auditor reports to City Council through the Audit Committee and is organizationally independent of all City Departments. This report will be distributed to the City's Audit Committee, City Council and appropriate management within the City of Virginia Beach. This report will also be made available to the public.



Office of the City Auditor Audit of Select Cybersecurity Controls

Background

A cyberattack is defined as a “deliberate exploitation of computer systems, technology-dependent enterprises, and networks. Cyberattacks use malicious code to alter computer code, logic, or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft¹.” The term “breach” refers to the compromise of confidential or proprietary information maintained in electronic form as the result of a cyberattack.

Cyberattacks against major organizations have been frequent of late and widely publicized in recent years. Examples include both private entities, like Target in 2013 and Marriott/Starwood properties in 2018, and governmental entities, such as the United States Office of Personnel Management (OPM) in 2015 and the ransomware attack on the City of Atlanta in 2018.

Data breaches from cyberattacks result in loss or corruption of data and/or exposure of individuals to harm when personal and confidential data is compromised. Furthermore, breaches are often costly to address and rectify and may harm the reputation of the compromised entity.

The *2018 Cost of Data Breach Study* completed by the Ponemon Institute² reported the average total cost of a data breach in the United States is \$7.91 million. Figure 1, below, provides a summary of the study’s findings related to the United States.

Figure 1. 2018 Cost of Data Breach Study by Ponemon Institute: Results for United States



SOURCE: www.databreachcalculator.mybluemix.net

The Ponemon study also reported an average cost per lost or stolen record containing sensitive or confidential information of \$75 for government sector entities.

Figure 2, provides a summary of the main causes of data breaches in the United States based on the findings of the *2018 Cost of Data Breach Study*: 52% of incidents involved a malicious or criminal

¹ <https://www.techopedia.com/definition/24748/cyberattack>

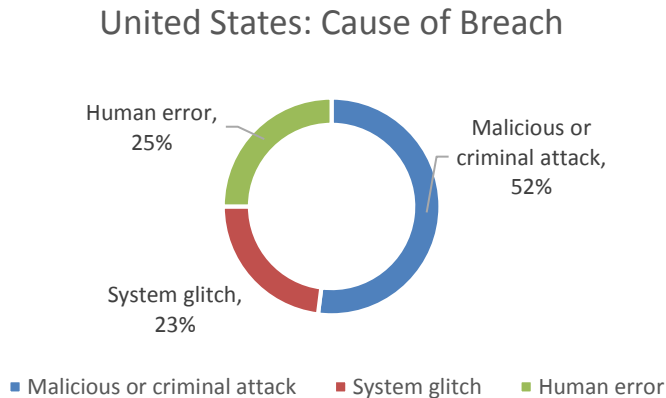
² The Ponemon Institute, founded in 2002, is an independent research center dedicated to privacy, data protection, and information security policy.



Office of the City Auditor Audit of Select Cybersecurity Controls

attack, 25% were due to negligent employees or contractors (human factor) and 23% involved system glitches, including both IT and business process failures.

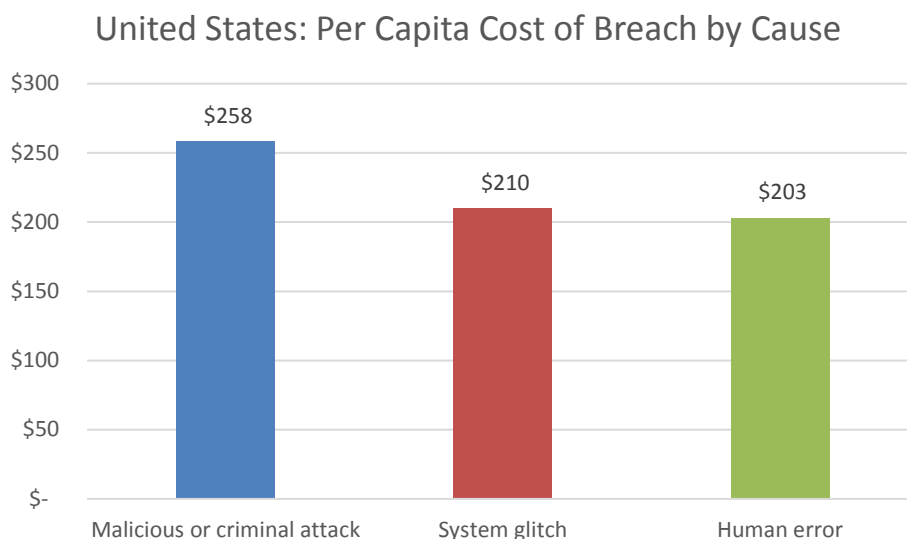
Figure 2. Distribution by Cause of Breach



