Building an Incident Response Plan

June 2022

Building an Incident Response Plan

CIAS-ISA
COMMUNITY CYBERSECURITY PROGRAMS

This webinar was developed by
the Center for Infrastructure Assurance and Security
at the University of Texas at San Antonio

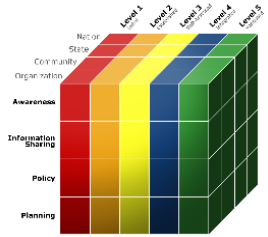
The CIAS has been working with communities to improve their cybersecurity posture since 2002.

Core competencies include cybersecurity training, exercises, competitions, game development, culture of security initiatives, information sharing and cybersecurity community programs.

UTSA

About the CIAS-ISAO

- An initiative of the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio
- Focus Areas: Outreach & Grassroots Security
  - Cybersecurity Professional Training & Exercises
  - Cyber Competition Programs
  - Cybersecurity Educational Games
  - Culture of Cybersecurity
  - Information Sharing and Analysis Initiatives
  - National Cybersecurity Preparedness Consortium (NCPC)



Membership Resources

- Educational Content
- Quick Access to National Resources
- Access to Customized Training
- Recorded Webinars
- Discount on Cybersecurity Prep Courses & Workshops
- Roadmap to Establishing an ISAO
- Assessments
- Your CIAS-ISAO Support Team!

Membership Benefits (Levels 2 & 3)

- **Discount on CIAS Prep Courses**: CISSP, CompTIA A+, CompTIA Security+
- Access to **Customized Training** Resources
- Customized **Consultations**
- **Discount on book** "Establishing Cyber Security Programs Through the Community Cyber Security Maturity Model (CCSMM)"
- **Discount on Panoply**, a virtual cyber defense event
- Personalized **Roadmap** to Establishing an ISAO

Upcoming Events

CIAS-ISAO Webinars:

- Look for new webinars
- Let us know what you need

Instructor-Led (Virtual) Courses:

- $(ISC)^2$ CISSP Exam Preparation: July 30, 2022

Jeff Reich

Senior Information Security Instructor

Actively involved in the security community for 40+ years and holds numerous leadership positions in technology and professional associations. Additionally, Jeff has delivered hundreds of educational sessions and industry presentations, and is currently the vice president of member success at the Cloud Security Alliance.

- Created and led the security and risk functions at Dell, Rackspace, CheckFree and other companies
- Consulted in Business Continuity and Incident Response
- ISSA Distinguished Fellow, ISSA Hall of Fame
- CISSP CRISC and Foundation Certificate in IT Service Management certifications

Abstract and Takeaways

- **Description**
  Incident Response Plans are critical to an organization's ability to minimize damage caused by threats, including data loss, abuse of resources and loss of trust. Many laws, regulations or cyber-insurance providers require organizations to implement and exercise Incident Response Plans. A well-designed plan ensures a prepared approach to mitigate impacts on your organization's critical business services.

  This webinar focuses on an organizations' initial activities when building or updating their Incident Response Plan. In addition, the presentation will discuss challenges, outsourcing, and when you should escalate and to whom.

- **After this webinar, you will be able to**
  - Specify the most important questions to ask and answer for your organization
  - Identify who should be engaged in Incident Response and when
  - Recognize common pitfalls in Incident Response planning
  - Get your organization’s incident response planning underway

Agenda

- Security Framework
- Incident Response Plans
  - What
  - Why
  - How
- Incident Response Lifecycle
  - Preparation
  - Detection and Analysis
  - Containment, Eradication & Recovery
  - Post-Incident Activity
- Maintaining Your Plan

Five Step Security Framework

https://www.nist.gov/blogs/manufacturing-innovation-blog/dealing-cyber-attacks-steps-you-need-know

Incident Response Plans

Incident Response Plans are fundamental to an organization's ability to respond to potentially devastating security events.

A well-designed plan ensures a prepared approach to mitigate impacts on your organization's critical business services.

