INCIDENT RESPONSE PREPAREDNESS

March 2021

Presenters

Trent L. Leavitt
Digital Forensics & Incident Response Manager
tleavitt@eidebailly.com
385.282.5460

Matthew Solomon
Manager - Cybersecurity Services
msolomon@eidebailly.com
385.282.5422

LEARNING OBJECTIVES

- Discuss the importance of incident response preparedness
- Review the incident response process
- Identify testing that can be done to prepare an organization for an incident

EideBailly

AGENDA

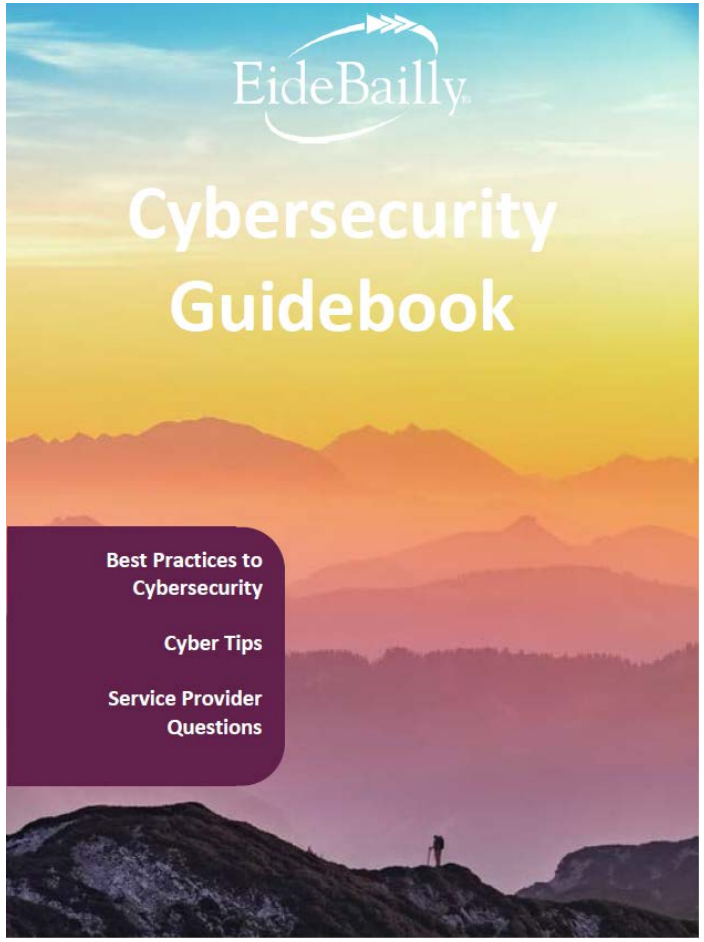
- Recent Breaches
- Incident Response Myths
- Incident Response Process
- Incident Response Do's & Don'ts
- Next Steps

PREVENTION

Best thing to do is prevent incident before it happens.

Follow the foundational security controls found in the guidebook.

- Privileged Access
- Data Backup & Recovery
- Multifactor Authentication
- Endpoint Protection
- Firewall w/ Security Services
- Email Security
- Wireless Security
- Password Management

