



**Cybersecurity
Incident Response:
BEFORE,
DURING
AND AFTER**



Table of Contents

Overview	3
Before	4
• Security Incident Defined	
• Why create an Incident Response Plan?	
• Who's in a Computer Incident Response Team	
• Data Classification	
• Training & Testing	
During	7
• Incident Response Lifecycle	
• Detection and Analysis: "The Boom"	
After	10
• External Resources, Lessons Learned	
Conclusion	12
About ECI	13

What is a Cybersecurity Incident? An Overview

When a cybersecurity incident occurs, it is crucial to act fast to minimize the exposure of sensitive information and mitigate any risk to your firm. That said, being able to act swiftly requires you to have an Incident Response Plan in place before a cyber incident occurs.

Incident response methodologies typically emphasize preparation—not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure.

What is a Cybersecurity Incident?

- A **cybersecurity event** is any observable occurrence in a system or network. Examples of cybersecurity events include unauthorized users connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Examples: router ACLs were updated, firewall policy was pushed
- **Incident** – A security event that compromises the integrity, confidentiality or availability of an information asset. Examples: attacker posts company credentials online, attacker steals customer credit card database, worm spreads through network
- **Breach** – An incident that results in the confirmed disclosure – not just potential exposure – of data to an unauthorized party

You can't stop every cyberattack. However, your key stakeholders, clients, and other observers do expect you to take reasonable measures to prevent breaches in the first place, and when that fails, to respond quickly and appropriately. An effective incident response program is essential to protect your firm from potential financial and reputational loss, and this eBook will walk you through developing your plan.

Before: Create an Incident Response Team

We know there's always the potential for a cybersecurity incident, so when this incident occurs, you'll want to have the appropriate team in place ahead of time to be prepared to respond in the appropriate manner. A CIRT, or a Cybersecurity Incident Response Team, is a specialized group to respond to these incidents. At its core, the CIRT is a cross functional team of internal and external experts who are responsible for remediating. This team is responsible for alerting regulatory agencies and implementing policies and procedures around incident response, ensuring situations are handled with best practices.

All employees in your firm have a role in incident response, starting with reporting any suspicious activities. Firms should consider bringing in outside help from external vendors and partners to support in-house resources if necessary.



All employees

Do they know how and when to report an incident? Make IT part of the security awareness.



External investigators

Who will you hire in each potential situation? How quickly will they respond? How much will it cost?



IT staff

Find out who owns and manages each system. Who has forensics skills? Who has database administrator access?



External breach notification providers

How will they alert your customers to an incident? What compliance regulators are in place?



Incident response team

Requires communicator, systems expert, and network expert at a minimum. Larger teams often include: physical security, forensics, risk management and legal.



Corporate communications

Who is responsible for conveying relevant messages to employees, partners, or customers? Who will craft and approve that message to ensure that it is correct?



Lines of business

Help identify important business assets and drive process improvements.



Legal representatives

Who do you contact when the investigations show signs of criminal activities?

Before: Data Classification & Protection

If you don't know what proprietary or sensitive information and data you have to protect and where it's located, you won't be able to properly protect it. All firms need to protect:

Personally Identifiable Information (PII)

According to the U.S. General Services Administration – PII is information that can be used to identify an individual's identity, either when the information is alone or combined with other identifying information that is linkable to an individual.

Protected Health Information (PHI)

The HIPPA Privacy Rule defines Protected Health Information as demographic information, medical history, test and laboratory results, insurance information and other data that healthcare organizations and professionals store and have access to.

Non-Public Information (NPI)

The Federal Trade Commission defines NPI as any personally identifiable financial information.

The first two types of data are legally required to be reported to the Security Exchange Commission if there is a breach. When creating your asset inventory, an organization should cover:

- Where the information resides;
- Who has access to the information;
- How the data is stored, removed or transferred; and
- How the data is protected.

Before: Training and Testing

Although this may seem obvious, training and testing is critical in the development of your incident response plan:

- ✓ Train employees on their roles and responsibilities during an incident response. Taking time to train on a biannual or annual basis ensures that your employees are able to act swiftly and follow prescriptive steps and work as a team to achieve your singular goal: remediating and recovering from your cybersecurity incident.
- ✓ Develop response and recovery plans based on scenario specific events. Make sure your team knows exactly how to respond for specific events, not generalized scenarios.
- ✓ Walk through and simulate incident procedures. When employees have been through simulated incidents, they're able to replicate those efforts if and when an incident occurs in real life.

