Incident Response Process

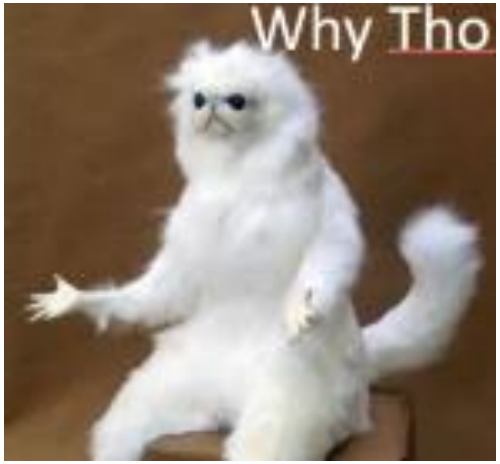
EDUCATION SERVICE CENTER, REGION 20

Serving the Educational Community

Agenda

- What users should know
- Incident Response Process
- Incident Response Tools
- Notification Requirements

Incident Response - Why Though?



Without an incident response capability, the potential exists that in the event that a security incident occurs, it will go unnoticed and the magnitude of harm associated with the incident will be significantly greater than if the incident were noted and corrected.

We are familiar with fire drills.
Active shooter drills are becoming more common.
How do you respond to a Cyber incident?

1. Who are your first responders?
2. Can your users recognize a threat?
3. How do you manage an incident?

In 2017, there were **1,579** publicized breaches that led to **178 million** personal records being exposed (ITRC).

Source: Identity Theft Research Center (ITRC) Data Breach Reports, 2015

Promote Security Sense

If you experience any of the below, report it **immediately**:

- Receive a suspicious email, text, or call, and they ask for personal or confidential information.
- Find activity on your account that you didn't do.
- If you see a suspicious person or activity in the workplace.
- You lose a device or have one stolen (computer, laptop, phone).
- Observe someone breaking policy or in a position to compromise IT security.
- Your device isn't working properly (if it's slowed down, that could be a sign of a virus).
- Security protocols are missing or not working (e.g. VPN doesn't work or laptop lock is missing).
- If you give your password to anyone, or your account has been compromised.
- If you forget your password, report it and we can get you a new one.
- If you experience a cyber attack (e.g. a virus, ransomware, etc.)
- If you find USB sticks lying around, take them to the help desk and report them.
- If you enter a bad site or if you have been a victim of pharming.

Activity to Practice Techniques

ESC 20 Serving the Educational Community

For each scenario below, state if you think it should be reported.

Scenario	Yes/No
You find a USB stick lying around in the parking lot.	YES
Your drop your personal phone on the floor and the screen cracks.	NO
Your receive an email claiming to be from the help desk. It asks you to provide your user name and password for verification.	YES
You see someone breaking policy by writing their password on a sticky note on their desk.	YES
Your co-worker brings their baby into work and it is making a lot of noise.	NO
You see an email that was sent from your email account but you don't remember sending it.	YES
Today your laptop seems very slow and hotter than usual.	YES
You clicked a link and all of a sudden you are locked out of your laptop.	YES
Your co-worker keeps spamming you with candy-crush invites.	Unfortunately, No
Everyone has a laptop lock but you don't seem to have one.	YES

Reporting and Contact Information

ESC 20 Serving the Educational Community

KNOW YOUR IT DEPARTMENT!

To report any incident:

- Contact [insert contact name] and they will be happy to help you
- [Insert contact info]
- Fill out [name of form] on [website]

Outline incident-specific reporting.

