Information Security and the Real World

A Primer for Agency ISOs who got the job with a one-liner in their SJD and an appointment letter vice a career choice.

REPORT A CYBER SECURITY EVENT:

During Business Hours:

Monday-Friday; 7:30AM-4:30PM EST

Phone: (603) 271-7555

Email: helpdesk@doit.nh.gov

Non-Business Hours: (603) 271-7555, Option 2

This document is created and maintained by the State Chief Information Security Officer as a resource for individuals with Cybersecurity Responsibilities but who are not Cybersecurity Professionals. You professionals can go read the references.

Table of Contents

Introduction and Background

Agency ISOs and the Real World

So, welcome to the world (the real world?) of Cybersecurity and Information Security. Congratulations! No, we mean it. We need your help. Most importantly, **THANKS IN ADVANCE FOR ALL OF YOUR HELP!** We know this is most likely "Other Duties as Assigned" and on any given day, is probably not high on your list of priorities…until "THAT day." Don't worry, on that day, we'll all rally to your cause and be there to assist.

Here is what the Statewide Information Security Manual and RSA-21R:16 says your responsibilities are:

"The Agency ISO shall be responsible for protecting and maintaining the confidentiality, integrity, and availability of information assets under his/her purview. The Agency ISO fulfills the following responsibilities in support of the Statewide Information Security Policies and Standards:

- Serve as a member of the Cybersecurity Advisory Council;
- Identifying security requirements to effectively limit cyber risks associated with the agency's business goals and objectives;
- Implementing and promoting information security awareness within their respective agency;
- Ensuring compliance with the Statewide Information Security Manual's Policies and Standards within their respective State agency, including, but not limited to:
    - Coordination of risk assessments and compliance audits with NHCIC;
    - Coordination of vulnerability assessments of agency networks, applications, databases, and systems; and
    - Coordination of risk assessments of third parties having access to agency information assets;
- Assisting in the implementation of the Information Security Incident Response Plan; and
- Reporting all information security incidents to the CSG."

The information in this Primer will help you do those things! Look for frequent updates and reach out with ALL questions you may have! Look for this Purple Text in various sections to find out what you can do to help!

Access Control Management and UserSecurity

Access Control and the Real World

Humans are generally bad at creating passwords, so making employees change passwords regularly really does not help data and system security. What tends to happen is employees will create new passwords that are virtually identical to the lastand will follow predictable patterns when creating new passwords. Alternatively, theywill choose commonly used passwords or weaker passwords each time a change is required. In both cases, threat actors (hackers) can easily guess these types of passwords. A better, more secure practice is to create a passphrase. A passphrase is a sentence-like string of words used for authentication that is longer than a traditional password, easy to remember and difficult to crack. To create a passphrase as a password, use the initial letters and numbers from the sentence-like string of words.

An example: I have lived in 7 cities over 15 years!The
passphrase could be: Ihli7cO15Y!

Additionally, use of a password manager program is recommended as password manager programs offer easy ways to create — and remember — long, complex and unique passwords, or preferably, passphrases, for each site or system.

For additional information, refer to the Summary of the NIST Password Recommendations ***and share some of that information with the employees in your Agency!***

Credential Values

Data protection requirements and some simple best practices should be considered for credential values. Best practice for credential values standards includes:

- **Center for Information Security (CIS):** Use unique passwords for all IT assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using multifactor authentication (MFA) anda 14-character password for accounts not using MFA.
- **Federal Tax Information (FTI) data protection requires:** Minimum passwordlength of 14 characters with a combination of numbers, uppercase letters, lowercase letters and special characters. More guidance can be found in IRS Publication 1075.

- **Criminal Justice Information Systems (CJIS) data protection requires:** Minimum password length of 8 characters and no dictionary words or propernames. When agencies elect to follow the advanced password standards, a minimum of 20 characters in length with no additional complexity requirements is imposed (e.g.,

ASCII characters, emojis, all keyboard characters, and spaces will be acceptable). More guidance can be found in CJIS Security Policy v5-9.

- **Social Security Administration (SSA) data protection requires:** Minimum password length is equal to or greater than 8 characters, with a complexity ofupper- and lowercase letters, numbers, and special characters (at least one ofeach type).

- **Health Insurance Portability and Accountability Act (HIPAA) PHI data protection requires:** HIPAA follows NIST guidelines.

  More guidance can be found under "5.1 Requirements by Authenticator Type"of NIST 800-63b.

Unsuccessful Logon / Authentication Attempts

The need to limit unsuccessful login attempts and take subsequent action when the maximum number of attempts is exceeded applies regardless of whether the logon occurs via a local or network connection. Some best practices for this safeguard include but are not limited to:

- A limit of five (5) consecutive invalid logon attempts by a user during a15-minute period for Data Types classified as public or low.
- A limit of three (3) consecutive invalid logon attempts by a user during a15-minute period for Data Types classified as moderate or high.

Security safeguard requirements may vary by data type classifications. Below are linksto data type-specific guidance.

- CIS section 3 (You must download the guide to access it.): CIS Password PolicyGuide.
- FTI section AC-7: Publication 1075 Rev.11-2021**.**
- CJIS section 5.5.3: CJIS Security Policy.
- NIST 800-63b section 5.2.2: NIST 800-63b.

One of the most important things you can do is ensure that employees (Data Owners) are aware of the Data Classification Policy and the controls that are necessary to protect that data from unauthorized disclosure. Help educate people by sharing and talking about Data Classification.

For more information on Data Type Classification see the Data Classification Policy.

Access Control for Mobile Devices

Managing access control on mobile devices can sometimes be frustrating. The devices are usually not connected to the managed network, which can limit the amount of control organizations maintain over the devices. DoIT uses a Mobile DeviceManagement System (MDM) to assist in the management of the devices. Additional guidance on security for mobile devices is available below:

- CIS has some specific guidance: CIS Critical Security Controls v8 Mobile Companion Guide.
- CISA guidance: MOBILE DEVICE ADOPTION BEST PRACTICES.
- National Security Agency (NSA) guidance: Mobile Device Best Practices.

Mobile Device Management Systems (MDM)

MDMs are the administration application primarily used to configure and set policiesfor mobile devices. MDMs typically have an on-device application that allows the organization to define security and access controls on an employee's device. This application limits what the mobile device may and may not do. The mechanism of privileged actions is usually managed by operating system (OS) Application Programming Interfaces (API) and granted OS permissions at installation time. MDMsmay come with a suite of applications, including a secure container.

What should you do? About every 6 months, remind those in your Agency with Mobile devices to ensure they are connected to WiFi at least once a week to ensure security and feature updates are installed on time! If a user does not do this, they are actively adding risk to state networks and at the end of the day, violating their user agreement. But let us stay positive…by connecting to WiFi, they are making all of the networks and business processes more secure!

CIS offers a guide on best practices for Mobile Controls that can be downloaded: CISCritical Security Controls v8 Mobile Companion Guide.

Security Awareness Training

Note: DoIT provides a learning management system (LMS)-based online information security awareness training for the agencies it supports.

IT Security Training and The Real World

Multiple industry studies suggest that many databreaches are caused by human error, which makes ensuring state employees are current with Information security knowledge and best practices that much more important.

IT Security Training Topics

Annual information security topics provided by the NH Cybersecurity Group (CSG) include but are not limited to:

1) Recognize social engineering attacks.
2) Phishing.
3) Password best practices.
4) Authentication best practices.
5) Data handling best practices.
6) Causes of unintentional data exposure.
7) Identify and report if their enterprise assets are missing security updates.
8) The dangers of connecting to and transmitting enterprise data over insecure networks.
9) Incident response.
10) Clean Desk.
11) Locking Devices.
12) Social Media best practices.

