SESSION 5: BACKUP STRATEGIES
OCTOBER 27, 2020
IN THIS PRESENTATION

- Overview
- Controls & Protections Recap
- Internal Hard Disk Drives
- Removable Storage Media
- Cloud Storage
- Incident Response
- Disaster Recovery
- Process Improvements
OVERVIEW: TRAINING SERIES

Raise awareness about cybersecurity's importance
Help keep data from bad actors
Understand use of hardware/software tools
Understand practical steps to protect your networks
Reduce volume and impact of attacks
No program leads to 100% success

OVERVIEW: TRAINING SERIES

Ensure all users are made aware of security risks, applicable policies, standards and procedures
Ensure personnel are trained to carry out their assigned security-related duties and responsibilities

Provide security awareness training on recognizing and reporting potential indicators of insider threat
Provide awareness training focused on recognizing and responding to threats from social engineering, etc. Update at least annually or when there are significant changes.
Include practical exercises aligned with current threat scenarios

IN THIS PRESENTATION

• Overview
• Controls & Protections Recap
• Internal Hard Disk Drives
• Removable Storage Media
• Cloud Storage
• Incident Response
• Disaster Recovery
• Process Improvements
CONTROLS & PROTECTIONS RECAP

Plan, Protect, Preserve

Assume You are a Target

Install and Update Security Software

Implement and Test Backups

Physically Protect Network and Hardware

10/27/20
CONTROLS & PROTECTIONS RECAP

- Ensure Wi-Fi Connection is Secure
- Change the default password
- Require a password to get on network
- Segregate your network
- Enable firewall

Older Installations May Not Be Secure
- Ensure Anti-Virus is Fully Running & Updated
- Ensure All Security Software is Updated
- Regularly Check Privacy Tools, Add-Ons & Patches

Have a Back-Up Strategy
- Lock Your Screen
- Use a Secure Connection
- Make Sure Encryption Tools Installed
- At home, segregate Work From Personal Computing
CONTROLS & PROTECTIONS RECAP

Which is an example of a strong password?

a) scottbaseball  b) chadpassword  c) abcdef123456  d) iBwPxGaC934!

These update software to correct security concerns and improve functionality

a) Downloads  b) Protocols  c) Viruses  d) Patches
CONTROLS & PROTECTIONS RECAP

These update software to correct security concerns and improve functionality

a) Downloads  b) Protocols  c) Viruses  d) Patches

You notice a flash drive in your office training room. You should NOT ___________.

a) Report it to your IT department
b) Insert it into your computer
c) Destroy it
d) Leave it, maybe the owner will come get it

CONTROLS & PROTECTIONS RECAP

You notice a flash drive in your office training room. You should NOT ___________.

a) Report it to your IT department
b) Insert it into your computer
c) Destroy it
d) Leave it, maybe the owner will come get it
CONTROLS & PROTECTIONS RECAP

*It is important that you install and ______ your security software.*

a) Update  b) fugetaboutit  c) Remove  d) All of the Above

This is an example of an encryption tool.

a) Firelocker  b) Bitlocker  c) Bitmoji  d) Scrambler
CONTROLS & PROTECTIONS RECAP

This is an example of an encryption tool.

a) Firelocker  b) Bitlocker  c) Bitmoji  d) Scrambler

DATA BACKUP OPTIONS: 3-2-1 RULE

All critical data should be backed up
One backup may not be enough
3 – Keep 3 copies of any important file
2 – Keep files on 2 different media types
1 – Store 1 copy offsite
Rewritable drives that store most of the information computers need in order to run, as well as the user’s primary working files. Secondary systems and backup servers also store data on internal hard drives.

**INTERNAL HARD DISK DRIVES: PROS**

- Quickly update backup files
- Maintain simple file structure
- Saves cost of purchasing another storage device

**INTERNAL HARD DISK DRIVES: CONS**

- Rolling backups can silently propagate malware in primary files to backup files.
- Damage to internal hard drive could cause loss to primary and backup files.
- More backups means less space for computer to operate
- Limited working lifespan of internal hard drive
INTERNAL HARD DISK DRIVES: SECURITY

- Backup files have the same vulnerability to damage and corruption as primary files.
- Only as physically secure as the computers that house them.
- Primary and backup data can be erased via magnetic degaussing.
- Encrypt drive's contents, physically secure computer, follow network security recommended practices.

