Commonwealth of Massachusetts
OFFICE OF THE COMPTROLLER
One Ashburton Place, 9th Floor
Boston, Massachusetts 02108
(617) 727-5000
macomptroller.org

William McNamara
Comptroller

CYBERSECURITY LESSONS LEARNED

Last Updated: October 18, 2021

Overview

Over the past few years cyberattacks against organizations, from large government Departments to small businesses, have been steadily growing, with hackers specifically targeting employees (phishing). Phishing attacks are still a leading form of cyber-crime. When combined with social engineering, ransomware, identity theft, etc. cyberattacks are becoming more sophisticated and a persistent threat in our workplace. The Commonwealth has engaged expert firms to help remediate several of these unfortunate cyber incidents and advise Departments of the proper policies and procedures to improve overall cyber hygiene. Below are some lessons learned to assist Departments with building appropriate cyber security internal controls, protections, and strategies.

Department Related Observations

1. All state employees need continuous training on their role in preventing cyber-attacks.
2. Departments have varying degrees of sophistication in IT infrastructure, number and skillsets of IT staff.
3. Use of separate networks, segmenting networks and segregating sensitive, confidential and other protected data, reduces the risk for financial and banking function losses and fraud.
4. Some Departments lack detailed network diagrams, user access management and IT inventory controls. Departments that have conducted assessments for Payment Card Industry (PCI) compliance for accepting credit cards and other security assessments are better positioned for expedited containment in a cyber event with updated Department documents.
5. Department Security Officers (DSOs) could benefit from additional training on the business purposes of security roles and how to evaluate roles to ensure sufficient access with appropriate segregation of duties.
6. Segregating and securing Personally Identifiable Information (PII), sensitive and confidential data in accordance with state and federal privacy laws, are mandatory internal controls for all Departments for legal and fiscal compliance due to the extreme costs to mitigate data breaches.

7. Budgeting for resources for data and network management (even if cloud storage used), cyber awareness training, risk assessments and technology detection and protection tools should be included as part of the Department's annual budget request since preventing cybersecurity disruptions and losses is a necessary Department operational standard for fiscal responsibility and minimum internal controls. The following are routine controls that should be in place. Are you adequately funded in your budget to achieve the following:
    a. Annual review of your data management inventory (data and network maps). Do you have an inventory of data types, classifications, and network maps where data travels or is stored (onsite or virtually)?
    b. Annual review of data backup management. Do you implement "3-2-1" model of backups with multiple mediums, multiple locations and segregated backup that is air-gapped or not connected to the network or internet? Do you have process in place to segregate backups to ensure that files infected with malware are not backed up and overwrite clean files?
    c. Annual update your cyber risk assessment and Internal Control Plan (including Business Continuity, Disaster Recovery and Incident Response Plans)
    d. Annual test of your Incident Response, Disaster Recovery, and Business Continuity plans to ensure you can restore applications and files to full operation.
    e. Annual review of your process for monitoring, detecting, testing and remediating vulnerabilities and cyber-attacks.
    f. Annual and ongoing periodic Cyber Awareness Training for all staff.
    g. Sufficient trained technology and compliance staff to manage above internal controls.

The Top Two (2) Cybersecurity Recommendations

1. **Security Awareness Training**. With many staff teleworking and working hybrid schedules, the perimeter of security controls remains extensive. Research shows that phishing is the leading cause of cyber-attacks. Provide continuous security awareness training to all staff and contractors on the latest cyber threats and red flags. Tips:
    - Provide staff with teleworking tips and protocols. Use these Telework Cyber Tips to prevent operational disruption from a ransomware attack.
    - When in doubt, check it out. Do not respond to emails, texts or calls UNLESS you have personally verified (with information on file) that the request is expected and legitimate

For assistance with cybersecurity issues, internal controls and to report Cyber Incidents and suspicious activity contact: CTREmergencyNotification@mass.gov. See CTR Cyber at https://www.macomptroller.org/ctr-cyber for additional Cyber resources.