If your Agency requires additional modules because of Data Protection and Privacy requirements, these can be coordinated with CSG and delivered through the learning-management system. When it is time for your Agency to do training, CSG will send out individual links. Partner with your IT Lead to request completion rates and lists of those who have not completed the training and ask your Agency Leadership to endorse your request for ALL employees to complete the required annual training. Also, get the stats on the Phishing Email Testing. Engage with those that "clicked" to help improve the overall cybersecurity readiness of the State.

IT Role-Based Security Training

It is best practice to provide role-based security and privacy training to IT personnelaccording to their IT responsibilities before authorizing access to the Information System or performing assigned duties, when required by Information System changesand annually thereafter.

IT role-based security training should be tailored to a user's IT role which may include but is not limited to:

1) System Developers.
2) Software Developers.
3) Network Administrators.
4) Server Administrators.
5) Information System Managers.
6) Individuals with Technical Duties.

In most cases, these people will receive this training through DoIT and CSG directly, but for your Agency systems, don't be afraid to ask these folks if they have had role-based cybersecurity training.

Audit Log Management and Accountability

Audit Log Management and The Real World

Log collection and analysis is critical for an organization's ability to detect malicious activity quickly. Sometimes audit records are the only evidence of a successful attack.Thus, it is important to maintain a collection of audit logs for Incident Response and data compliance requirements. It is also important to frequently review the logs for malicious activity, or the logs are no better than that file cabinet in the office basement full of old dusty files. Do not collect *everything* but do collect what is required and useful.

CSG will review these logs as part of a standard process. Usually, no news is good news, but do not hesitate to reach out and ask, "Good Morning, CSG. Anything I should know about logged events on system (insert system name here.)"

Content of Audit Records

Audit logs typically include user-level events — when a user logged in, accessed a file,etc. — and take more planning and effort to set up. Best practices for the types of records to maintain include the following:

1) Type of event that occurred.
2) Date and time the event occurred.
3) Where the event occurred (Terminal or System ID).
4) The source of the event.
5) The outcome of the event.
6) The User IDs of any individuals or subjects associated with theevent.
7) Successful and failed attempts to access systems, data, or applications.
8) Files and networks accessed.
9) Changes to system configurations.

10) Use of system utilities.
11) Exceptions and other security-related events, such as alarms triggered.
12) Activation of protection systems, such as intrusion detection systems.

Audit Storage Capacity

It is very important that CSG works with the Business Process Owner to ensure we collect and retain the necessary logs. Keep these things in mind to determine how much storage will need to be allocated for audit logs:

- What information needs to be logged.
- Log retention period for audit requirements.
- Requirements for Service Provider logs.

Please be prepared to request additional funds as necessary to ensure enough storage is available for your system logs. Your IT Lead is there to assist!

Security Assessments and Authorization

Security Assessments, Penetration Testing and the Real World

What is the security posture on your Agency or Contractor managed systems? How well protected is your organization from hackers and other bad actors? How do you know? One way to know is by testing your organization's security posture, which can be done by having a third party assess your IT defensive posture and readiness. This assessment is usually performed with a penetration test.

In February 2002, former United States Secretary of Defense Donald Rumsfeld said, "There are known knowns; there are things we know we know. We also know there areknown unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know." (2002, as cited in *Washington Post*, 2021) If you want to keep your customer happy, it is best to work on finding the "unknowns." One best practice for finding those "unknowns" is developing and implementing a continuous cybersecurity assessment program.

General IT System, Software and Device Penetration Testing

A successful cybersecurity posture requires a comprehensive program of effective policies and governance and strong technical defenses combined with appropriate action from people. In a complex environment where technology is constantly evolving and new attacker tradecraft regularly appears, organizations should periodically test their Information System security controls to identify gaps and assess their resiliency. Tests may be from external network, internal network, application, system, or device perspectives. Tests may include social engineering of users or physical access control bypasses.

Application Penetration Testing

For critical applications, authenticated penetration testing is better suited to findingbusiness logic vulnerabilities than code scanning and automated security testing.
Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user. Keep the following bestpractices in mind when developing a model for penetration testing:

1. Define your scope and budget (What do I want to test and the cost).

2. Include financial and customer data sources.
3. Consider penetration testing remotely accessible resources.
4. Prepare for the test.
5. Create a communications plan.
6. Choose a qualified pen tester.
7. Follow a penetration testing methodology for best results.
    i. Penetration Testing Execution Standard (PTES).
    ii. Payment Card Industry Data Security Standard (PCI-DSS).
    iii. Open-Source Security Testing Methodology Manual (OSSTMM).
    iv. OWASP Web Security Testing Guide.
    v. National Institute of Standards and Technology (NIST) Special Publication 800-115.

If you have applications that fall in-scope for PCI-DSS or other programs, Penetration Testing is periodically required for those applications. Coordinate this testing with your IT Lead and CSG so the Managed Detection and Response provider can know in advance these Penetration Testing events are occurring…they will look malicious, and we'd hate to interrupt your required testing because the Crowdstrike Team busted them and nuked them during testing!

Types of Security Scanning

There are several types of security scanning:

Static Code Scanning

Static scanning is performed in a non-runtime environment. Static application security testing (SAST) is a testing process that looks at the application from the inside out. This test process is performed without executing the program, but rather by examining the source code, byte code or application binaries forsigns of security vulnerabilities. In the static test process, the application dataand control paths are modeled and then analyzed for security weaknesses.
Static analysis is a test of the internal structure of the application rather than functional testing.

Dynamic Scanning

Dynamic scanning is executed while the program is in operation. Dynamic application security testing (DAST) looks at the application from the outside in— by examining it in its running state and trying to manipulate it in order to discover security vulnerabilities. The dynamic test simulates attacks against a web application and analyzes the application's reactions, determining whetherit is vulnerable.

Server Configuration CIS Benchmark Scanning

CIS Benchmarks™ are configuration baselines and best practices for securely configuring a system. Each of the guidance recommendations references one ormore CIS controls that were developed to help organizations improve their cyber defense capabilities. The benchmarks can be found on the Center for Internet Security's website: CIS Benchmarks.

This is mostly taken care of by DoIT Operations Division, but your Agency probably has servers that host applications for you. It is o.k. to work with your IT Lead to understand these configurations and baselines if questions arise.

I have findings. What next? Remediate, Remediate, Remediate

The testing and scanning found problems. What should I do now? The answer: developand implement a remediation plan to fix or remediate what is wrong and validate the remediation. Here are some things to keep in mind with remediation:

- ***Plan time for implementation of the remediation.***
- ***Prioritize the vulnerabilities found and plan out how you are going to fix them.***
- ***This is a good time to review your IT security tools to see how effective they were in reporting the attacks and assisting your IT security team in identifyingthreats.***
- ***Perform a lessons learned review of the whole testing and remediation process.***

Assessment of System Interconnections

It is important that you know what is connected to your network. Interconnections aresystem connections between IT systems and separate constituent system components (i.e., connections between components that are part of the same system), including components used for system development. Intra-system connections include connections with mobile devices, notebook and desktop computers, tablets, printers, copiers, facsimile machines, scanners, sensors, and servers). Keep the following in mind:

- Group your connections together (e.g., printers with printers, servers with servers, desktops with desktops, firewalls with firewalls). Grouping can helpyou keep track of the connections between devices with similar IT security safeguards.
- Continually review the need for the connections. Is each connection stillneeded for business functions?
- What are the characteristics of the connection?
- What are the security safeguards in place around each type of connection?
- Know, understand and implement security and privacy requirements to ensure protection of the ***information*** communicated through the connection.