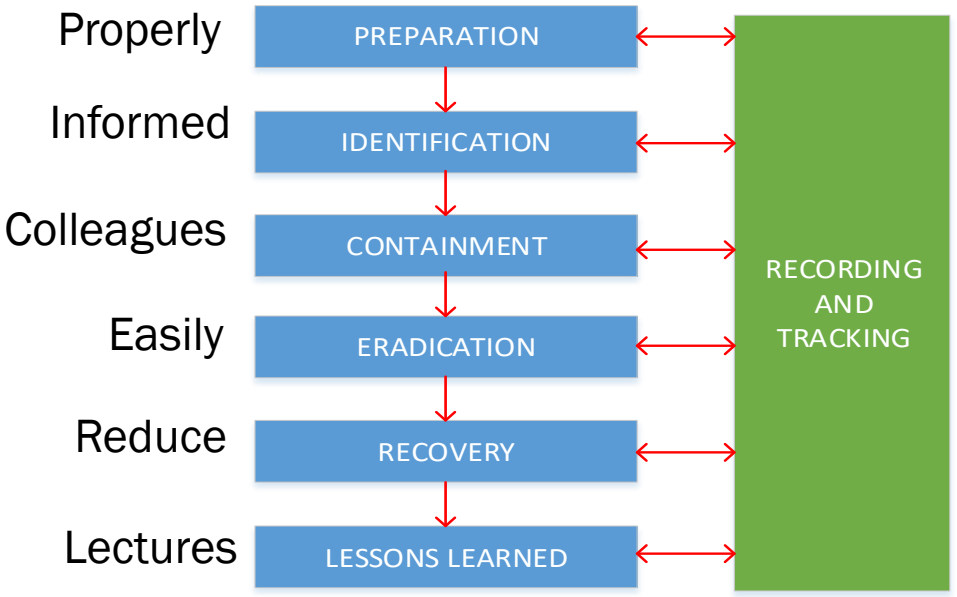
- If you have been phished, follow policy [#.#] and change your password by [method to change password]
- If you see a suspicious person or activity, contact [insert contact info] directly
- If you find a USB stick, take it to the help desk [insert location]

If you have any general questions:

- Contact [insert contact name] and they will be happy to help you
- [Insert contact info]

Incident Response Processes

Purpose: To define a specific process for managing information security incidents to minimize their impact on the organization, thus ensuring that the best possible levels of service quality and availability are maintained.



Incident Response Processes - Preparation

- Are all members aware of the security policies of the organization?
- Do all members of the Computer Incident Response Team know whom to contact?
- Do all incident responders have access to journals and access to incident response toolkits to perform the actual incident response process?
- Have all members participated in incident response drills to practice the incident response process and to improve overall proficiency on a regularly established basis?

Incident Response Processes - Identification

- Where did the incident occur?
- Who reported or discovered the incident?
- How was it discovered?
- Are there any other areas that have been compromised by the incident? If so what are they and when were they discovered?
- What is the scope of the impact?
- What is the business impact?
- Have the source(s) of the incident been located? If so, where, when, and what are they?

Incident Response Processes - Containment

ESC 20 Serving the Educational Community

1. Short term containment
   a. Can the problem be isolated?
   b. Are all affected systems isolated from non-affected systems?

2. System Backup
   a. Have forensic copies of affected systems been created for further analysis?
   b. Have all commands and other documentation since the incident has occurred been kept up to date so far?
   c. If not, then place the forensic images into a secure location to prevent accidental damage and/or tampering.

3. Long Term Containment
   a. Can the system be taken offline?
   b. If the system must remain in production proceed with long term containment by removing all malware and other artifacts from affected systems, and harden the affected systems from further attacks until an ideal circumstance will allow the affected systems to be reimaged.

Incident Response Processes - Eradication

- Have all malware and other artifacts left behind by the attackers been removed and the affected systems hardened against further attacks?
- If not, then please explain why?

- If possible can the system be reimaged and then hardened with patches and/or other countermeasures to prevent or reduce the risk of attacks?
- If not, then why?

Incident Response Processes - Recovery

- Has the affected system(s) been patched and hardened against the recent attack, as well as possible future ones?
- What day and time would be feasible to restore the affected systems back into production?
- What tools are you going to use to test, monitor, and verify that the systems being restored to productions are not compromised by the same methods that caused the original incident?
- How long are you planning to monitor the restored systems and what are you going to look for?
- Are there any prior benchmarks that can be used as a baseline to compare monitoring results of the restored systems against those of the baseline?