- Do not click on links or attachments in emails, and do not "enable macros/content" in email attachments. Have your IT staff scan email attachments or scan yourself
- Never provide your log in credentials (usernames/passwords) in response to any requests in emails. Validate that the email is legitimate
- Verify personally with the requester (with information in file) before you make any changes to high-risk items, such as bank accounts, payment addresses, EFT or direct deposits etc.
- Notify IT immediately of any suspicious emails or activity
- Users with elevated security access privileges or security responsibilities should underdo additional training to ensure they manage security roles with appropriate internal controls
- See CTR Cyber page for additional Cyber Awareness Training resources
- Send staff the weekly Cybersecurity Tip issued in the weekly E-Update or refer staff to the CTR Cybersecurity Tips and Alerts page.

2. **Continuous Updating and Patching Protocol**. Many avoidable system compromises occur because of unpatched known software vulnerabilities. Attackers continue looking for vulnerabilities. Set up a rigorous process to keep servers, desktops, virtual teleworker laptops/PCs, operating systems and third-party applications up-to-date with anti-virus software and security patches/updates to ensure that vulnerabilities are not created or exploited. Patching programs and policies should include third party applications, third parties handling Department data and any "smart" device connected to the network (printers, scanners, cameras etc.) Third party applications and smart devices can serve as an entry point for attacks and malware in the network.

Strategic Recommendations

3. **Incident Response Plan**. Have an updated Incident Response Plan that clearly identifies the resources and processes should a cyber-incident occur. As part of the Department Internal Control Plan include an updated Incident Response Plan that clearly identifies the critical tasks, resources and processes that could potentially be impacted due to a cyber incident, and a plan of containment and remediation. In addition, the Incident Response Plan should have a process to record and keep artifacts and copies of compromised files, screen shots and other logs in separate repository for forensics investigation. Incident Response Plans should coordinate with the Internal Control Plan (which should include the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)).

For assistance with cybersecurity issues, internal controls and to report Cyber Incidents and suspicious activity contact: CTREmergencyNotification@mass.gov. See CTR Cyber at https://www.macomptroller.org/ctr-cyber for additional Cyber resources.

4. **Risk Assessments and Internal Controls**. As part of the required Internal Control Plan, Departments should conduct a risk assessment to identify the data and systems assets that need to be maintained and secured from a cyber-incident. The Department should also develop a strategic plan to continually monitor and secure these assets from cyber-threats.

    a. **Business Continuity Plan (BCP).** Internal Control Plans should include a Business Continuity Plan that identifies critical tasks and how these are maintained in the event of a business, supply chain, technical or other disruption.

    b. **Disaster Recovery Plan (DRP).** Internal Control Plans should also include a Disaster Recovery Plan that identifies how critical tasks will be managed in the event of an environmental, health, supply chain or technology disaster.

    c. **Plan B Considerations**. Work with your staff to identify a "Plan B" if critical systems are taken off-line. Below is a five-step plan to consider, using the internal control plans you already have in place:
        i. Identify your critical operational tasks.
        ii. Identify the networks, systems, third-party software, and other entities that you depend on to achieve your critical tasks.
        iii. Develop processes and workarounds to manage these critical tasks without email and technology at each step of the process.
        iv. Test and retest these processes to identify risks and weaknesses, and continue training staff on cyber awareness.
        v. Update your Incident Response, Business Continuity, and Disaster Recovery Plans with your Plan B processes.
        vi. Developing and testing your Plan B can greatly improve risk assessments across the Enterprise and improve security at each step to reduce the chances of a cyber incident.

    d. Statewide Contract ITS78 has qualified contractors available to assist with risk assessments, mitigation and remediation plans, and incident response preparation to ensure that the Internal Control Plan is complete.