Connections and Firewalls

Connections allowed through firewalls are also areas of concern regarding data and Information System security. When systems are put online, the developer asks for many ports to be opened on the firewall to allow their applications to “talk” to theworld, which can be a bullseye for a hacker. Security Operations usually comply and do their best to ensure everything is secure, but one thing many organizations do poorly is not removing those connections when they are no longer needed. Remember,best practice is to frequently clean up firewalls and firewall connections, and verify what connections are necessary on a regular basis.

We recommend at the Summer Solstice you work with your IT Lead to review the status and reaffirm that any open connections are still needed. Maybe they are…but just maybe, a system got decommissioned or hosted in the cloud and there is still an open port or two. Thanks for the help in closing the holes in our defenses!

Secure Configuration of IT Assets andSoftware

Secure Configuration and the Real World

This is about minimizing and managing risk. The security threat landscape is challenging. Attackers are constantly on the lookout to exploit security vulnerabilities in applications and systems to gain access to, or control of, sensitive information and launch cyberattacks such as ransomware. This means integrating information security must be a core part of the development process. Organizations in the real world today require that secure configuration of allsoftware, systems and applications be part of any properly running IT security program. DoIT manages this through the ICR Process.

Configuration Change Control Body

Configuration change control includes changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers). The organization includes emergency changes in the configuration change control process,including changes resulting from the remediation of flaws. Before changes are made, it is a best practice to set up a Change Control Body to review, approve or deny any changes before they are implemented and to review the outcomes after the change has been implemented. Keep in mind the following actions are best practices when creating a Change Control process:

- Define the Change Request to include these items.
    a) **Actual Request:** Clearly outline the change (i.e., the who, what, where,when, cost, resources needed, etc.).
    b) **Reason for the Request:** Customer impacts if the request cannot be completed.
    c) **Conditions of Success:** Clearly defined criteria that will verify the implemented change worked as planned.
    d) **Expected Completion:** Requestor should provide the date and time bywhich the change implementation will be performed/completed.
    e) **Value of the Change:** Explain why the change is needed.
- Define how the change requester should submit the Change Request.

- Define the Change Request review process.
    - What subject matter experts (SMEs) will be involved?
    - What parameters are to be considered when determining if the Change Request should be approved or denied?
- Define what happens after the Change Request is approved or denied.
    - What is the Change Request approval/denial notification process?
        - If approved, the change will need to be scheduled.
        - If denied, the Change Control Body will need to give a response asto its decision.
- Define an after-action review of the change.
    - Did the change work with the necessary outcomes, or did the changecause disruption and must be rolled back?

As the ISO, you probably will not be doing these things yourself for your Agency, but Agency coordination and situational awareness are critical to successful configuration management. Moving updates from Development to Test or Production Environments? That matters! Make friends (or at least friendly acquaintances with your IT Lead and Database Manager(s) if you have them and let them know you are there to help with Agency Coordination and to make sure these things happen for the benefit of the Agency Business!

Robust Communications Plan for Change Control

When developing a Change Control Body and change control process, remember to create a robust communications plan. Let the customer know what changes are aboutto happen and any outages that may occur.

Default Administrator Accounts

Information systems usually come with default administrator accounts. Best practices regarding default Information System administrator accounts include but are not limited to:

- On each device change the default administrator account name to a uniquename.
- Use a unique password on each node so that if an intruder finds the password,only one node is compromised.
- Use strong passwords such as a passphrase which are harder for dictionaryattacks to defeat.
- Carefully document new passwords.
- Verify each password change was successful.

Secure Configuration Settings

Secure configuration refers to information technology security measures that are implemented

when building and installing computers and network devices to reduce unnecessary cyber vulnerabilities. Security misconfigurations are one of the most common gaps that criminal hackers look to exploit. Look to the following resources forsecure configuration best practices:

- Center for Internet Security provides security configuration benchmarks: CIS Benchmarks.
- NIST provides specific guidance on Server Security: NIST SP 800-123, Guide toGeneral Server Security.

Usually, your EDS team does this for you, but every now and again there will be non-standard software involved, and as part of that request and annual verification, you will need to be aware of the configuration settings required by or installed with the non-standard software. As a reminder, the procedure for getting non-standard software approved can be found HERE.

IT Asset and Software Inventory

Do you know where all your organization's IT assets and software inventory are stored? What processes do you have in place for preventive maintenance or management of warranties? When was the last time you ran an asset inventory report?These are all key questions to ask when dealing with IT Asset and Software Inventory. Keep the following best practices in mind when setting up an inventory process or system:

- Use asset management software. This is a better method than using a manualprocess and spreadsheets, which are prone to errors.
- Run audits to verify that the asset reports are correct.
- Monitor depreciation rates and maintenance needs (warranty requirements).
- Be sure your inventory processes are completed consistently with Standard Operating Procedures (SOPs).
- Maintain proper security efforts. Make sure you know who has access to what(user access controls) within your IT assets, including software.

What Inventory Data Should I Collect?

Collect enough information on your IT assets and software to ensure the inventory iskept current and useful. An IT asset and software inventory should include the following:

1) Licensing.
2) Secure development.
3) Data storage.
4) Intended use.
5) Supportability.
6) Patch cycle cadence.

In addition to the above, you may also choose to consider the following:

- Uniform Resource Locator (URL).

- App store(s).
- Version(s).
- Deployment mechanism and decommission date.

This seems like such an easy thing to do. Every agency does this for hardware because it is required under the "Property Management" requirements from Department of Administrative Services and by Law. But…did you know this also helps with Cybersecurity? We cannot protect what we do not know exists. We cannot properly perform a "damage assessment" if an unknown device (or more importantly, the data on that device) is stolen while you glanced away while finishing that last bite and swallow at Dunkin. If a device is missing from inventory, it is about more than property accountability. Report it!

Contingency (Continuity of Operations)Planning

IT Contingency Planning (Continuity of Operations (COOP)) and theReal World

Contingency planning for Information Systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses Information System restoration and implementation ofalternative mission or business processes when Information Systems are compromised or breached. Contingency planning should be considered throughout the Information System development life cycle and is a fundamental part of the Information System design. Information systems can be designed for redundancy, to provide backup capabilities and for resilience. The real world is a dangerous and constantly changing landscape, from natural disasters to cyber-attacks. It is best practice to have an IT Contingency Plan (i.e., a COOP) in place.

IT Contingency Planning from the Beginning

Some items to consider when developing a contingency plan include the following.These items will help identify what needs to be protected.

1) Make a list of all the risks that may impact your business operations.
2) Weigh risks based on severity of impact and likelihood. These risks vary frombig to small and may include but are not limited to the following:
    a) Hardware failures.
    b) Fire.
    c) Flood.
    d) Criminal Acts.
    e) Power surge/outage.
    f) Natural disasters.
    g) Loss of communications systems.
3) Determine the likelihood and severity of each risk and create a contingencyplan for risks that are high likelihood and high severity.
    a) A contingency plan is probably not needed for risks that are low likelihood and low severity.