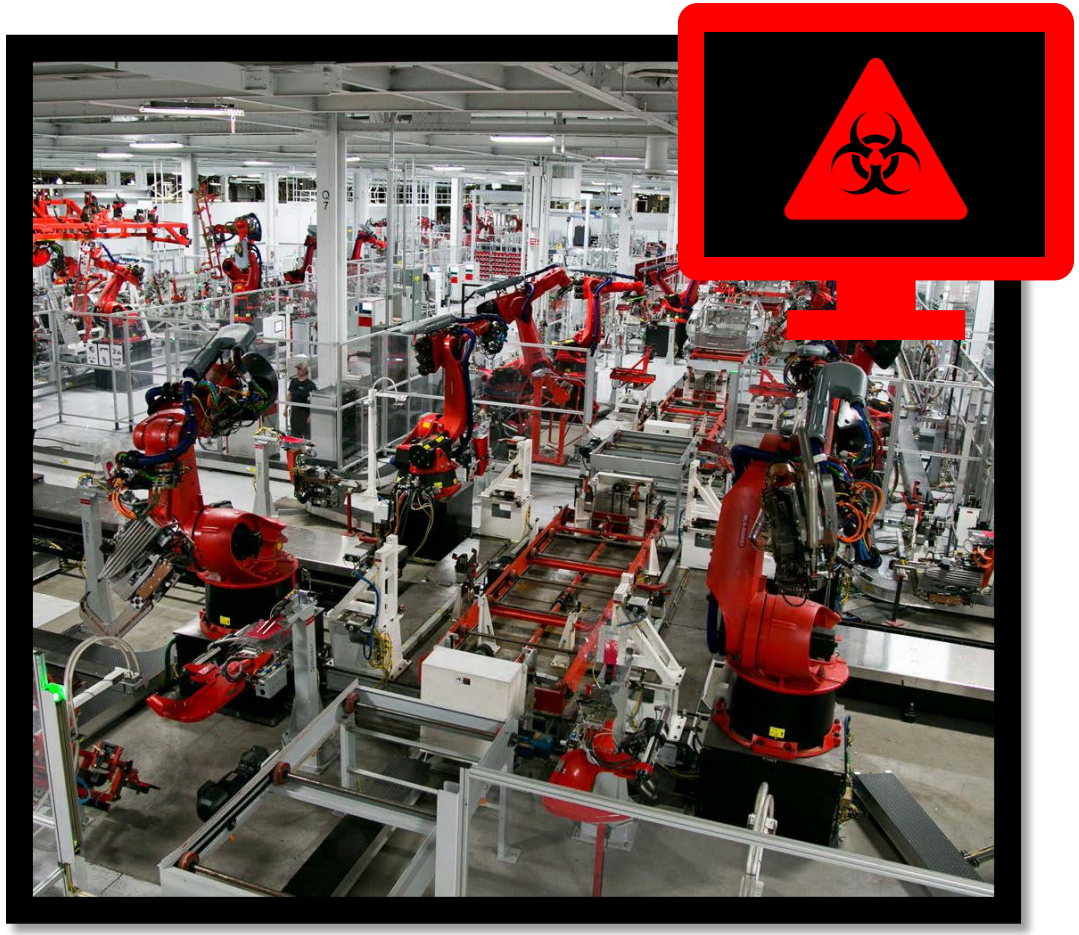


EideBailly

RECENT INCIDENTS

BREACHES OF 2020

VERIDIAN DYNAMICS



Overview:

- Ransomware attack.
- Client chose not to pay ransom.
- Systems could not be used for seven days.
- Data backups unreliable.

SISTERS of CHARITY FOUNDATION OF CLEVELAND

Overview:

- Victim of wire transfer fraud.
- Criminals had access to all the organization's email.
- Exposed 1,300 records with personal privacy information.

MYTHS

- The higher the spend, the better the security
- All you need is Anti-Virus
- I’m set, I have cyber insurance
- I’m not responsible for Cybersecurity

TERMINOLOGY

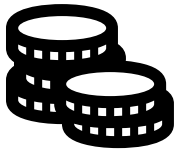
Event	Incident	Breach
• Receiving an email • Updating operating system • Firewall policy was modified	• Malware infection • Distributed denial of service attacks • Unauthorized access	• Data Loss • Unauthorized access • Insecure storage or transmission

STATISTICS

Cyberattacks are the fastest growing crime in the US

Ransomware claims a new victim ***every 5 seconds***

On average ***315 days*** to detect and contain Malicious Breach



The 2020 average cost per Breach:

- ***$3.86 million*** per breach worldwide.
- ***$8.64 million*** in the US.

83% of data breaches against small businesses are financially motivated.