5. **Department Security Policies**. Draft and implement Department data management and system security policies. Executive Departments are required to follow the Enterprise Security Policies issued by the Executive Office for Technology, Security and Services. (EOTS). Non-Executive Departments are required to follow either the EOTS Enterprise Security policies as the default Commonwealth standard or comparable Department standards as part of their Internal Control Plans. See: **EOTSS Enterprise Security Policies and Standards.**

For assistance with cybersecurity issues, internal controls and to report Cyber Incidents and suspicious activity contact: CTREmergencyNotification@mass.gov. See CTR Cyber at https://www.macomptroller.org/ctr-cyber for additional Cyber resources.

6. **Asset and Data Security Management.** Maintain a centralized asset management system to track internal assets, their locations, and the asset owners. Properly identify and secure (encrypt, store) confidential data separate from other operational data. Unsecured sensitive and confidential data that resides on PCs, networks, servers, mobile devices can be breached if these assets are compromised. Every Department should have a data management policy and plan to encrypt this data, securely manage the encryption keys, and manage the lifecycle of the encryption keys. Staff should be trained on how to manage files and how to secure and store confidential data.

7. **Network Documentation**. Department networks and devices are fluid. The Department should always keep network diagrams, data flows and records of updates current, which improves the ability to properly patch and keep applications up to date, as well as assisting with remediation in a cyber incident. The first documents needed for risk assessments and incident responses are network diagram, data flows and other network documentation.

8. **Secure Transmission**. Disable macro scripts from office files transmitted over e-mail. Encrypt all emails with PII, sensitive or confidential data. Ensure that any data travelling from the Department to a 3rd party vendor, or to a cloud provider is encrypted in transit, and at rest. Validate that all vendors handling or storing Department data is maintaining the cybersecurity requirements outlined in the **EOTSS Enterprise Security Policies and Standards.**

9. **Software Restrictions**. Implement software restriction policies or other controls to prevent programs from being executed from common ransomware locations (e.g., temporary folders supporting popular Internet browsers, compression/decompression programs).

10. **Access Management.** Local administrative rights should not be present on users' computers. Limit the use of shared privileged accounts and remove unused accounts. Define users and machine configurations in different user groups based on their roles so that appropriate group policies can be applied. Perform a regular audit of Active Directory permissions. Access should be limited to what is needed to perform role and securing sensitive files and networks with restricted access is highly recommended.

11. **Report to CTR**. Since employees of the Commonwealth of Massachusetts are often using enterprise systems, it is critical to notify the Office of the Comptroller (CTR) to ensure enterprise systems are protected. Contact us at: CTREmergencyNotification@mass.gov. Ransomware and other viruses can quickly spread and disrupt operations and compromise data. In all recent incidents when Departments "thought" their remediation was complete, 3rd party vendors discovered latent and hidden malware that could have been deployed at a later date, or malware that was not fully removed. CTR can often provide expertise to assist Departments during a cyber incident, as well as support to continue fiscal transactions if the Departments systems are offline.

For assistance with cybersecurity issues, internal controls and to report Cyber Incidents and suspicious activity contact: CTREmergencyNotification@mass.gov. See CTR Cyber at https://www.macomptroller.org/ctr-cyber for additional Cyber resources.

12. **Report to EOTSS**. Executive Departments supported by EOTSS should immediately report any suspicious activity or an incident to their IT staff and to the EOTSS helpdesk.

13. **Contact the FBI** (at www.IC3.gov). Report suspicious email addresses, bank account change requests on where funds were, or were attempted to be, redirected. The FBI collects information about cyberattacks, successful breaches and cyber-attack attempts.

14. **Contact Banks**. Department banks should be notified in the event of a known or suspected cyber-incident to alert them to the incident and ensure that access to online banking systems are suspended until a due diligence review confirms that there is no threat. Hidden malware may have scraped bank log-in credentials, so this extra step to notify the bank, change passwords and other controls are encouraged even if a wide cyber incident may not have happened.

    a. Ensure that positive pay and other restrictions are put on payments so that the bank won't pay unless it matches a separate payment file authorization, which prevents fraudulent checks from being cashed.

    b. Set up extra controls to validate specific people at the bank or a validation process is in place (with PINs or other validation steps) to prevent cybercriminals posing as bank employees to gains access to your credentials or bank accounts.

    c. Never provide any credentials over email, text or phone unless you have validated (through direct contacts already on file) that the request is legitimate.

    d. Using separate PCs/laptops for banking that is not connected to the regular network provided additional protection.