Incident Response Processes – Lessons Learned

ESC★20
Serving the Educational Community

- Has all necessary documentation from the incident been written?
  a. If so, then generate the incident response report for the lessons learned meeting.
  b. If not, then have documentation written as soon as possible before anything is forgotten and left out of the report.

- Assuming the incident response report has been completed, does it document and answer the following questions of each phase of the incident response process: (Who? What? Where? Why? And How?)?

- Can a lessons learned meeting be scheduled within two weeks after the incident has been resolved?
  a. If not, then please explain why and when is the next convenient time to hold it?

- Lessons Learned Meeting
  a. Review the incident response process of the incident that had occurred with all CIRT members.
  b. Did the meeting discuss any mistake or areas where the response process could have been handled better?

Incident Response Tools

ESC 20
Serving the Educational Community

Create an IR Binder

1. Incident Response Policy
2. Incident Response Process Guide
3. Run Books
4. Table Top Exercises

Incident Response Policy

ESC 20 Serving the Educational Community

Basic Security Requirements:

- An operational incident-handling capability will be developed and implemented for all organizational information systems that house or access controlled information. The incident response capability will include a defined plan and will address the six stages of incident response:
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons Learned
- Incidents will be tracked, documented, and reported to appropriate officials and/or authorities both internal and external to the organization.

Derived Security Requirements:

- Incident response capabilities will be tested.
- To facilitate incident response operations, responsibility for incident-handling operations will be assigned to an incident response team.

Incident Response Process Guide

ESC 20
Serving the Educational Community

- Outline an organizational approach to incident response.
- Define roles and responsibilities.
- Define severity and impact of incidents.

Credential Compromise Run Book

What is the incident?

- Credential compromise is when a user's ID is taken advantage of for malicious purposes.

Why should we care?

- Depending on the credentials, the attacker could then obtain access to critical information and systems

How do we respond?

- Impact, scope, and threat escalation

Table Top Exercises

Example:

Over spring break, you received an urgent message on your cellphone.

This message states that based on open-source intelligence conducted by a federal partner, some users within your domain have been found in a recent credential dump posted on the JustPastelt.su site.

This dump not only included usernames and email addresses, but also plaintext passwords. From quickly reading through the notification, you notice that there are in total 20 accounts from your organization and two of them are from network administrators.

How do you respond?

OMG!!

- How could you verify if the compromised accounts were valid?
- How is authentication and authorization done within your organization?
- How quickly could you revoke access to the compromised credentials?
- How many applications, internal and external, utilize this system or other system to manage users?
  - Which applications that your staff utilize are Internet facing?
  - Which applications are not hosted internally?
  - Which applications contain PII or other sensitive information?
- How can you verify that the compromised credentials were not used?
- How do you communicate to those users whose accounts were compromised?
- If attackers were able to use those compromised credentials, what could they access?
  - What would be the impact?
  - What about the administrator credentials?
- Does your organization have any policies regarding password use?
- Does your organization utilize multi-factor authentication?

Reporting Requirement

There is not a state statute requiring LEA's to report an Incident to DIR or TEA.

- Recommend contact their ESC to advise of an issue that might impact other LEA's or ESC's as well.

- Recommend contacting the CISO-TEA to let them know should there be a need to advise other ESC's or LEA's of a potential outbreak or threat.

Should there be a possible unauthorized access of sensitive or personal Identifying Information (PII) they are required to notify the potentially impacted students/parents or LEA employees of the potential exposure.

Breach Notification Requirements

Breach Notification Requirements

Texas Business Code

Sec. 521.053. NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA.

(a) In this section, **"breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information** maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner.

(b) (b) A person who conducts **business in this state and owns or licenses** computerized **data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.** The disclosure shall be made as quickly as possible, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.