SOURCE: Poneman 2018 Cost of Data Breach Study

According to the Ponemon study, malicious or criminal attacks are the costliest. The most common types of malicious or criminal attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection. In 2018, the average cost of data breaches due to malicious or criminal attacks in the United States was \$258 per capita. This is significantly higher than the per capita cost for breaches caused by system glitches and human factors, which were \$210 and \$203, respectively.

Figure 3. Per Capita Cost by Cause of Breach



SOURCE: Poneman 2018 Cost of Data Breach Study

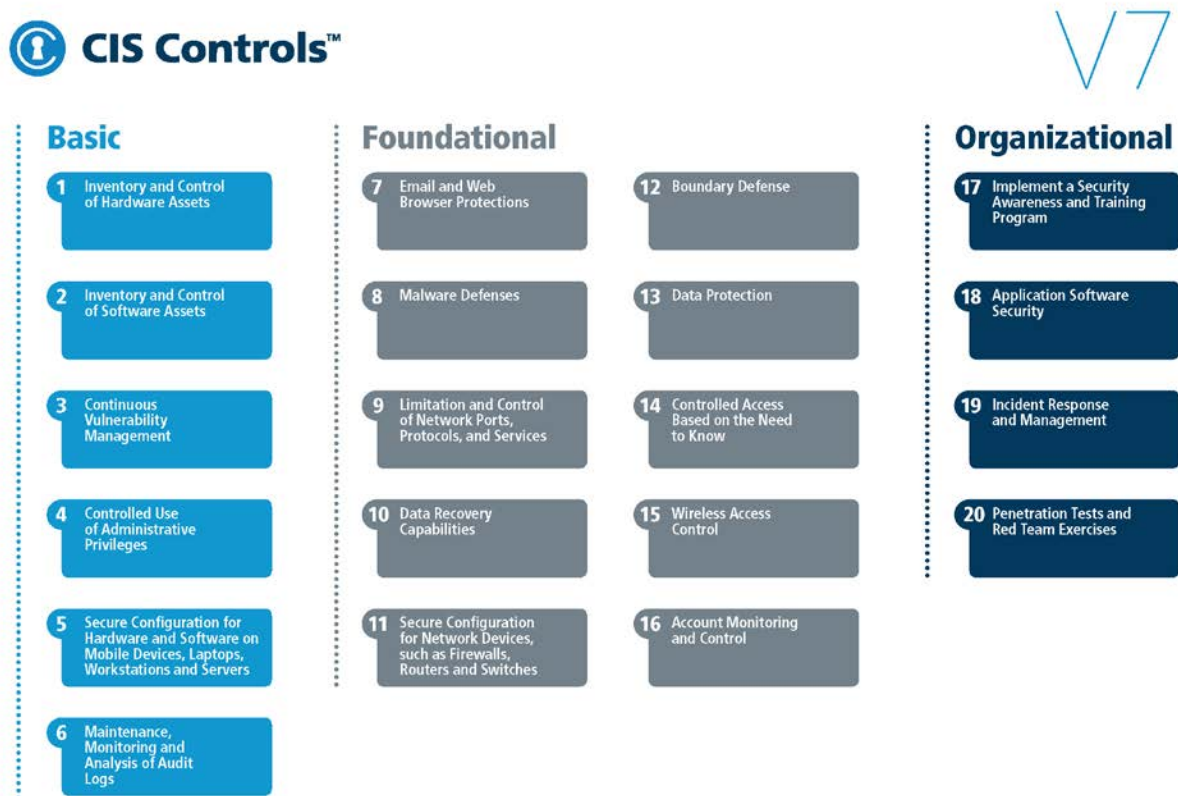


Office of the City Auditor Audit of Select Cybersecurity Controls

Center for Internet Security (CIS)

The Center for Internet Security (CIS) Top 20 Critical Security Controls (previously known as the SANS Top 20 Critical Security Controls) is a prioritized set of best practices created to stop the most pervasive and dangerous threats of today. It was developed by leading security experts from around the world and is refined and validated every year. By adopting these sets of controls, organizations can prevent or quickly detect the majority of cyberattacks. The controls are listed below in Figure 4.