4) Have your organization's leaders approve the contingency plan(s.)
5) Distribute the contingency plan(s) to the right people. Make sure those whohave responsibilities within the contingency plan(s) know what they are expected to do.
6) Monitor the contingency plan(s) and adjust as the IT environment changes.
7) Create new contingency plan(s) if your organization's IT environment expandsor develops new risks.

IT Contingency Planning "What's Inside"

IT contingency plans can become complicated. However, there are a few specificthings that should be considered for all IT contingency plans:

1) Determine clearly what is the "trigger" or "triggers" that will put the plan intoaction.
2) What is the immediate response?
3) Who should be involved in the immediate response and who should be informed?
    a) Identify key responsibilities and include a Responsible, Accountable, Consulted, Informed (RACI) chart if necessary.
    b) Develop and include a communications plan as part of the IT contingencyplan.
        - The communications plan should identify the individuals or roles that should be informed when an event occurs that causes the activation of the IT contingency plan and how they are informed.
        - Remember to consider that electronic communication may not be available.
4) IT contingency plans should also include an Information Technology Disaster Recovery Plan (ITDR) that can meet your organization's needs for recovering operations promptly following a business interruption.
5) The timeline of your response (i.e., immediate actions vs. longer-termactions).

Information Technology Disaster Recovery Plan (ITDR)

An ITDR plan describes scenarios for resuming work quickly and reducing interruptionsin the aftermath of a disaster. It is an important part of a business continuity plan, and it allows for sufficient IT recovery and the prevention of data loss. Key items to consider for an ITDR plan:

1) Conduct a thorough IT assessment and Inventory of your organization's ITassets.
2) Determine an IT backup management strategy under the ITDR plan.

a) A cost-effective option may be for a business to migrate to the cloudinstead of maintaining physical off-site data centers.

3) Ensure backups include data and workflow. Just having the data will not beenough. Backups also need the applications, operating systems, and any workflows that they include.
4) Backup encryption is a must. It is a critical step in keeping the information inyour organization's IT files and applications away from prying eyes.
5) Create IT disaster response teams that will determine to what extent thedisaster recovery plan must be invoked.
6) Know what metrics to consider in an ITDR.
   a) What is the recovery time objective (RTO)?
   b) What is the desired recovery point objective (RPO)?
   c) How quickly can your team transition from the failed "live" system to the recovery solution?
7) Proper ITDR management requires employee training.
   a) Plan for disaster recovery testing exercises. Tabletop testing should be performed with key internal stakeholders to make certain that disaster recovery processes are working as they should and that everyone knowswhat to do in the event of an IT disaster.

This is truly a team sport between Agencies and DoIT. Each Agency must account for business process risk, DoIT must account for the IT risk and prioritize recovery operations based on Agency priorities. If you are not involved in the process for your Agency directly, reach out to your COOP planner(s) and work with your IT Lead to become aware of what DoIT thinks the priorities are based on your Agencies' input. Reassess this when major system changes take place. This is great "over the holidays" work when the State Pretty much shuts down and you have time to yourself…if you are not also on vacation!

IT Account Management (Identification and Authentication)

IT Account Management and the Real World

In the real world, Identity Access Management (IAM) teams put most of their focus around Privileged Account Management (PAM). These are the accounts that pose the biggest security risk to an organization. Protect privileged accounts with IT security safeguards to ensure the right person is authorized to access each IT Asset.

Multifactor Authentication (MFA)

MFA mitigates password risk by requiring additional factors for authentication (i.e.,identity verification). MFA enhances your organization's IT security by identifying users, processes, or devices by more than one identity verification method. MFA cantake many forms, including but not limited to:

- Something you know (knowledge).
    a) Answers to personal security questions.
    b) Password.
    c) One-Time Password (OTP). This can be both knowledge and possession.
- Things you have (possession).
    a) OTP generated by smartphone apps.
    b) OTP sent via text or email.
    c) Access badges, USB devices, smart cards, fobs or security keys.
- Things you are (inherence)
    a) Fingerprints, facial recognition, voice, retina or iris scanning or other biometrics.
    b) Behavioral analysis.

Adaptive Authentication

Standard authentication methods, including MFA, ask users for specific credentials whenever they try to log in or access organizational resources. Adaptive authentication asks for different credentials, depending upon the situation—tighteningsecurity when the risk of breach is higher.

Adaptive authentication can be seen as risk-based authentication. The authenticationmethod is determined by the person's role or needed access to sensitive information. Adaptive authentication can implement machine learning using algorithms to monitorand learn user behavior over time to build an accurate profile of a given user's login patterns. It may track devices, typical user login times or usual work locations. It maycheck IP addresses and network reputations in addition to threat data for those networks.

Adaptive authentication solutions usually assign a risk score based on behavior and context and respond to the perceived risk based on the rules established by the organization. The most advanced adaptive authentication solutions automatically adjust the authentication requirements based on the risk score and an organization'sIT policies. Adaptive Authentication is another type of authentication an organizationcan consider based on the security needed to protect an Information System.

Shared Accounts

Shared accounts make it difficult to identify the actual user and often allow maliciousparties to use the shared account with anonymity. Accounts used by a shared group ofusers typically have poor passwords that users do not change frequently or when a member of the group leaves, which makes them easy for malicious actors to guess. It is best to avoid shared accounts whenever possible. However, best practices to consider when using shared accounts include but are not limited to:

- Shared accounts should only be allowed when used in conjunction with an MFA solution.
- If possible, users of a shared account should be individually identified beforeallowing access. MFA can assist in this process.
- Limit who has access to shared accounts.
- Log and audit usage of shared accounts. Know who is responsible for handlingthe shared account.
- Develop and implement a process for changing the passwords of shared accounts on a regular basis.

Device Identification and Authentication

It is a best practice to have the unique identity of Information System devices authenticated before establishing a remote network connection. Items to considerwhen implementing such a safeguard include but are not limited to:

- Authenticate before establishing a remote connection using bi-directional authentication that is cryptographically based.

- Where addresses are allocated dynamically, standardize dynamic address allocation lease information and the lease duration.
- Require, where possible, connection to internal network resources via an organizational-managed VPN solution.

Identifier Management - Assigning Unique Identification

It is important that all identifiers be unique. Unique identifiers should be based on the individual, group, role, or device. Best practices include but are not limited to:

- Unique identifiers should be unique, a lifetime identifier and stored in asecure manner.
- Unique identifiers should never be re-issued.

Virtual Private Networks (VPN) and VPN Split Tunneling

A VPN provides users with a secure tunnel through which all data traveling to and from their device is encrypted. This allows users to enjoy secure remote access andprotected file sharing. It is a best practice to use when your user group is remote.

VPN split tunneling allows an organization to route some of its application or devicetraffic through an encrypted VPN while other applications or devices have direct access to the internet. However, VPN split tunneling introduces some IT security challenges. Any data that does not traverse a secure VPN is not protected by the organization's firewall, endpoint detection and response system, anti-malware, and other IT security mechanisms.

On the state network, VPN split tunneling is seen as too high of a security risk. Only under certain situations, and with the appropriate exception request detailing securitysafeguards that will be applied, will VPN split tunneling be considered.

If you hear anyone suggest, "We can just use split tunnelling," squash it like a Black Fly. The risk is not worth the reward and the split tunnel will most likely not be approved anyway.

Authenticator Feedback

Authenticator feedback is the information returned when a user attempts an authentication process on an IT device. This IT security safeguard states that the Information System obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use byunauthorized individuals. Two examples of authenticator feedback include:

- Obscure the password when being typed (i.e., displaying asterisks when a usertypes in a password).