Statistics from Cybersecurity Ventures, Accenture, Hashedout, EY, Ponemon

CYBER INCIDENTS ARE NOT TO BE TAKEN LIGHTLY BECAUSE IT'S NOT A MATTER OF "IF" YOU WILL GET BREACHED, IT IS A MATTER OF "WHEN" IT WILL HAPPEN

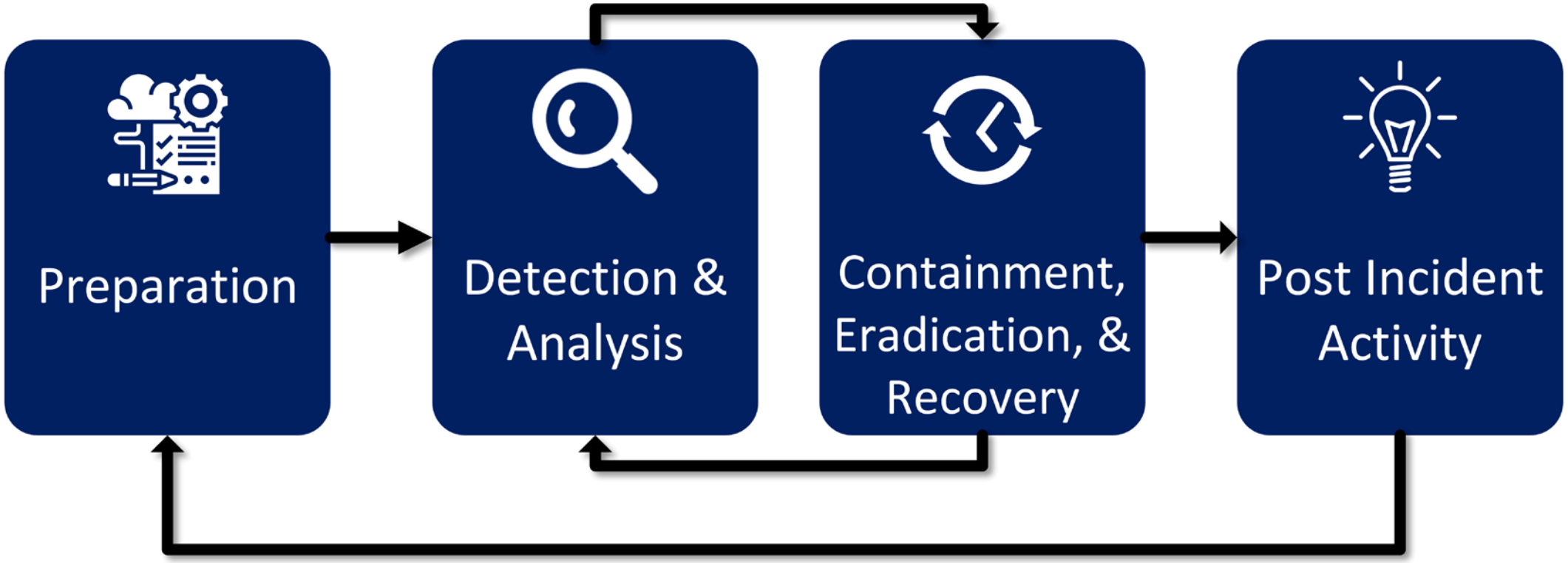
IMPORTANCE OF INCIDENT RESPONSE

- Restore operations
- Minimize losses
- Fix vulnerabilities quickly and thoroughly
- Strengthen security to avoid future incidents

Your future self will thank you for the time and effort you invest on the front end.

INCIDENT RESPONSE PROCESS

INCIDENT RESPONSE PROCESS



EideBailly

PREPARATION

PREPARATION

Preparation phase is very important.

Proper preparation:

- Allows for quicker and more effective incident handling
- Lowers probability of an incident occurring (incident prevention)

PREPARATION

This phase will be the work horse of your incident response planning, and in the end, the most crucial phase to protect your business

4 Steps of Preparation

1. Identify Key Assets
2. Prioritize Risk
3. Incident Response Plan
4. Test

Imagine doing a speech with no preparation.

STEP1: IDENTIFY CRITICAL SYSTEMS AND ASSETS

Identify critical data

- Find out where this information is stored. Is it on single machine in your office? Is it on a remote server? Is it stored in the cloud, by a third party?

Identify key processes and systems

- What business processes and systems are critical to keep your organization running?

Identify key partners

- What partners, vendors, and third-parties do you need to contact in the event of an incident?

EideBailly

STEP 2: PRIORITIZE THE RISK, AND MANAGE IT

Prioritize where you need the most protection.