Figure 4. Center for Internet Security Top 20 Controls V7



Department of Information Technology

The City's Department of Information Technology (IT) provides and supports communications, information, and technology solutions to enable City businesses, inform the community, improve and promote quality of life and public safety. Responsibility and coordination of the City's cybersecurity efforts fall primarily under the IT Department and its Information Security and Privacy Office (Info Sec).



Office of the City Auditor Audit of Select Cybersecurity Controls

InfoSec serves to protect the security and privacy of the City's information systems and communications networks. InfoSec's overall role is to:

- Protect the confidentiality, integrity and availability of data in every form
- Provide guidance on how legislation may affect how data is managed
- Perform routine internal and external security assessments
- Educate the City's members regarding information security and privacy issues

InfoSec operates under the direct supervision of the Chief Information Officer (CIO). The Office has four (4) budgeted positions: a Deputy Chief of Information Security; a System Engineer III and two System Engineer IIs. The Deputy Chief of Information Security position is currently vacant.

Our audit focused on the City's policies, procedures and tools as they relate to select CIS Top 20 controls.



Findings and Recommendations

1. Ensure the accuracy and completeness of IT hardware inventory data

Inventory and Control of Hardware Assets (CIS Control 1)

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

This control addresses the need to know what is on your network and to use information gathered to detect and/or prevent unauthorized users and devices from connecting to the network. The inventory and control of hardware assets complements other CIS Top 20 controls such as network access, asset configuration, system management and incident response.

Recommended practices (sub-controls) in this area include:

- Utilize both active and passive discovery tools to identify assets and update inventory.
- Use of Dynamic Host Configuration Protocol (DHCP) to update asset inventory.
- Maintain an accurate, up-to-date, and detailed inventory of all technology assets.
- Ensure unauthorized assets are identified and removed, quarantined, or added to the inventory in a timely manner.
- Utilize port level access control tied to the hardware asset inventory to authenticate to the network.
- Use of client certificates to authenticate hardware assets.

A key component of asset management is the initial and ongoing IT hardware inventory. Information should be accurate, complete and current. The City currently uses Solar Winds Web Help Desk (WHD) to record and maintain its IT asset inventory. The current process relies heavily on individual reporting and centralized manual batch processing. Uploads to WHD are not reconciled to source documentation on a regular basis. Nor, is there a consistent process in place to ensure all asset status changes are recorded. The City also uses System Center Configuration Manager (SCCM) to identify, manage and maintain assets connected to the City's networks through remote control, patch management, operating system deployment, network protection and other services.

At the time of our audit, there were 19,492 IT hardware assets listed as "*in service*" in WHD. **Exhibit 1** provides a summary of the *in service* assets by type.



Office of the City Auditor Audit of Select Cybersecurity Controls

Exhibit 1. In Service Hardware Assets by Type

Asset Type	Number In Service per WHD
Desktop Computer	5,622
Display	7,965
Dock	1,028
iPad	22
Laptop	915
Mobile Comm	2
Network	22
Peripherals	3,681
Printer	28
Smartphone	30
Tablet	177
Total	19,492

Source: WHD Extract of In Service Assets as of September 27, 2018

We reviewed the WHD asset inventory data and found a number of inconsistencies and/or omissions in key fields such as Asset Number, Serial Number, and Location. **Exhibit 2** provides a summary of the inconsistencies by type.

Exhibit 2. Summary of Exceptions by Exception Type

Exception Type	Number of Exceptions	Percentage of Population
Duplicates	105	0.5%
Serial number is blank	237	1.2%
Location is blank	3,746	19.2%
Department is blank	1,049	5.4%
Location and department are blank	319	1.6%

Source: WHD Data Extract of In Service Assets as of September 27, 2018

We selected a random sample of recent IT hardware purchases and traced the items purchased from the invoice to WHD inventory records. The results of our sample are presented in **Exhibit 3**.