Incident Response Introduction

According to the National Institute of Standards and Technology (NIST), Incident Response is the same as Incident Handling*

1. The mitigation of violations of security policies and recommended practices
2. An adverse event becomes an incident
3. An IT security incident is an adverse event in a computer system or network caused by the failure of a security mechanism or an attempted or threatened breach of these mechanisms

According to Jeff

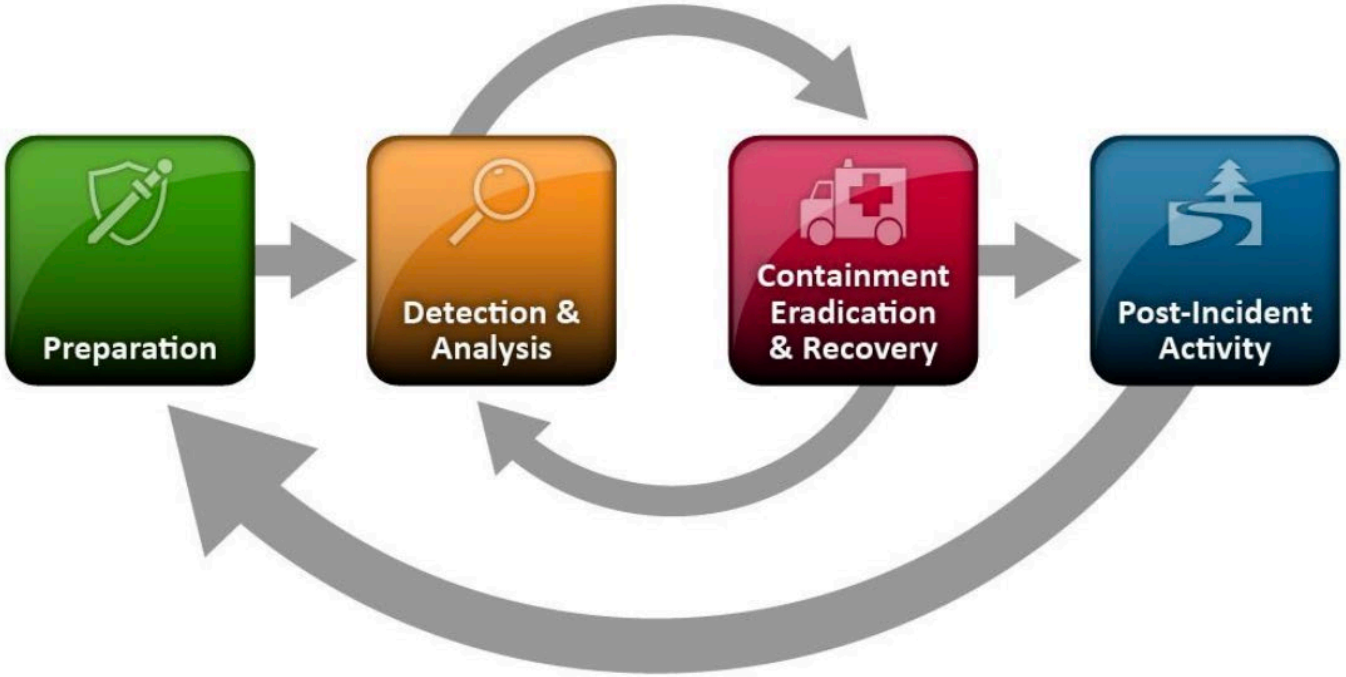
- It's not working the way you want and it's not good

* https://csrc.nist.gov/glossary/term/incident_handling

Why Do We Need Incident Response?

- Attacks frequently compromise personal and business data
- Supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken
- Ability to use information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data
- Helps with dealing properly with legal issues that may arise during incidents

Incident Response Life Cycle



Computer Security Incident Handling Guide

Respond By Not Needing To Respond

- Incident Response means different things to different people
- For Jeff, it means: “How well did you prepare?”
- Your response is directly related to your preparation

The Best Preparation:

Prevention!

Identify

- No matter how difficult it may seem to quantify every asset in your organization, it is always easier to do *before* you have to respond to an incident

- What is your most important asset?

Identify More

- Deal with what's already broken
- Known and repeated failures
- Find single points of failure
- Expect that every piece of hardware will fail
- Every software program or application will fail
- Every individual will be unavailable at some point

Identify Who

- More people than expected will be involved in your plan

- Security
- Operations
- Corporate Communications
- Legal

- Executive Management
- Vendors, Third Parties
- Every person that might see the effect of an incident

Preparation *(partial list, yours will be longer)*

- Know your assets
  - Where, value, owner, etc.
- Contact information
  - Who to contact: leadership, staff, vendors, etc.
  - How to find each person
- Incident reporting mechanisms
  - Are they still available?
- Issue tracking system
  - Even a spreadsheet helps
- War room
  - Information hub, decision making
- Secure storage facility
  - Maintain evidence

TEST YOUR PLAN!!