- Failed login messages do not indicate which part of the username or passphrase combination is incorrect.

Re-Authentication

Re-authentication occurs when an Information System or software requires users ordevices to re-verify their identity to regain access to the Information System or software. There may be specific circumstances when this may be a best practice. Examples of when re-authentication should be considered include:

- After a system or network-initiated session lock (period of time).
- When authenticators change.
- When roles change.
- When the security of a system changes.
- Any abnormal behavior determined by the system (i.e., unacceptable geographic change).

Single Sign-on (SSO)

SSO reduces the number of attack surfaces because users only log in once each day and only use one set of credentials. Reducing login to one set of credentials improves the IT security posture for the organization. While users should use unique passwords for each application they access, many do not. If the user is hacked, it makes it easierfor the attacker to access many doors.

This is just so important! There are so many use cases when emotional responses are used to attempt to justify NOT using MFA, or not using MFA "often enough." Please recognize that these statements are usually anecdotal, not supported by data, and most times are made for the sake of individual perceived convenience rather than a legitimate business need. Do not get me wrong, there are some very limited cases when a legitimate business need exists to not use MFA or not use it as often as the standard policy requires. Just ask the question "Why?" several times and require requestors to define the problem they are trying to solve rather than just jumping to a solution of "Less MFA less often."

IT Incident Response Management

IT Incident Response Management and the Real World

Where business continuity plans focus on creating a system to prevent and recover from potential threats to an organization, whether that be personnel, assets or natural disasters, IT incident response management is concerned with security incidents and breaches that impact information, network, and data security. Whether a business small or large, organizations need to have an IT Incident Response Plan (IRP)in place to mitigate the risks of being a victim of the latest cyberattack. In the real world, security incidents happen all the time. Protect your organization's IT Assets with a well-developed IT IRP.

The key to knowing an incident response is necessary is to know a cyber event took place! Constantly remind your Agency Employees to:

REPORT A CYBER SECURITY EVENT:

During Business Hours:

Monday-Friday; 7:30AM-4:30PM EST

Phone: (603) 271-7555

Email: helpdesk@doit.nh.gov

Non-Business Hours: (603) 271-7555, Option 2

IT Incident Response Management Resources

The following are recommended IT incident response resources:

1) NIST IR Guidance Chapter 3.8, p. 149 (Updated 2020): NIST 800-53 Rev. 5.
2) NIST Computer Security Incident Handling Guide (Updated 2021): NIST SP800-61.
3) NIST Guide to Integrating Forensic Techniques into Incident Response (Updated 2006): NIST SP 800-86.
4) NIST Guide to Intrusion Detection and Prevention Systems (IDPS). (Updated2012): NIST Draft SP 800-94 Rev. 1.
5) NIST Guide for Cybersecurity Event Recovery (Updated 2016): NIST SP 800-184.
6) Cybersecurity and Infrastructure Security Agency (CISA) IR guidance: CyberIncident Response
7) Additional guidance for federal agencies: Security Incident Response Guide

Do not worry. You are not alone. When an event or incident occurs, help will arrive. Let us know as soon as you think something does not "smell right." Better 10 false reports than miss a single real event!

Information System Maintenance

Information System Maintenance and the Real World

Information system maintenance is the process of modifying an Information System to continually satisfy organizational and user requirements. Remember the maintenancenot only includes the hardware and software but also includes the other components that make up the system. Having a process to keep everything maintained and operational will keep your organization ready for business.

Maintenance Tools (Verify what is being brought in)

Sometimes vendors and other providers may have to dispatch to your location to perform Information System maintenance. They will likely bring their own tools or software to perform maintenance. It is important to understand and review exactlywhat Information System maintenance they will be performing. Best practices include:

- Inspect what the vendors or other providers bring on location and any softwarebeing used.
- Be sure your system has the latest software patches applied.
- If maintenance tools have been altered or updated, verify the tools do notcontain any malicious code or software.
- When the maintenance is complete, verify that no organizational data or information contained in the equipment exits with the maintenance tools or hardware being serviced.

Predictive Maintenance

The goal of predictive maintenance is to perform maintenance at a scheduled time when the maintenance activity is most cost-effective and before the equipment losesperformance within a threshold. A few things to consider when evaluating how best touse predictive maintenance in your organization include:

- Focus your predictive maintenance toward critical Information Systems and infrastructure.
- Gather real time information on the Information Systems (analyze, correlate, and understand your system's performance). Analytics can reveal a lot about the performance of your Information System's components.
- Act on your evidence before your machine fails or quality declines; performthe right preventive maintenance actions at the right time.
- Document the results of all predictive maintenance to improve your predictive maintenance program.

Data Protection, Recovery and Sanitization

Data Protection, Recovery and Sanitization and the Real World

Data is everywhere. From the information you type into a computer database to the emails you send and even the words you speak. The kind of data we are talking about here is electronic data. You need to know how to best protect that data based on the organization's requirements. Failing to do so can put you at risk of data loss or unintended data disclosure which, depending on the type of data lost, could be costly.

Data Classification Scheme

Organizations usually develop a data classification scheme that determines how to best use, transmit, protect, and sanitize their data. Best practices to consider whendeveloping a data classification scheme:

- Determine what type of data is being protected. Is it public data or does the data contain protected information such as FTI, HIPAA, SSA or CJIS, which havespecific data protection requirements?
- Once you understand the type of data your organization uses and the work it is used for, the data can be classified based on sensitivity level. An example sensitivity-level data classification grouping includes:
    a) **Low sensitivity data**: Intended for public use. For example, publicwebsite content.
    b) **Moderate sensitivity data**: Intended for internal use only, but if compromised or destroyed, would not have a catastrophic impact on theorganization or individuals. For example, emails and documents with no confidential data.
    c) **High sensitivity data**: If compromised or destroyed in an unauthorized transaction, would have a catastrophic impact on the organization or individuals. For example, Social Security Administration data, federal taxrecords, medical data, criminal justice information.

Additional guidance on classification of data can be obtained by reviewing the DoIT Data Classification Policy here.

Data Flows

A data flow is the movement of data through one or more Information Systems and networks. It is important to document and diagram the flow of data to understand what information security safeguards are required to protect the data. The diagram should include interconnections between user clouds, network zones, cloud instances,document protocols, IP addresses when determined, direction of connections and API type specification.

Encrypt Sensitive Data at Rest and in Transit

Encryption is a process of scrambling data so it can only be read by authorized people (e.g., those with the right encryption key). You want to encrypt your data so that if anunauthorized person (cyber-criminal) gets into your network they have a more difficult time stealing your data. You want to encrypt your sensitive data not only because it is a best practice but because it may also have legal requirements for encryption based on the classification of the data. Items to consider regarding data encryption:

Encryption at rest

Refers to the encryption of stored data such as that which is stored on a harddrive. Items to consider with encryption at rest:

- **Full disk encryption:** Ensures that even if the hard disk is lost or stolenthe data is secure and can only be decrypted with the encryption key.
- **File level encryption:** Requires the encryption key to decrypt the file, however, additional overhead is required for managing encryption at thefile level.
- **Encryption of data at rest in the cloud:** Data encryption best practicessuggest both file level and full disk encryption can be used.