Exhibit 3. Sample Results

Results	Number of Items	% of Sample
Located in WHD	35	68.6%
Not in WHD, Added	11	21.6%
Not Found	5	9.8%
Total	51	100.0%

IT is in the process of implementing a new asset/service management tool called ServiceNow. ServiceNow uses an asset first, person second approach to document the full asset management lifecycle (planning, procurement, deployment, managing, replacement, and retirement) and the associated workflows. Implementation of ServiceNow's asset management and inventory



Office of the City Auditor Audit of Select Cybersecurity Controls

capabilities is expected to begin following the completion of a third party physical inventory of the City's IT assets. The expected go live timeline is late 2019.

ServiceNow is workflow driven. Development of standard asset management workflows (i.e., procurement, installation, moves, removal, replacement, and disposal) and incorporating asset management requirements within other workflows that both directly and indirectly impact the asset management lifecycle (i.e., granting and removal of employee access rights, troubleshooting, repair and maintenance) will not only ensure consistency of services but result in complete, accurate and current asset information. ServiceNow includes an automated discovery component which will detect and record assets installed (in use) on the City's networks.

The implementation of ServiceNow will enhance the quality and accuracy of the information within the asset management tool and the City's ability to identify new and/or unauthorized devices.

Recommendations

To enhance the City's ability to identify, record and control IT hardware assets, management should:

- 1.1 Review assets with a current status other than in service (i.e., received, CR hold, etc.) to ensure status is correct.
- 1.2 Reconcile the third party physical inventory to asset data from WHD and SCCM. Discrepancies should be investigated and resolved.
- 1.3 Incorporate asset management requirements in the development of all ServiceNow workflows that impact the IT asset management lifecycle.
- 1.4 Ensure features that allow tracking (i.e. auditing) of all changes to asset information are activated within ServiceNow.
- 1.5 Implement a quality assurance process to ensure the City's IT hardware asset inventory is accurate, complete and current.
- 1.6 Develop a process for departments to verify IT assets on hand annually.



2. Enhance ability to collect and analyze security event logs through expansion of bandwidth

Continuous Vulnerability Management (CIS Control 3)

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, and to remediate and minimize the window of opportunity for attackers.

Organizations operate in a constant stream of new information: software updates, patches, security advisories, threat bulletins, etc. Understanding and managing vulnerabilities has become a continuous activity requiring significant time, attention and resources. Attackers have access to the same information and take advantage of gaps between the identification of vulnerabilities and remediation.

Figure 5. Vulnerability Management Tools



Identifying and remediating vulnerabilities on a regular basis reduces an organization's risk of having their computer systems compromised. It is also essential to a strong overall information security program.

Recommended practices (sub-controls) in this area include:

- Use of automated vulnerability scanning tools.
- Perform authenticated vulnerability scanning.
- Protect dedicated assessment accounts.
- Deploy automated system patch management tools.
- Deploy automated software patch management tools.
- Compare back-to-back vulnerability scans.
- Utilize a risk rating process.

The City's Information Security and Privacy Office (InfoSec) is responsible for the vulnerability management process, the main objective of which is to identify, detect and remediate vulnerabilities in a timely fashion. In order to achieve this objective, InfoSec uses a wide array of tools to scan, capture, and monitor events and activities.

We reviewed the vulnerability identification, monitoring, reporting and remediation processes, supporting documentation and results with InfoSec.



Office of the City Auditor Audit of Select Cybersecurity Controls

Current licensing and bandwidth limitations impact the full automation of the City's vulnerability management process. InfoSec has implemented work arounds to address the limitations, but the work arounds are time-consuming and cumbersome.

Based on our review, we determined the City's processes and procedures related to continuous vulnerability management, for the most part, meet the best practice criteria defined within the CIS Control framework, but would greatly benefit from enhancement of the event security management system and scanning capabilities.

Recommendation

We offer the following recommendation to enhance the capabilities of the City with regard to continuous vulnerability management:

- 2.1 Pursue the purchase of increased bandwidth and licensing for log management and vulnerability management tools.



3. Enhance security control over administrative privileges

Controlled Use of Administrative Privileges (CIS Control 4)

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

The misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise. If administrative privileges are loosely and widely distributed, used for everyday activities or allow passwords used on less critical systems, the attacker has a much easier time gaining full control of accounts that can act as avenues for the attacker to compromise administrative privileges.