Consider what would happen if you no longer had access to the critical systems or assets you've identified.
By understanding:

- What's important to your business?
- Why it's important, and
- What are you doing to protect them?

EideBailly

STEP 3: CREATE AN INCIDENT RESPONSE PLAN

Essential Elements

- A list of roles and responsibilities
- A business continuity plan, or reference continuity plan
- Key contact information
  - Authorities
  - Insurance Provider(s)
  - Vendors
  - Legal
- Communication plans
- Senior management approval

Preferred Elements

All elements within essential

+

- Strategies and goals
- Detailed playbooks
- Inventory of tools
- Prioritization of issues
- System Details (Network Diagrams/ Data Flows)

Optimized Elements

All elements within essential and preferred

+

- Inclusive When It Comes to Stakeholders
- Reporting

STEP 4: TESTING

Once you have a clear, documented plan in place, you should periodically test it through simulations to assess effectiveness and make continuous improvements.

Conduct Tabletop exercises

- A security incident preparedness activity, taking participants through the process of dealing with a simulated incident scenario and providing hands-on training for participants that can then highlight flaws in incident response planning.

EideBailly

STEP 4: EXAMPLE TABLETOP EXERCISE SCENARIOS

Scenario

A user calls the service desk complaining that their device files won't open. Appears to be ransomware.

Discussion Questions

- Would the organization ever pay the ransom? Is a cost benefit needed to be done?
- Can the organization retrieve all of the necessary data from backups? Does the organization know how long the restoration process will take?
- What steps will you take if restoring from backup is not an option?

Curveballs

- Backups are a week old
- Backups are encrypted
- Appears to be isolated to a specific department, then two days later another department is hit
- Lead IT service desk is on vacation
- You were able to recover the encrypted data, but soon realize the data will be posted online if ransom isn't paid.

Resolution & Lessons Learned

Scenario

Multiple employees stated their identity has been stolen. Found that CFO was tricked into sending all employees W-2 to criminals.

Discussion Questions

- How does your organization handle this disclosure of PII?
- Who do you contact regarding the disclosure?
- Who would be responsible for taking the lead?
- What policies or practices do you have in place to address the data loss?
- What should management do? Who else in the organization should be involved?

Curveballs

- Employees go to social media to complain and worry their information has been stolen.
- Local news picks up the story as a possible breach at your organization
- Lead IT personnel just had a baby and on leave.

Resolution & Lessons Learned

STEP 4: TESTING

Once you have a clear, documented plan in place, you should periodically test it through simulations to assess effectiveness and make continuous improvements.

Conduct simulated real-world incidents “Fire Drills”

- These tests not only evaluate what your team would do when faced up against a major incident, but how they would do it.
- Examples:
  - Communicate without email and/ or phones
  - Simulated phishing
  - Work from home
  - Utilize backup solution