15. **Contact Local Police**. Local law enforcement should be contacted to log an official report when there is a cyber fraud, theft, or identify theft incident.

16. **Mandatory State Reporting**.

    a. MGL Chapter 93H, and its corresponding regulations (201 CMR17.00), require reporting to the Attorney General and the Director of Consumer Affairs and Business Regulation of any *"known security breach or unauthorized use of personal information."*

    b. Chapter 647 of the Acts of 1989 requires that *"…variances, losses, shortages or thefts of funds or property shall be immediately reported to the state auditor's office…"*

For assistance with cybersecurity issues, internal controls and to report Cyber Incidents and suspicious activity contact: CTREmergencyNotification@mass.gov. See CTR Cyber at https://www.macomptroller.org/ctr-cyber for additional Cyber resources.

Technical Recommendations

- **Layered Virus and Malware Protections.** Implement a full-featured virus and malware protection software suite that offers layers of protections, such as signature recognition and behavioral detection heuristics capabilities, across the entire infrastructure - including all endpoints and mobile devices - and update frequently. Behavioral detection anti-virus options are superior to signature-based antivirus options.

- **DID - Defense in Depth (DiD).** Defense in Depth is an approach to cybersecurity in which a series of defensive mechanisms are layered to protect valuable data and information. If one mechanism fails, another mechanism provides redundant protection to control the threat.

- **Restrict Usage of Server Message Block (SMB).** These ports should be closed for workstation end points.

- **Tighten Port Security.** Threat actors commonly scan networks for open ports to identify their next targets. Ports used should be defined, tracked, and controlled. Changes to ports (opening, closing, forwarding) should follow the change management process and require proper authorizations.

- **Deprecate (Replace) Unsupported Hardware and Software.** Upgrade to the latest supported servers, operating systems and applications.

- **Separation of Networks**. Use separate network connections for processing financial and banking transactions - not connected to the email system or general internet traffic. Separation, segmentation, and segregation of networks with sensitive data provides additional protections.

- **Monitor Network Traffic.** Limit traffic between servers and workstations to only necessary protocols. Expand visibility of traffic by monitoring outbound and inbound network flow. Implement data loss prevention ("DLP") monitoring to protect financial information, employee and student PII (Personally Identifiable Information), HIPAA (patients' health information), etc.

- **Limit Domain and Network Administrator Accounts.** Routinely review and update domain administrator accounts. Remove any unnecessary accounts and limit solely to authorized personnel.

For assistance with cybersecurity issues, internal controls and to report Cyber Incidents and suspicious activity contact: CTREmergencyNotification@mass.gov. See CTR Cyber at https://www.macomptroller.org/ctr-cyber for additional Cyber resources.

CYBERSECURITY LESSONS LEARNED

- **Configure VPN and Remote Access.** VPN tunnel policies should restrict access for hosts and networks based upon the "principal of least privilege."

- **Apply Best Practice Password Policies.** "Length is Strength", "Change Often" and "Do not share" are the 3 pillars to effective password protections.

    - Enforce maximum password length and complexity. Long phrases with special characters are best. Do not publish password formats. Adding complexity and length to a password (12-16+ characters, numbers and symbols) can delay attackers as they attempt a brute-force password attack.

    - Change passwords frequently. Credentials can be scraped and sold on the dark web even if you do not know passwords have been compromised. Therefore, changing passwords frequently significantly improves protections from compromise.

    - Users should be instructed to have "distinct" passwords for each work account and NOT replicate or share all or portions of passwords for multiple work applications.

    - NEVER use similar passwords for work and personal social media accounts (which are often scraped by cybercriminals).