IN THIS PRESENTATION

• Overview
• Controls & Protections Recap
• Internal Hard Disk Drives
• Removable Storage Media
• Cloud Storage
• Incident Response
• Disaster Recovery
• Process Improvements

REMOVABLE STORAGE MEDIA

Storage media that connects to and disconnects from the computer and is a more versatile backup option than your computer's internal hard drive by keeping your data safe from both online attackers and power surges.
REMOVABLE STORAGE MEDIA: TYPES
- External Hard Disk Drives
- Solid-State Storage
- Optical Storage
- Magnetic Tape

REMOVABLE STORAGE MEDIA: PROS
- Portable
- Work with most computers
- Variety of storage capacities
- Can be cost effective
- Most are reusable.

REMOVABLE STORAGE MEDIA: CONS
- Portability increases chance of loss
- Increased chance of theft
- Rolling backups can spread malware from primary to backup files
REMOVABLE STORAGE MEDIA: SECURITY

- Direct control over data
- Password protect removable device
- Encrypt data when possible
- Only connect to systems that follow recommended network security practices
- Remove from computer after completing backup and physically secure

IN THIS PRESENTATION

- Overview
- Controls & Protections Recap
- Internal Hard Disk Drives
- Removable Storage Media
- Cloud Storage
- Incident Response
- Disaster Recovery
- Process Improvements

Cloud storage customers rely on expanded internet broadband to access a shared pool of computing resources (e.g., networks, servers, storage, applications, and services) owned by a cloud service provider.
CLOUD STORAGE: PROS

- Worst-case protection
- Protect against critical failures of local devices due to malware
- Anytime access to data anywhere you have an Internet connection
- Purchase cloud storage space as needed
- Some providers ensure regulatory compliance in handling sensitive data

CLOUD STORAGE: CONS

- Dependence on internet can delay communications between machine and cloud
- No universal standards, platforms or languages
- Potential problems with jurisdiction and fair information practices
- Customer has little knowledge of service provider's cloud infrastructure or reliability
- Users surrender most control over their own data

CLOUD STORAGE: SECURITY

- Cloud providers can encrypt user data and critical information
- Data stored with other users’ data posing a security risk
- Carefully check service agreement for security practices
CLOUD STORAGE: SECURITY

- Look for provider that encrypts data with established encryption algorithms (AES, Blowfish, etc).
- Transfers data via secure socket layer (SSL) connection.
- Follows network security recommended practices.
- Physically protects hardware that stores, processes and transmits data.
- Prevents data from leaking to other customers on its cloud.

DATA BACKUP SUMMARY: CONSIDERATIONS

- Consider advantages and risks of each media.
- Consider the quantity of data to back up.
- Consider the sensitivity of your data.
- Consider your financial resources.
- Consider the accessibility of the data.

IN THIS PRESENTATION

- Overview
- Controls & Protections Recap
- Internal Hard Disk Drives
- Removable Storage Media
- Cloud Storage
- Incident Response
- Disaster Recovery
- Process Improvements
INCIDENT RESPONSE

An organization’s systematic approach to prepare for, detect, contain and recover from a suspected cybersecurity breach or attack.

INCIDENT RESPONSE

Helps ensure an orderly, effective response to cybersecurity incidents, which in turn can help protect an organization’s data, reputation and revenue.

INCIDENT RESPONSE

- Establish operational incident-handling capabilities
- Detect and report events
- Analyze and triage events to support event resolution and incident declaration
- Develop and implement responses to declared incidents according to pre-defined procedures
- Perform root cause analysis on incidents to determine underlying causes
INCIDENT RESPONSE

Track, document and report incidents to designated internal and external authorities
Test the organizational incident response capability
Use knowledge of attacker tactics, techniques, and procedures in incident response planning and execution
Establish and maintain a security operations center that facilitates a 24/7 response capability
In response to cyber incidents, utilize forensic data gathering across impacted systems
Use a combination of manual and automated, real-time responses to anomalous activities that match incident patterns

Incident Response doesn’t end when an incident is over. It continues to provide support for successful litigation, documentation to show auditors, and historical knowledge to feed into the risk assessment process and improve the incident response process itself.