Encryption in transit

Refers to the use of encryption to protect data as it moves from one location toanother. Items to consider with encryption in transit:

- **Symmetric encryption:** The same key is used for encrypting plaintextand decrypting ciphertext.
- **Asymmetric encryption (aka public key encryption):** Two different keysare used, a public key and a private key, and the private key is kept secret. If one of the keys in the key pair is used to encrypt plaintext only, the other key can decrypt it.

- **Hybrid encryption:** Using both asymmetric and symmetric encryption,most notably Transport Layer Security (TLS), which is the encryption used to secure web communications (e.g., HTTPS).

Protect Production Data from use in Non-Production Environments

Test and development environments, by necessity, do not have the same security controls as production environments. If you move your sensitive data into a test or development environment, you open it up to a much wider group of users who may ormay not be a user with the same amount of trust within your environment. The resultis a massively increased risk of a breach, whether malicious or inadvertent. Therefore, best practice is ***never*** to use production or sensitive data in a test or development environment.

Up to this point in this section, most of these actions and activities will be done by DoIT for enterprise systems. That said, in your Agency, you probably have a variety of Third-Party managed and/or hosted systems used for Business Processes. What you need to do is make sure that every RFP and Contract that your Agency submits follows the Third Party Risk Management Policy and Procedure (Link Coming Soon.)

Data Loss Prevention (DLP)

Every organization needs a data loss prevention (DLP) strategy to prevent data from being improperly accessed, stolen, or deleted. A DLP strategy should focus on the protection of sensitive, valuable, or regulated data. Best practices when implementinga DLP strategy include but are not limited to:

- **Which organizational data needs to be protected?** Identify exactly whatcontent needs protection.
- **Where does the data reside?** To protect data, identify all the places it canreside, including but not limited to shared network drives, databases, cloudstorages, email and hard drives.
- **What are the conditions for accessing different types of data?** Different types of data require different levels of protection. Organizations share some data freely with the public while other data may be associated with a Data Type that has specific security safeguard requirements and should be availableto only a select few individuals.
- **What actions are to be taken in case of information security incidents?** Clarify the steps to be taken when suspicious activity is detected and who isresponsible for each action. While DLP solutions can often respond automatically, such as by blocking the operation or sending a notification tothe responsible team, some data losses will require identified individuals torespond to data loss incidents.
- **What information is to be archived, and when?** The DLP scheme should detailrules for archiving data, including but not limited to your audit trail and information about the IT

security incidents. Secure your information from bothexternal attackers and insider threats.

Some Agencies already have DLP rules in effect for their email accounts. Some are not there yet. What you need to know is fi DLP rules are in effect for your Agency, what will happen is if a rule is "tripped" based on the content of an email, e.g. if the system detects something that looks like a bank account number, the system will automatically encrypt that email. The sender and recipients can view it just fine…no action required, but recipients will not be able to forward the email for others to read. This happens in Agency Finance and Accounting units frequently. Not to worry…better safe than sorry after a data breach! If your Agency's rules need adjusted, work with your IT Lead on the desired outcome and a helpdesk ticket will make it happen.

Data Backup and Recovery Strategy

Data is the most valuable commodity an organization can possess. Data loss can occurfor a multitude of reasons, ranging from hacker attacks to natural disasters. If you have not backed up your data properly, recovery could be costly, time-consuming andseem almost impossible. Consider the following when creating a backup strategy:

- Review all your Information Systems, including legacy systems.
    - Document all the workloads, data storage and applications within your IT environment.
- Create a Data Backup Plan.
    - This should include multiple backup copies of your data and utilize version control so that you understand what backup datayou have stored.
    - Maintain one copy on-site and another may be off-site or in a cloud storage solution.
- Perform regular tests of backup and recovery processes.
    - If you do not test your backup and recovery processes, you will not knowif they will work when you need them to.
- Establish documentation of your backup policies and procedures.
    - Not all data needs to be backed up the same way. Some data may have compliance rules that determine how you need to backup and store yourdata.
- Encrypt all backed up data.

Data Sanitization

Data Sanitization is essential. It protects your organization's data and mitigates your risk in disposing unwanted assets because it always ensures data compliance and security. Items to consider regarding data sanitization:

- **What is the data you are sanitizing?** Some data type classifications may havespecial

regulatory requirements regarding sanitization.

- **Be sure to document, document and document.** Have a chain of custody paper trail (or electronic trail) for the data or device that is to be sanitized sothat you have evidence that all the necessary steps have been taken in case you are audited.
- **Use a third party who can certify the sanitization or destruction of the data.** There are many vendors and businesses that can professionally sanitize your data. Consider using such a service. They may be able to keep everythingdocumented for you to ensure you follow any data specific regulations.

This is an area where you don't have to worry about it unless you r Agency already knows they need to worry about it due to data classification or compliance requirements. When in doubt, ask plenty of questions. Take a pause and make sure the right thing is happening. Easy days.

IT Environmental Protection and PhysicalSecurity

IT Environmental Protection and Physical Security and the Real World

Protecting your data centers and IT closets from intrusion as well as protecting the IT environment is key to maintaining a secure, working system. If you have unauthorizedpeople accessing your space, you cannot be sure they are not doing something nefarious. The same goes for the environment. If you do not have control over the temperature or water in the Information Systems' environment, you may wake up to aswimming pool in the server room.

Physical Security

Physical security is the protection of people, property and physical assets from actionsand events that could cause damage or loss. Best practices regarding implementing a physical security strategy include:

- **Access Control:** Limiting access to your organization's physical environment and IT systems is one of the best ways to protect your Information Systems. One method of implementing access control is using keycards or key fob systems. Some Information Systems may even allow mobile credentialsas a method of access.
- **Surveillance Tools:** Surveillance is crucial to physical security control for buildings with multiple points of entry. The most common surveillance tool isvideo camera surveillance. If you use video cameras, be sure to have either aperson monitoring them or some type of automated activity alert. Also, keepvideo footage stored in case review is needed for investigations.
- **Additional Sensors:** Additional sensors may be necessary in areas that cannotbe monitored by cameras or other means. Examples of additional sensors include:
    a) Motion sensors.
    b) Contact sensors.
    c) Glass break sensors.

- **Distribution System Access:** Not only should the physical Information System be protected but so should the means of transmission. Best practice involves implementing the following:
    a) Disconnect spare jacks.
    b) Lock wiring closets.
    c) Protect cabling with conduit or cable trays.

DoIT has you covered on this. That will not keep an auditor of some kind or another from asking you. Now you know the answer!

Access Control for Output Devices

Most organizations have some or many output devices. These devices convert digital data to a physical form. Some common output devices are printers, facsimiles, copiers,and monitors. Depending on the data classification, there may be requirements to protect the data output from unauthorized individuals. Actions to take to safeguarddata in physical from through an output device include:

- Implement a PIN or hardware token to access the output.
- Use screen filters that block the output from anyone who is not directly infront of the monitor.
- Implement a biometric measure like a fingerprint or facial recognition foraccess to the output.
- Lock the output device in a secure location where only authorized personnelare provided access.
- Link authorized personnel's identification to the output received. This willassist with audits and record keeping requirements.

Most Agencies manage this with User Security Groups for individual printers, copiers, scanners, multi-Functional devices, etc. The key here is to just ensure the correct employees are in the correct security group. This is usually part of the initial account creation process. It still does not protect you from "Abandoned Print Jobs" though. Occasionally remind your employees to be expeditious about retrieving print jobs from shared devices. Another good annual reminder email.