EideBailly

PREPARATION - MISTAKES TO AVOID

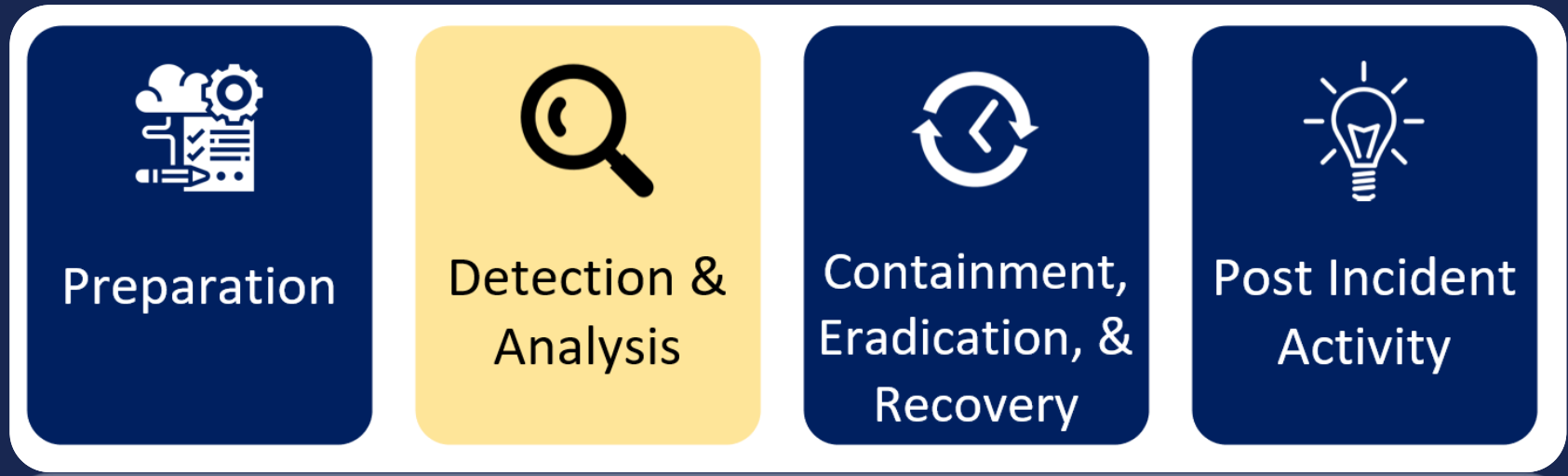
Adopting "one-size-fits-all" plans

Plans are not regularly reviewed and updated

Above all, remember the worst mistake any company can make when it comes to security incidents: thinking it couldn't possibly happen to them.

EideBailly

DETECTION & ANALYSIS

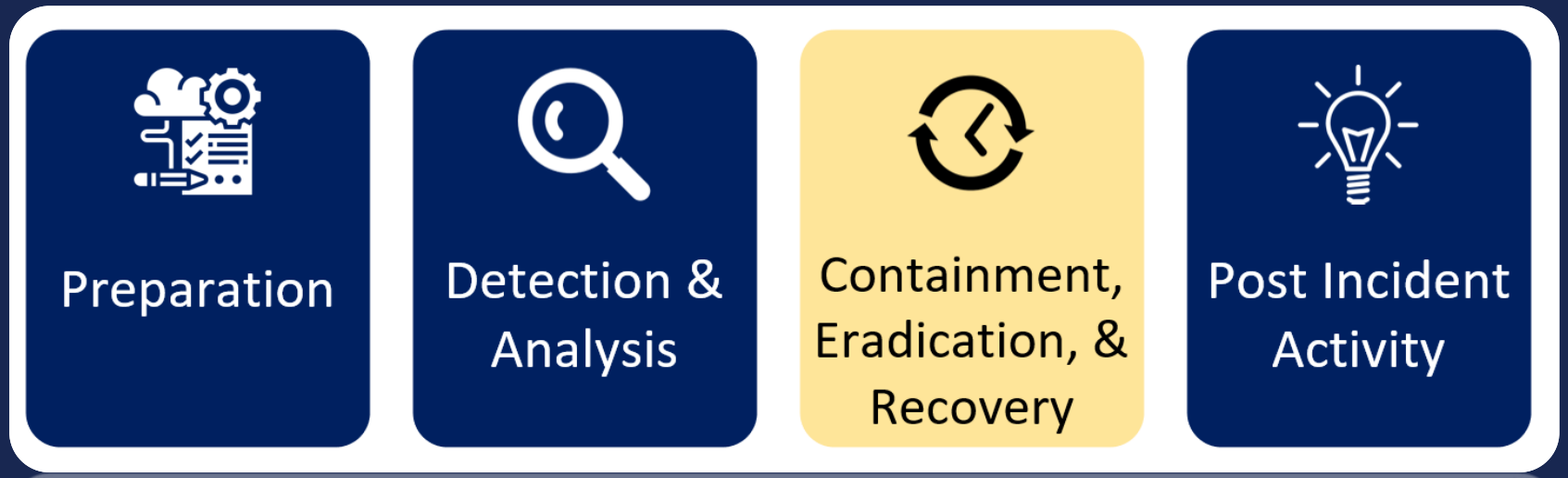


DETECTION AND ANALYSIS

The main purposes of this phase are to determine whether the incident is really occurring and analyze its nature.