In this presentation
• Overview
• Controls & Protections Recap
• Internal Hard Disk Drives
• Removable Storage Media
• Cloud Storage
• Incident Response
• Disaster Recovery
• Process Improvements
DISASTER RECOVERY

- Regularly perform data backups
- Regularly test backups
- Protect your backups

IN THIS PRESENTATION

- Overview
- Controls & Protections Recap
- Internal Hard Disk Drives
- Removable Storage Media
- Cloud Storage
- Incident Response
- Disaster Recovery
- Process Improvements

PROCESS IMPROVEMENTS

- Invest and support IT and security operations
- Conduct training at least annually
- Prioritize risk assessments and incident response plans
- Monitor networks for unusual traffic daily or continuously
- Regularly review, assess and improve policies and procedures
- Increase knowledge base by reading privacy and security publications
SUMMARY

- Chose the backup strategy that is right for you
- Regularly test backup strategy
- Implement and test Incident Response plan
- Continually assess and improve processes and procedures
- Document, Document, Document

Quiz
SUMMARY: QUIZ

Which of these is an example of Solid-State Storage?

a) CD-RW  b) Flash Drive  c) Zip Drive  d) Magnetic Tape

The more backup files are stored, the less space is available on the computer to operate. This is the downside of which type of backup?

a) Internal Hard Drive  b) Cloud Storage  c) Removable Media  d) Memory Stick
The more backup files are stored, the less space is available on the computer to operate. This is the downside of which type of backup?

- a) Internal Hard Drive
- b) Cloud Storage
- c) Removable Media
- d) Memory Stick

Additionally, this type of backup provides anytime access to data and applications anywhere there is an internet connection, with no need for you to invest in networks, servers, and other hardware.

- a) Internal Hard Drive
- b) Cloud Storage
- c) Removable Media
- d) Memory Stick
This type of storage media connects to and disconnects from the computer and helps keep data safe from both online attackers and power surges.

a) Flash Drive  b) Cloud Storage  c) Internal Hard Drive  d) RAM

This is the organization's systematic approach to prepare for, detect, contain and recover from a suspected cybersecurity breach or attack.

a) Disaster Recovery  b) Organizational Security  c) Process Improvement  d) Incident Response
This is the organization's systematic approach to prepare for, detect, contain and recover from a suspected cybersecurity breach or attack.

a) Disaster Recovery
b) Organizational Security
c) Process Improvement
d) Incident Response

SUMMARY: CYBER SECURITY MONTH

THINK BEFORE YOU CLICK

DO YOUR PART.
#BECYBERSMART

Cyber incidents are not just technical problems.
They are business problems

DO YOUR PART.
#BECYBERSMART
SUMMARY: NEXT SESSION

SESSION 6: DOCUMENTATION DEVELOPMENT
THURSDAY, OCTOBER 29, 2020
11:30 AM

RISK MANAGEMENT
INFORMATION SECURITY
USER BEHAVIOR
CONTROLS & PROTECTIONS
BACKUP STRATEGIES
DOCUMENTATION DEVELOPMENT

THANK YOU!
TRAINING SUPPLEMENT

SESSION 5: BACKUP STRATEGIES
OCTOBER 27, 2020
There are many risks to your data, including hardware failure, natural disasters, human error, theft, and attacks such as malware and ransomware. You might not be able to anticipate every data risk, but a strong backup and recovery plan will help you quickly return to operation.

Here are three things you can do in your role to #BeCyberSmart.
This short guide to leading practices for data backup and recovery draws on the experience of the State Auditor’s Office and experts such as the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS).

1. Define your expectations and intent in a policy

A policy over backup and recovery communicates your expectations and the goals for protecting the government’s data and assigns responsibility to ensure it happens. Are particular systems critical to your operations? If so, you might want to save multiple copies of your data in case access to your system and backup is prevented by a ransomware attack. If your data or systems were damaged, could you manually re-create all of your transactions? If not, you might want to make a backup very frequently.

2. Establish a strategy to communicate how you intend to implement the policy

The backup strategy may be incorporated in the policy or your procedures, or may be a separate document. The strategy is generally the responsibility of management (CIO/CISO/IT manager) and contains guidance to implement the expectations and goals you set in your policy. The strategy can depend on multiple factors, including specific departmental backup needs.