Recommended practices (sub-controls) in this area include:

- Maintaining an inventory of administrative accounts.
- Change default passwords before deploying new assets.
- Ensure the use of dedicated administrative accounts for elevated activities.
- Use unique passwords.
- Use multifactor authentication for all administrative access.
- Use of dedicated machines for all administrative tasks.
- Limit access to scripting tools.
- Log and alert on changes to administrative group membership.
- Log and alert on unsuccessful administrative account login.

The City's Account Management Policy governs the assignment and use of administrative privileges. A privileged account as "an account which has more privileges than a normal user." Privileged accounts are used to manage the system and are also known as elevated access.

Administrative privileges should be heavily restricted to only those users whose jobs, and more specifically tasks, require such privileges. Regular or normal users of a system do not require administrative privileges to perform daily tasks.

Privileged accounts are not necessary and, should not be used, for most normal business functions and routine tasks such as checking email or searching the internet. The City does not require privileged users to have separate user accounts for normal business functions.

The City does not use multifactor authentication or dedicated machines for administrative tasks.

Log and alert activity for changes to privileged group membership and login activity is monitored by InfoSec.



Office of the City Auditor Audit of Select Cybersecurity Controls

We reviewed membership for each of the City's privileged user groups as well as the processes for requesting and granting privileged access. We noted that members of the IT Executive Team are members of the domain-wide Desktop Computer Admins group.

Recommendations

To enhance the City's security practices related to privileged users and accounts, we recommend:

- 3.1 Implement multifactor identification for privileged user accounts.
- 3.2 Review all privileged user accounts to ensure regular access is required.
- 3.3 Require the use of separate accounts for elevated tasks.
- 3.4 Ensure password requirements for privileged accounts meet the latest National Institute of Standards and Technology (NIST) standards.



4. Enhance adherence to best practices related to account management

Account Monitoring and Control (CIS Control 16)

Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult.

Recommended practices (sub-controls) in this area include:

- Maintain an inventory of authentication systems.
- Configure access for all accounts through as few centralized authentication points as possible.
- Require multifactor authentication for all user accounts, on all systems.
- Encrypt or hash all authentication credentials.
- Encrypt transmittal of username and authentication credentials.
- Maintain an inventory of accounts.
- Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities.
- Disable any account that cannot be associated with a business process or business owner.
- Automatically disable dormant accounts.
- Ensure all accounts have an expiration date.
- Automatically lock workstation sessions after a standard period of inactivity.
- Monitor attempts to access deactivated accounts.
- Alert when users deviate from normal login behavior, such as time of day, workstation location and duration.

City policy requires termination of Active Directory (AD) accounts upon separation from employment and those that are inactive for 90 days. Processes are in place to identify and delete inactive accounts; and disable terminated and/or separated employee accounts upon termination/separation.

We obtained and reviewed an extract of the 9,834 active AD accounts. A summary of the results of our review of active accounts is provided in **Exhibit 4**, on the next page.



Office of the City Auditor Audit of Select Cybersecurity Controls

Exhibit 4. Active Accounts by Type

Account Type	Managed	Unmanaged	Other	Total	Never Logged On	Inactive > 45 Days	%
Accounts			2	2		1	50%
Applications			194	194	116	34	77%
BuiltIn			1	1	1	0	100%
New Users			3	3	3	0	100%
Servers			1	1		1	100%
Test Users	4			4		2	50%
Users	8,585			8,585	660	474	13%
Users Disabled		50		50	5	12	34%
Users Utility Accounts		962		962	405	174	60%
None			32	32	15	2	53%
Total	8,589	1,012	233	9,834	1,205	700	19%

We found 1,905 active accounts (19%) that had either never logged on or had been inactive for more than 45 days.

Recommendations

Management should consider the following in order to further enhance adherence to best practices in relation to account management:

- 4.1 Implement multifactor identification for remote access. Consider implementing multifactor authentication for all network access.
- 4.2 Update scripts used to manage accounts to include identifying and removing accounts that have not logged on within 90 days of creation.
- 4.3 Use groups to identify and manage temporary employees.
- 4.4 Regularly review application and user utility accounts to ensure continued necessity.
- 4.5 Confirm accounts periodically with departmental management.
- 4.6 Ensure contracts for vendors requiring access to the City's network include appropriate cybersecurity language.
- 4.7 Consider changing password requirements for privileged accounts to meet the latest National Institute of Standards and Technology (NIST) standards.