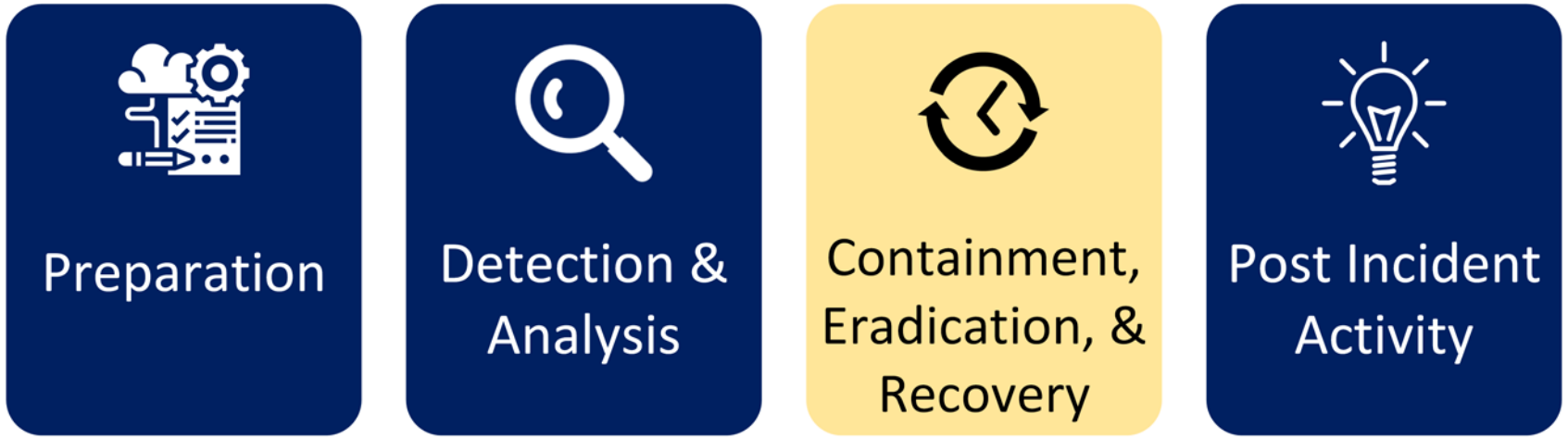
- Noticing signs of an incident (called “precursors” and “indicators”)
- Analyzing these signs
- Documenting the incident
- Prioritizing incidents
- Incident notification

CONTAINMENT, ERADICATION, & RECOVERY



CONTAINMENT, ERADICATION, AND RECOVERY

Containment: The actions required to prevent the incident or event from spreading across the network.
Eradication: The actions that are required to completely wipe the threat from the network or system.
Recovery: The actions required to bring back the network or system to its former functionality and use.



POST INCIDENT ACTIVITY

POST-INCIDENT ACTIVITY

Once the investigation is complete, hold an after-action meeting with all relevant members and discuss what you've learned from the data breach. This is where you will analyze and document everything about the breach. Determine what worked well in your response plan, and where there were some holes.

Lessons learned from both mock and real events will help strengthen your systems against the future attacks.

INCIDENT RESPONSE DON'TS AND DO'S

INCIDENT RESPONSE DON'TS

- Unplug or Power Off Any Network Devices.
- Wipe and/or Restore Devices.
- Contact the Attackers.
- Pay the Ransom Right Away.
- Notify of the Incident.
- Run an Anti-Virus (A/V) Scan.

EideBailly

INCIDENT RESPONSE DO'S

Unplug the Network Cable.	Isolate/Segregate the Network.	Preserve Logs.
Deploy an Endpoint Detection and Response (EDR) Tool.	Initiate a Global Password Reset.	Take a Screenshot of or Otherwise Preserve the Ransom Note.
Map the Network and Create an Inventory of Devices.	Document Incident.	Consideration of Creating Full Disk Forensic Images.

deBailly

NEXT STEPS

NEXT STEPS

- Don’t Wait!
- Simple Preventative measures can be implemented quickly
- Start your incident response preparedness
- There is Help

QUESTIONS?

THANK YOU

Trent L. Leavitt
Digital Forensics
& Incident Response Manager
tleavitt@eidebailly.com
385.282.5460

Matthew Solomon
Manager - Cybersecurity Services
msolomon@eidebailly.com
385.282.5422

eidebailly.com

EideBailly®

CPAs & BUSINESS ADVISORS

Find us online:

eidebailly.com