IT Risk Management

IT Risk Management and the Real World

Risk management is the process of identifying, assessing, and controlling threats to an organization's IT assets. These risks stem from a variety of sources including financial uncertainties, legal liabilities, technology issues, strategic management errors and accidents. Organizations need to identify what is at risk and derive a plan to mitigatethe risk before it can affect operations. All organizations have some type of risk.

What is yours and how will you address it?

Continuous Vulnerability Scans

Vulnerability scans are a critical part of any Security Program. Vulnerability scans cancatch any major security holes that need to be assessed and remediated. Defenders must have timely threat information available to them about: software updates, patches, security advisories, threat bulletins, etc., and they should regularly review their environment to identify these vulnerabilities before the attackers do.
It is better to know what vulnerabilities an IT system, device or software has insteadof finding out after someone has accessed or stolen valuable data. Items to considerwhen developing a Vulnerability Scan scheme include:

- Use vulnerability scanning tools that map vulnerabilities to one or more of the following industry-recognized vulnerability, configuration and platform classification schemes and languages, which are part of the Security Content Automation Protocol (SCAP):
    a) Common Vulnerabilities and Exposures (CVE®).
    b) Common Configuration Enumeration (CCE).
    c) Open Vulnerability and Assessment Language (OVAL®).
    d) Common Platform Enumeration (CPE).
    e) Common Vulnerability Scoring System (CVSS).
    f) Extensible Configuration Checklist Description Format (XCCDF).
    g) More information about SCAP can be found in NIST Special Publication 800-126 Revision 3: The Technical Specification for the Security ContentAutomation Protocol (SCAP).

- Perform both authenticated and unauthenticated vulnerability scans using aSCAP-compliant vulnerability scanning tool.
- Perform scans on both internally and externally exposed IT assets.
- Perform the scans on a regular basis or when a new vulnerability that has apossible impact to the organization has been identified.

Patch Management

A great way to protect IT systems and sensitive data from the "Real World" is to keepyour IT systems patched. Patch management fixes vulnerabilities on IT software and applications that are susceptible to cyberattacks, helping your organization reduce itsIT security risk. NIST 800-40R4 will tell you all you need to know about patch management.

CSG and DoIT will help you out with all of this by scanning and producing reports. These vulnerability reports are available to you. You can reach out to CSG at the NH-CIC email address. The critical action for you is to INSIST that those responsible and accountable mitigate the most critical vulnerabilities on the systems your Business Process relies upon. This goes for VENDORS as well…especially for VENDORS! Remember, the most important vulnerabilities to eliminate might be "medium" on a public facing system instead of a "critical" vulnerability outside the DMZ where nobody from the public can even see it, let alone exploit it. Ask questions and get answers!

IT Service Provider Management (Systems andServices Acquisition)

IT Service Provider Management and the Real World

Vendors are our partners. In many cases, we could not get the business done without them. Having a solid grasp of IT Service Provider Management will help you obtain maximumvalue from vendor relationships. Keep in mind that vendors provide a service and are looking to sell their products and services. Keep your feet on the ground and verify what it is that you need and purchase only the things you need to meet your strategicIT goals. Also remember, Vendors can be one of our largest sources of cybersecurity risk!

Reach out to NH-CIC@doit.nh.gov and work with your IT LEAD to talk about how to work with prospective vendors to complete a Vendor Readiness Assessment (Link coming soon) or obtain StateRamp Certification to help manage this risk.

Application Software Security

It is imperative that information and system security be built into projects from thevery beginning, before the first line of code is written.

Best practices for application software security are available on the Open Web Application Security Project (OWASP) Software Assurance Maturity Model (SAMM) pageof the OWASP site.

Integral areas of a Secure Software Development LifeCycle (SSDLC) include but are notlimited to:

- Application Security Governance.
- Security Requirements and Assessment.
- Secure Design and Implementation.
- Application Security Verification.
- Application Security Operation/Maintenance.

More info about SSDLC can be found at Digital Varys' Secure SDLC (S-SDLC) – DevSecOps Road Map.

Penetration testing is recommended (and may be required depending on the classification of the data the application processes) as it helps ensure that an application is resilientand free from vulnerabilities.

DoIT's Software Development Methodology should be used for internal development projects.

Software Supply Chain

Software supply chain attacks are an ever-increasing risk in our complex computing environments, which often contain many dependencies, and which is why it is important to have an inventory of all components used in a product's developmentprocess. A software supply chain inventory is also known as a software bill of materials (SBOM) and should take into consideration the risks that each third-partycomponent could pose. Best practice is to review the list monthly to identify any changes or updates and validate that all components are still supported.

The entire concept of a Software Bill of Materials (SBOM) is included here for awareness purposes. Right now, the SoNH (and most other organizations) are not quite far enough in the maturity model to effectively use SBOMs.

Security Engineering Principles

Cyber-attacks are increasingly targeting software vulnerabilities at the applicationlayer. It is difficult to address these vulnerabilities: Software at this layer is complex,and software security ultimately depends on the many software developers involved.

Examples of best practice security engineering principles include:

1) Concept of least privilege.
2) Enforcing mediation to validate every operation that the user makes.
3) Promoting the concept of "never trust user input."
4) Developing layered protections.
5) Establishing sound security policy, architecture and controls as the foundationfor design.
6) Incorporating security requirements into the system development lifecycle.
7) Delineating physical and logical security boundaries.
8) Tailoring security controls to meet organizational and operational needs.
9) Reducing risk to acceptable levels, thus enabling informed risk management decisions.

Developer Training

Increasing developers' awareness of secure coding practices is an essential componentin reducing the likelihood of software vulnerabilities being introduced during the development process. Ideally, developers will be provided in-depth training on generalsecurity principles and secure coding practices at least annually.

Excellent resources can be found at the Open Web Application Security Project (OWASP) Source Foundation for Application Security website, including:

- Security Knowledge Framework.
- Secure Coding Practices.
- Secure Coding DoJo.

What should you do about this? Ask your IT Lead and Agency Business Manager if there are sufficient funds in the Class 27 Budget to Train your embedded ASD Developers. A small investment every year can have significant impact on a Developer's technical health and ability to best support the Agency's Digital Transformation Efforts.

Threat Modeling

Threat modeling is a good way to identify and address application security flaws whendesigning a system or software.

A threat model typically includes:

- Description of the subject to be modeled.
- Assumptions that can be checked or challenged in the future as the threat landscape changes.
- Potential threats to the system.
- Actions that can be taken to mitigate each threat.
- A way of validating the model and threats, and verification of success ofactions taken.

Additional Resources:

- Threat modeling overview, from OWASP.
- Threat modeling for the cloud, from NIST.
- Threat Modeling Fundamentals, from CISA.

Service Provider Classification, Contracts and Decommissioning

Classification of service providers may include one or more characteristics, such asdata sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk.

Service provider contracts can include security requirements, such as security incidentand/or data breach notification and response, data encryption requirements and data disposal commitments.

Secure decommissioning of service providers should not be overlooked. Some considerations include user and service account deactivation, termination of dataflows and secure disposal of enterprise data within service provider systems.

This is all included in the Vendor Readiness Assessment Report and/or third-party attestations we mentioned previously. These Policies and Procedures are your Agency's friend! Use them to your advantage.

IT System and Communications Protection

IT System and Communications Protection and the Real World

Many people put up a fence around the yard to keep their pets safe and in the yard and everyone else out. Similarly, the goal of IT system and communications protectionis to provide network segmentation and boundary protection throughout an organization's IT Infrastructure.

Network Infrastructure Management

Keeping network infrastructure up to date includes running the latest stable releaseof software and using currently supported network-as-a-service (NaaS) offerings.