An effective backup strategy addresses:

- Who is responsible for implementing, managing, maintaining, and verifying the system works as planned
- What data or systems should be backed up
- Where the backup should be located – onsite, offsite, or in the cloud
- When and how often data or systems should be backed up. Data with no paper record must be backed up more frequently, while data that changes infrequently or is easily created can be backed up less frequently.
- How the backup files will be protected. For example, is the backup physically protected, and do only authorized users have access?
- How long the backup files will be kept. For critical backups, you might want an additional copy maintained offsite to protect the data in the event of a regional disaster or ransomware.

3. Establish a documented plan or procedures to ensure consistent implementation

The backup procedures are the steps used by your IT staff to implement the backup strategy. Clearly documented steps identify the procedures to initiate, schedule, and validate each backup to ensure data has been saved. These procedures will also help you manage the process during employee absence or turnover.

An effective backup procedure will include:

- **Backup schedules.** The frequency of the backup will be defined based on your strategy. If you use an automated backup system, the schedule
Now that your data is backed up safely, the next step is to ensure you can continue operations while you recover your data from your backup. The key to ensuring your government can rebound from a natural disaster or cyberattack is being able to quickly recover your most important data. There are two plans that address different aspects of ensuring speedy recovery of data and operations:

- **A business continuity plan** helps you continue all aspects of business operations during and immediately after a disaster. This can include plans for operating using manual records, establishing functionality to work remotely, defining alternate emergency office locations, and recovering data needed for critical operations during the disaster.

- **A disaster recovery plan** focuses on how a government responds and returns operations back to normal once the event has concluded, with a focus on information and technology. This can be included as part of a business continuity plan, or presented separately.

### 1. Identify your most common significant disaster risks

Identify all the risks that can affect operations and carefully consider how they could affect your organization. Ransomware is a significant risk for most governments. In Western Washington, a major earthquake or flood is a significant risk. In Central and Eastern Washington, wildfires and floods can be significant risks.
2. **Evaluate your backup and recovery plans relative to your significant disaster risks**

   There is no one-size-fits-all plan. The process for recovery will vary depending on what happened and how you implemented your backups. Consider whether your backup solution(s) will support your recovery for the risks you identified.

   - Consider storage location. A backup stored locally on disks or tape is easy to quickly restore but could be destroyed by the same fire that destroyed your normal operations. A backup stored with a cloud provider or an external vendor might protect your backup from a regional event.

   - Consider where you will restore your backup. A regional event might destroy your normal operations center. Is there a secondary site that you can use?

   • Once business continuity and disaster recovery plans are established, periodic checks over the recoverability of the backed up data will help to ensure that information can be accessed when necessary.

   **Here are a few resources to consider:**
   - [Ready.gov](https://ready.gov)
   - Purpose of an IT Disaster Recovery Plan and information related to data backup.
   - [IT Disaster Recovery Plan](https://www.ready.gov/equipment/it)
   - Washington State Office of the Chief Information Officer Guideline on setting up a recovery plan
   - [IT Disaster Recovery and Business Resumption Planning Guidelines](https://www.ready.gov/equipment/it)

Maintain your backup and recovery best practices

1. **Communicate and train employees on best practices**

   Regular training on your backup practices, expectations and risks will help to ensure that data can be recovered in an emergency. This can address:

   - How employees schedule and initiate data backups and what they should do if the backup fails
   - How often and what data should be backed up
   - The importance of keeping backups and testing backup recovery on a routine basis

2. **Annually review the backup, business continuity and disaster recovery plans**

   As you add new systems or technology or eliminate old systems, your backup, business continuity and disaster recovery plans will need to change. An annual review will help you capture those changes in a timely fashion so you will be prepared when you need to use your backup.

   **Here is a resource to consider:**
   - National Institute of Standards and Technology
   - In-depth guide for backup and recovery plans, policies, and strategies
You have an important role to play

As a leader, you help set the tone and cultural direction of your organization. By starting with these three steps, and ensuring the departments within your government work together on these issues, you are on your way to improving your cybersecurity program.

Department of Homeland Security - Questions every CEO should ask about cyber risks:
https://www.us-cert.gov/ncas/tips/ST18-007

Our Office also offers training at conferences on cybersecurity. For upcoming dates and times, visit

sao.wa.gov/BeCyberSmart

Sources:
Department of Homeland Security
National Institute of Standards and Technology
Center for Internet Security