5. Promote security awareness through training

Implement a Security Awareness and Training Program (CIS Control 17)

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

It is easy to think of cybersecurity primarily as a technical challenge, but the actions of people play a critical role in the success or failure of an entity's cybersecurity program.

Attackers know this and plan their attacks by designing phishing messages that look like routine and expected traffic to the unsuspecting user; exploiting the gaps between policy and technology (e.g., policies that have no technical enforcement); working within the time window of patching or log review; using nominally non-security-critical systems as jump points or bots.

In order to effectively limit cyber risk, this fundamental vulnerability, often referred to as the 'human factor', must be addressed.

Recommended practices (sub-controls) in this area include:

- Perform a skills gap analysis.
- Deliver training to fill the skills gap.
- Implement a security awareness program.
- Update awareness content frequently.
- Train workforce on secure authentication, identifying social engineering attacks, handling sensitive data, and causes of unintentional data exposure
- Train workforce on identifying and reporting incidents.

Security Awareness Training and Education (SATE) is key to eliminating the City's exposure to both malicious threats and accidental errors and omissions. SATE is not only defined as industry best practice, it is also a statutory requirement for dealing with sensitive information as defined in the Health Insurance Portability and Accountability Act (HIPAA).

The term "Security Awareness" is considered the daily "moment-by-moment" awareness level while the term "Security Training" relates to the rudimentary training all employees need to build their basic security skills.

The City's Security Awareness, Training and Education Policy sets forth a minimum standard for SATE to reduce the City's risk. Each department is responsible for ensuring that all employees are trained to at least this minimum standard.



Office of the City Auditor Audit of Select Cybersecurity Controls

All newly hired, full time City members receive at least two hours of Security Awareness training as part of their New Member Orientation. This training is provided on “Day 2” of the New Member Orientation program. New members generally attend “Day 2”, 30-45 days after beginning work. Additional security training may be required if the member has access to sensitive information (i.e., Criminal Justice Data or Personal Health Information).

We reviewed “Day 2” attendance/enrollment records for the six-month period of February 2017 through July 2017. 95.5% the new hires in our sample attended this training or received the training through a public safety academy program.

New Member Orientation is not available for part-time members, temporary employees, contractors and/or vendors. Therefore, it is left to the respective departments to ensure these members receive the required training.

Additional live training programs are available through the HR/Training and Development Catalog, and an annual refresher is available online.

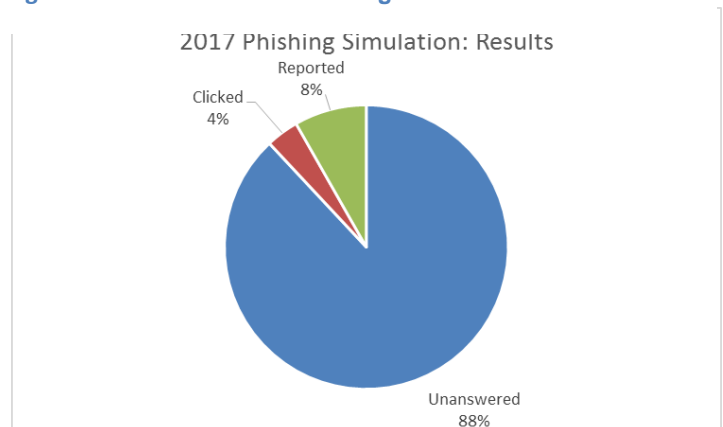
All users with City email accounts are required to complete the online refresher annually.

Implementation of Taleo and recent changes to the City’s online training capabilities have delayed the rollout of the annual refresher course. The last offering was calendar year 2016.

To address this, and complement available live programs, InfoSec is in the process of implementing an ongoing awareness training and management program developed by the SANS Institute.

To test cybersecurity awareness, InfoSec periodically conducts restricted phishing attempts. These in-house endeavors, although beneficial for assessing employee vulnerabilities, are manually designed and executed and tend to be resource intensive and metrics associated with the response are difficult to gather and analyze. See Figure 6, for the results of the 2017 internal phishing simulation. Of the 4,000 emails sent, 3,521 went unanswered, 149 users clicked on the link provided and 330 users reported the email as suspicious.