Failing to prepare is preparing to fail.

John Wooden

Prepare for What?

- Plan for the outcome, not the cause
- According to the Cybersecurity and Infrastructure Security Agency (CISA), today's risk landscape includes:
  - Insider Threats
  - Acts of Terrorism
  - Cyber Attacks
  - Extreme Weather
  - Pandemics
  - Accidents or Technical Failures
- Continue building your plan for outcomes that are related to your most important assets. You could use some CISA Cybersecurity Incident & Vulnerability Response Playbooks as templates*.
  Note: Not every scenario will apply to you.

*https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Let's Talk About Testing

"No plan survives first contact." - Helmuth von Moltke

Test Type	Investment/Risk
Read Through	Minimal time/may miss key scenarios
Tabletop	Measurable portion of a day, or more/easy to digress into non-relevant discussions
Parallel Test	Run systems and processes to test in parallel environment/May be expensive
Full-Failure Test	Full interruption of operations/Expensive

- CISA provides some Table Top Exercises at https://www.cisa.gov/cisa-tabletop-exercises-packages.
- After each test, always find what does not work and revise the plan accordingly. Repeat your tests regularly. The more your processes change and evolve, the more you need to test.

Building an Incident Response Plan

What do you do when the incident happens?

Detection and Analysis

Use available detection tools

- Eyes, ears, people, cameras, intrusion detection, etc.

Signs of an incident

- Missing property, systems unavailable, people unavailable, unexplainable activity

Determine what is different from your standard baseline or profile

- What is the impact?

Seek assistance

- Don’t wait
- Don’t wait

Containment, Eradication and Recovery

- Containment
  - Stop the bleeding
- Gather evidence
  - Identify the last known source
- Maintain evidence
- Eradication
  - Determine the source
  - Remove the cause
- Restore normalcy
  - Test systems
    - Relock the doors, apply backups, invoke Disaster Recovery or Business Continuity plans
  - Monitor to ensure recovery

Post-Incident Activity

- Conduct retrospective
  - Exactly what happened and at what times?
  - How well did staff and management perform in dealing with the incident?
    - Were the documented procedures followed? Were they adequate?
  - What information was needed sooner?
- Summarize recommendations
  - Were any steps or actions taken that might have inhibited the recovery?
  - What would the staff and management do differently the next time a similar incident occurs?
  - How could information sharing with other organizations have been improved?

Post-Incident Activity

- Remediation action plan
  - What corrective actions can prevent similar incidents in the future?
  - What precursors or indicators should be watched for in the future to detect similar incidents?
- Finalize incident report

Let's Bring It Home

- **After an incident, when you do not know what caused it, you will suffer it again**
- Always:
  - Preparation
  - Detection and Analysis
  - Containment, Eradication, and Recovery
  - Post-Incident Activities

- **Root Cause Analysis (RCA)**
  - Pareto Chart
  - Fishbone Diagram
  - FIve Whys
- Not the exhaustive list, just some popular ones. Once you have a defined root cause, implement mitigation or avoidance and avoid a repeat incident

Some Additional Takeaways

- NIST Computer Security Incident Handling Guide
  - Great way to look at what you need to accomplish
- CISA Cybersecurity Incident & Vulnerability Response Playbooks
  - Good templates, regardless of your vertical, to use to create your plans
- Executive Order on Improving the Nation's Cybersecurity

Thank you!

In addition to today's webinar, we can help you with:

- Training & Exercises
- Implementing a Culture of Cybersecurity & K-12 Educational Cybersecurity Program
- Customized Cybersecurity Competitions
- Assessments
- Access to Educational Content
- ISAO Support for Communities
- Establishing and Growing a Program (CCSMM)

Thank you!

Jeff Reich
Senior Information Security Instructor
Jeffrey.Reich@utsa.edu

Julina Macy
Director of Communications
Julina.Macy@utsa.edu

CIASISAO.org