Examples of securely managing network infrastructure and communication protocolsinclude using version-controlled-infrastructure-as-code and secure network protocolssuch as SSH and HTTPS.

Failure in Known State

Failure in a known state addresses IT security concerns in accordance with the mission/business needs of organizations. Failure in a known secure state helps to prevent the loss of confidentiality, integrity, or availability of information in the eventof failures of organizational Information Systems or system components. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving IT system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission/business processes.

Email and Web Browser Protections

Network-based URL filtering can reduce the risk of connecting to malicious websites.Examples of URL filtering implementations include:

- Category-based filtering.
- Reputation-based filtering.
- Using block lists.

Spoofed emails are a common problem. Implementing DMARC, starting with the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standardslowers the chance of spoofed or modified emails from valid domains.

Here are some easy things for you to do:

- ***DoIT takes care of email filtering for you, but ask your IT Lead sometime to get you one of the monthly reports from Technical Support Services so you can see how much email is filtered out before it even gets to your inbox!***
- ***Also – Encourage your users to take advantage of the "Report Phish" button in Outlook if they receive an email that just does not smell right! It looks like this:***

IT System and Information Integrity

IT System and Information Integrity and the Real World

To protect your IT assets, you need to know what is happening in your IT environment,including knowing and understanding what your users are doing and attempting to do.You do not want your users bringing random, unauthorized devices and software into your network. Controlling, monitoring, and logging devices and software on, and all actions on, your IT network is a key step to maintaining the integrity of your IT systems and data contained therein.

Malware Defenses

One of the best ways to keep the network and computing environment secure is to keep unknowns out of the environment. Some key areas to keep in mind include butare not limited to:

- **Rogue devices** on the network. When an unauthorized or unknown computer or device is connected to a trusted network or resource, it could (accidentallyor intentionally) allow malicious software into the environment. When an unauthorized asset is found on the network, it is best practice to remove the asset from the network, deny the asset from connecting remotely to the network or quarantine the asset.
- Using technical controls, such as digital signatures and version control, can help to ensure that **only authorized scripts**, such as specific .ps1, .py, etc.,are allowed to execute.
- Disabling autorun, auto-play and auto-execute functionality for **removablemedia** is an excellent way to reduce the risk from malware-infected USB devices.
- **Enable anti-exploitation features**, such as Microsoft DEP (Data Execution Protection), wherever possible. This feature prevents code from executingfrom memory spaces not explicitly tagged for executable code.
- It is best to have a separate computer/device, segmented from the primary network, for **administrative tasks** or those tasks requiring administrative access.

Monitoring

Automated tools are critical for near real-time analysis and monitoring. These toolscan include host-based intrusion detection systems (HIDS), network-based intrusiondetection systems (NIDS), transport-based or storage-based event monitoring and Security Information and Event Management (SIEM) technologies. The NHCIC has you covered.

Unsupported Software

Outdated, unsupported software is a danger that cannot be overstated. There may beno greater security risk than continuing to use unsupported software. The Center for Internet Security (CIS) maintains a list of end-of-support software:

- End-of-Support Software Report List.

For Enterprise systems, DoIT and CSG have you covered. It is very important you periodically ask your vendors about this. Make them prove it to you annually. If you did it correctly up front, it is part of the contract and they are REQUIRED to provide you this information. Hold them to it!

IT Security Planning

IT Security Planning in the Real World

IT security planning can at times seem like a mountain to conquer. Keep in mind that NASA did not get to the moon on the first rocket launch. It took many trials and errorsuntil their plan was a success. Take the same approach with IT security planning.
Approach it slowly and methodically to determine what works best for your organization.

What is an IT Security Plan?

An IT security plan describes, at a high level, how the IT security controls, and control enhancements, meet IT security requirements. IT security plans contain enough information to enable a design and implementation that is compliant with the intent of the plans.

What Makes an Effective IT Security Plan?

IT security plans need not be single documents; the plans can be a collection of various documents including ones that already exist. Effective IT security plans makeextensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. For example, IT security plans do not contain detailed contingency plan orincident response plan information; instead, they provide explicitly or by reference, sufficient information to define what needs to be accomplished by the contingency and incident response plans.

What IT Systems Should Have a System Security Plan (SSP)?

Technically speaking, all IT systems should have an SSP. An SSP documents the who,what, where, why, when about the system, including but not limited to:

- What is the system's functionality and purpose?
- Who owns and administers the system?
- Where does the system reside and what data does it process, store and/or transmit?
- Who is impacted if the system is offline?

- What system security and maintenance practices are in place for the system?
- What language is an application written in?

These are all questions that are answered within an SSP, which is why they are so important. Here's the Policy and DoIT has a template you can use to create an SSP.

Acceptable Use of State Data and IT Resources (AUP)

Acceptable Use and the Real World

Although most users may know what acceptable use for IT resources is within an organization, it is still important to create a formally documented acceptable use policy that is read, understood, signed, and followed by employees. Most organizationsuse an AUP to support due diligence regarding the security of the IT environment.Remember to consult stakeholders in human resources, finance, legal and IT security when developing an AUP. An AUP can also protect organizations from legal actions, which can become costly.

Here ***is how to get it right!***

Best Practice Regarding Using State Email Accounts to SendInformation to a Personal Email Account

Do not forward email that contains state data from your state email account to yourpersonal email account. The only emails you should forward from a state email account to your personal account would be those about you alone, such as a certificate for completed training, your résumé or information about benefits and such.

Continuous IT Vulnerability Management &Patching

Continuous Vulnerability Management & Patching and the Real World

Just as with other IT security topics, vulnerability management and patching can sometimes seem overwhelming. What you need to do is take a step back and see whatyour organization's IT footprint looks like. Start small and build out a plan taking into consideration the highest risk areas first. NHCIC will help you with this and even provide vulnerability scans to you. Just ask!

Continuous Vulnerability Scans & Patch Management

When performing vulnerability scans, it is recommended that tools being used areusing Secure Content Automation Protocol (SCAP).

Refer to the NIST publication on Enterprise Patch Management here.

Network Monitoring and Defense

Best practices for network defense include:

- Intrusion monitoring solutions such as Network Intrusion Detection System(NIDS) or equivalent Cloud Service Provider (CSP) service.
- Network segmentation.
- Traffic filtering between network segments.

An example of port-level access controls is utilizing 802.1X or similar network accesscontrol protocols such as certificates and may incorporate user and/or device authentication.

Here again, DoIT and CSG have you covered for Enterprise systems and any Agency systems/applications hosted in DoIT Data Centers. Keep an eye on the vendors. Again, if we did it right up front, it is part of the contract requirements…hold them to it!

Exception Requests

Security Exception Process / Compensating Controls

At the end of the day, it is all about risk. If you need an exception to an IT Policy, Procedure, or Standard there is a way to request it. Generally, this policy tells you how to make the request.

However, if you have a business need for some non-standard software, this is how you go about getting it reviewed for approval.

Wrapping It Up

Cybersecurity is a team sport. Never feel alone. You are not. There is help, guidance, and support available. You may not have asked for this job specifically, but you can excel at it. We are here to help you!

If you only take one thing away from this entire document:

REPORT A CYBER SECURITY EVENT:

During Business Hours:

Monday-Friday; 7:30AM-4:30PM EST

Phone: (603) 271-7555

Email: helpdesk@doit.nh.gov

Non-Business Hours: (603) 271-7555, Option 2