Figure 6. Results of 2017 Phishing Simulation





Office of the City Auditor Audit of Select Cybersecurity Controls

Recommendations

To enhance the City's cybersecurity awareness program and reduce the City's risk associated with the "human factor", we recommend the following:

- 5.1 Require completion of a basic overview of the City's security awareness and acceptable use requirements prior to allowing initial system access (i.e., at initial log on or within a limited time) for **all** new users, including full-time, part-time, temporary, contractors and vendors.
- 5.2 Explore opportunities to acquire complementary modules (i.e., phishing) in conjunction with the SANS training program.
- 5.3 Enforce annual refresher requirements through disabling or limiting user access until completion.



Office of the City Auditor Audit of Select Cybersecurity Controls

Conclusion

Based on the results of our audit, the policies and procedures in place are adequate to reasonably reduce the risk of service disruption, data loss and/or data corruption resulting from certain types of cyberattacks, except as noted herein.

Acknowledgements

We would like to thank the management and staff of Information Technology, particularly the Information Security and Privacy Office, for their cooperation and responsiveness to our requests during the audit and their receptiveness to questions, recommendations and suggestions.



City of Virginia Beach


INFORMATION TECHNOLOGY
 (757) 427-4121
 FAX (757) 426-5782
 TDD (757) 427-4305

VBgov.com
 MUNICIPAL CENTER
 BUILDING TWO
 2405 COURTHOUSE DRIVE
 VIRGINIA BEACH, VA 23456-9115

INTER-OFFICE MEMORANDUM

DATE: January 4, 2019

TO: Lyndon S. Remias, City Auditor

FROM: Pedro "Peter" Wallace, Chief Information Officer 

SUBJECT: Audit of Select Cybersecurity Controls

On 4 December 2018, the Office of the City Auditor provided a report to the Information Technology (IT) Department addressing the adequacy of select cybersecurity controls. The report included 21 recommendations. The Information Security (InfoSec) Office worked with other teams in the IT Department to provide solutions for the recommendations from the report. Audit's recommendations with the IT Department's responses are listed below.

1.1 Review assets with a current status other than in service (i.e., received, hold, etc.) to ensure status is correct.

IT Response: Current status of assets will be available when Service Now is implemented. The implementation of the Asset Management module is in its final stages. We expect to be managing assets in Service Now by 4th quarter 2019.

1.2 Reconcile the third party physical inventory to asset data from Web Help Desk and System Center Configuration Manager. Discrepancies should be investigated and resolved.

IT Response: The End User Computing (EUC) Team conducts routine record maintenance on inventory records. Quarterly inventory spot checks will validate inventory discrepancies with documented causative research. The implementation of the Asset Management module is in its final stages. We expect to be managing assets in Service Now by 4th quarter 2019.

1.3 Incorporate asset management requirements in the development of all Service Now workflows that impact the IT asset management lifecycle.

IT Response: The Service Now implementation team and the Program Manager (PM) have incorporated IT asset management Lifecycle in the development of Service Now. The program is within 6 months of implementation.

1.4 Ensure features that allow tracking (i.e. auditing) of all changes to asset information are activated within Service Now.

IT Response: The Service Now implementation team and PM have incorporated audit functions with the modules in the development of Service Now. The Auditing function will be used to validate the inventory within the first 2 months of implementation.

1.5 Implement a quality assurance process to ensure the City's IT hardware asset inventory is accurate, complete and current.

IT Response: The Service Now implementation team and PM have incorporated audit functions with the modules in the development of Service Now. The Auditing function will be used to validate the inventory within the first 2 months of implementation. The IT EUC policy has been updated to reflect sample sizes and periodicity of audits.

1.6 Develop a process for departments to verify IT assets on hand annually.

IT Response: The IT EUC policy has been updated to reflect sample sizes and periodicity of audits. The inventory validation process will be re-evaluated after 6 months of using Service Now to manage assets. An analysis will be conducted for process improvement and gap analysis of Service Now.

2.1 Pursue the purchase of increased bandwidth for Splunk in order to allow correlation of all available log data.

IT Response: In the 2020 Fiscal Year budget proposal for the InfoSec Office, additional funds have been requested in order to double the existing bandwidth for the Security Event Management tool used by InfoSec. These funds will be available in July 2019. The increased bandwidth will allow security logs from newly added key devices to be forwarded to the event management tool. Planning for additional budget dollars to include new systems has been included in the IT Master Technology Plan 2.0.