- **Multi-Factor Authentication (MFA).** Use multifactor authentication (each user is granted access only after presenting two or more pieces of identification) wherever possible. MFA should not be an "option" for users since lack of MFA significantly increases risks of compromise. The compromise of one individual's PC/laptop can compromise an entire Department's network, so using MFA for work related applications should be standard practice. MFA should also be used for any administrator access in the environment to assure that administrative actions are conducted by authorized personnel only.

- **Firewalls.** Network traffic should go through a security device (such as a firewall) that employs web filtering. Setup security devices to block end users from accessing threatening web sites. Review and update firewall rules sets that contain 'any' connections. These rules should be updated to limit access to only those that need access. Firewall rule sets should follow the principle of least privilege, limiting access only to resources with a need and ideally, authorization, for a connection.

- **External Facing Internet Protections.** (DMZ and Firewall) Public facing servers should be separated on their own subnet which has its own firewall to protect from internet threats. An attacker who gains access to hosts within a DMZ, finds it much more difficult to gain access to hosts that reside on the internal networks.

For assistance with cybersecurity issues, internal controls and to report Cyber Incidents and suspicious activity contact: CTREmergencyNotification@mass.gov. See CTR Cyber at https://www.macomptroller.org/ctr-cyber for additional Cyber resources.

CYBERSECURITY LESSONS LEARNED

- **Group Policies**. Implement group policies that are applied to all Department computers upon log in. These group policies, with cyber security in mind, prevent end users from executing threatening actions on the agency network.

- **Back Up Files and Avoid Paying Ransom**. Back up servers and files frequently (for production servers – up to several times during the day); backups should then be saved both locally and offsite (daily offsite is preferred). If a server or its data is impacted by a cyber-event the server can be rebuilt and restored from a recent, non-impacted backup version. Digital content can be compromised or corrupted, so you really want to have multiple backups in multiple mediums and locations to protect and restore your valuable information.

    - The current guide is "3-2-1" which is at least three (3) copies of your data, on two (2) different types of storage media, and one (1) of these media located offsite or with an "air gap" which means it is not accessible to the internet. Having multiple backups, that you have tested, and that can be restored (as part of your Incident Response Plan, Business Continuity Plan and Disaster Recovery Plan) may prevent you having to pay ransomware to recover your files. Just note that paying ransomware does not guarantee that you will recover your files, and avoiding paying ransomware does not guarantee that a cybercriminal won't threaten to release confidential and other encrypted files, if you don't pay.

- **Vulnerability and Penetration Testing**. Conduct regular (at least quarterly) independent vulnerability assessments and penetration testing of networks to determine weaknesses in networks/end-point devices and whether sensitive data is sufficiently protected. A process should be put in place to identify vulnerabilities and remediate as quickly as possible. Third party vendors and cloud providers should also be demonstrating to you that they are conducting similar vulnerability assessments.

    - Statewide Contract ITS78 has vendors available to assist with vulnerability and penetration testing.

    - The Cybersecurity & Infrastructure Security Agency (CISA) offers free Risk and Vulnerability Assessments (RVA) to state and local governments.

- **Intrusion Detection (IDS) and Intrusion Protection (IPS).** IDS and IPS capabilities guard against known threats and zero-day exploits, SQL injection attacks and other web application attacks. IDS technology detects vulnerability exploits against a target application or computer while IPS technology adds the ability to block those exploits.

For assistance with cybersecurity issues, internal controls and to report Cyber Incidents and suspicious activity contact: CTREmergencyNotification@mass.gov. See CTR Cyber at https://www.macomptroller.org/ctr-cyber for additional Cyber resources.

Cyber Security Resources:

- **CTR Cyber** – The Office of the Comptroller has developed CTR Cyber to identify key cybersecurity internal controls for Commonwealth of Massachusetts departments, and to promote cybersecurity awareness and cyber vigilance for everyone in these organizations. CTR Cyber includes links to additional cyber resources.

For assistance with cybersecurity issues, internal controls and to report Cyber Incidents and suspicious activity contact: CTREmergencyNotification@mass.gov. See CTR Cyber at https://www.macomptroller.org/ctr-cyber for additional Cyber resources.