3.1 Implement two factor identification for privileged user accounts.

IT Response: The InfoSec Office is investigating incorporating multi-factor authentication for accessing privilege accounts. We will have to identify which accounts would be included in the definition of privileged accounts and get a cost projection for a third party application. The InfoSec Office will work the Converged Architecture (CA) Team to develop a budget proposal for multifactor authentication.

3.2 Review all privileged user accounts to ensure regular access is required.

IT Response: The InfoSec Office will update the Account Management Policy to require annual auditing of the privileged account groups. The updated policy will be included in the 2019 InfoSec Policy review which will be completed in the 2nd quarter of 2019.

3.3 Require the use of separate accounts for elevated tasks.

IT Response: Currently, the Domain Administration group contains separate accounts for tasks that require Domain Administrator access. The InfoSec Office recommends that we use multi-factor authentication for access to the Domain Administration, File Administration, and Desktop Administration groups.

3.4 Ensure password requirements for privileged accounts meet the latest National Institute of Standards and Technology (NIST) standards.

IT Response: We currently meet NIST standards for minimum password length and complexity. NIST recommends excluding passwords that have been previously compromised by hackers and breaches. In order to collect and exclude these previously disclosed passwords, we will have to implement a third-party solution, as Active Directory does not include this feature. The InfoSec Office will investigate the costs of a third-party solution to meet NIST's requirement.

4.1 Implement two-factor identification for remote and/or Virtual Private Network (VPN) access. Consider implementing two-factor authentication for all network access.

IT Response: We currently implement two factor authentication for VPN access through the Microsoft Threat Management Gateway. We are investigating a new remote access architecture that will use multi-factor authentication.

4.2 Update scripts used to manage accounts to include identifying and removing accounts that have not logged into the network within 90 days of creation.

IT Response: The CA Team will run an additional script monthly to disable accounts not accessed within 90 days. The results of disabling the accounts will trigger the current process to remove them. This change will be implemented during the 2nd quarter of 2019.

4.3 Use groups to identify and manage temporary employees.

IT Response: The InSite system needs to include a way to identify temporary employees. In order to manage a group of users, we need a trusted source to identify temporary employees. We will have to coordinate with the Human Resources Department on a method to identify temporary employees.

4.4 Regularly review application and user utility accounts to ensure continued necessity.

IT Response: The InfoSec Office will conduct semiannual reviews with Solutions Engineering, the CA team, and Application Development team. The InfoSec Office will

also investigate the opportunity to purchase a tool to assist with service account management.

4.5 Confirm accounts periodically with department management.

IT Response: The InfoSec Office will investigate tools to help catalog account access and create a process for confirming account access with departments.

4.6 Ensure contracts for vendors requiring access to the City's network include appropriate cybersecurity language.

IT Response: We will work with purchasing to ensure that city contracts include cyber security language.

4.7 Consider changing password requirements for privileged accounts to meet the latest NIST standards.

IT Response: We currently meet NIST standards for minimum password length and complexity. NIST recommends excluding passwords that have been previously compromised by hackers and breaches. In order to collect and exclude these previously disclosed passwords, we will have to implement a third-party solution, as Active Directory does not include this feature. The InfoSec Office will investigate the costs of a third-party solution to meet NIST's requirement. We recommend that we use multi-factor authentication to authenticate access to privileged accounts.

5.1 Require completion of a basic overview of the City's security awareness and acceptable use requirements prior to allowing initial system access (i.e., at initial log on or within a limited time) for **all** new users, including full-time, part-time, temporary, contractors and vendors.

IT Response: We will coordinate with Human Resources to investigate methods for delivering training to employees as they receive their network accounts.

5.2 Explore opportunities to acquire complementary modules in conjunction with the System Administration and Network Security (SANS) training program.

IT Response: The InfoSec Office is requesting an increase in the annual budget to pay for cyber security awareness training for all employees. Once the cost for the basic training has been added to the budget, we can evaluate the costs for additional training modules.

5.3 Enforce annual refresher requirements through the limiting of user access until completion.

IT Response: The InfoSec Office is piloting a new cyber awareness program that will be contracted through SANS. The training will be mandatory for city members with email accounts, including volunteers and contractors. The new awareness training will be implemented during the 1st quarter of 2019.