During: Detection

When a cybersecurity incident occurs, identification can come from various sources:

- Infrastructure alerts
- Logs
- Vendors/Partners
- Public Information or Subscription Services or
- Employees
- **SIEM (Security Information and Event Management) Analysis**
 - SIEM provides real-time analysis of security alerts generated by applications and network hardware
 - Analyze the SIEM logs, which allows for immediate lock-down of any potentially vulnerable areas or confirming there was no exfiltration of files or data

PRO TIP:

Having a Security Information and Event Management (SIEM) Tool has become an invaluable tool for managing cyber incident alerts. As the amount of security related data available has grown, it's become too massive for humans or dispersed systems to decipher which threats are significant.

SIEM provides real-time security analysis of data to proactively identify potential security risks – and can stop cyber threats in their tracks.

On top of fulfilling numerous security regulations, SIEM is a critical piece of any firm's incident response and security strategy.

During: Analysis

When alerted of a security incident, the first step is to escalate to the organization's Cybersecurity Incident Response Team.

Once the Cybersecurity Incident Response Team has been notified, they should take immediate response, including:

- Perform a full anti-malware sweep of the organization's corporate infrastructure
- Retrieve all logs associated with the compromised account using the Security Information and Event Management (SIEM) tool
- Using this information, the CIRT should evaluate the information to determine if there was a cybersecurity incident or breach

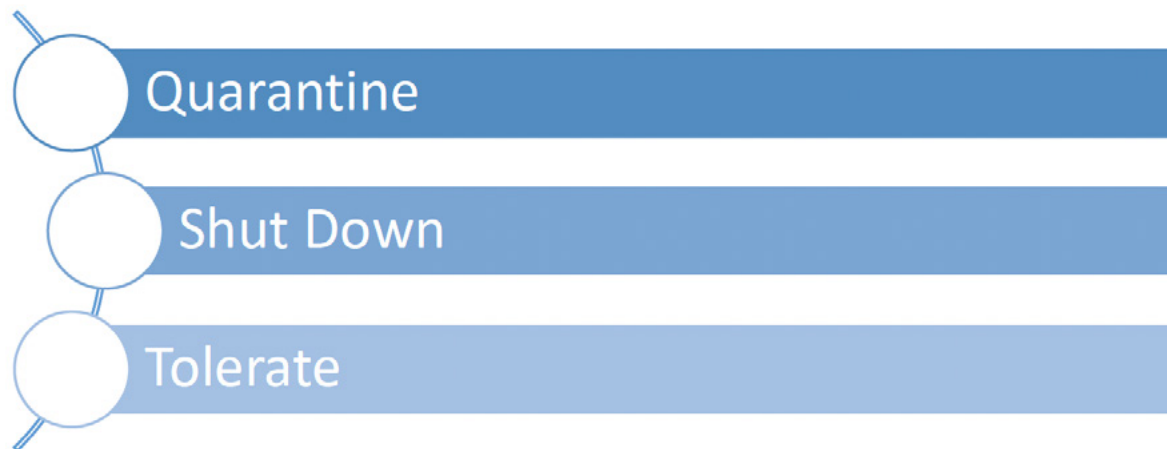
The CIRT should also:

- Call in assistance when needed
- Communicate appropriately internally and externally with consistent messaging



During: Detainment, Eradication & Recovery

In the event of an incident, the CIRT has three options:



Next Steps Include:

Eradiation: Gather evidence while removing the threat from the system, whether that means patching the system, restoring file systems, removing malware, performing a complete rebuild. Make sure there's no additional problems, so it can be removed.

Recovery: This is the time to restore systems and assets based on your firm's business priorities and needs.

After: Post Incident Activity

There are times where it is critical to bring in external teams after the incident. Digital Forensics Incident Response Teams (DFIR): If you plan to have insurance involved to assist with the potential costs caused by the incident, firms will work with a forensics team to prove they did everything you could. If there's regulatory impact, you'll want a forensics report to show that the firm used best practices and adhered to the incident response plan throughout the event.

In case of legal action taken against your firm, be sure to consult with legal counsel.

Post-Mortem Report: After an incident, the CIRT should take a post-mortem report, or, document findings from the incident with additional feedback in case of another breach own the line. After, incorporate lessons learned into the Incident Response Plan for incident preparation and planning moving forward.



WISP, DR, BCP, Incident Response – How do they all work together?

Written Information Security Plan

Documentation of a firm's plan and systems put in place to protect personal information and sensitive company data. This data can include anything from investor information and data to employees' personal information.

Disaster Recovery Plan

A documented process to recover your firm's IT infrastructure in the event of a disaster, whether that be a natural disaster, a ransomware attack, or other scenarios

Business Continuity Plan

A document that illustrates how your firm will respond when confronted with unexpected business disruptions, such as weather, downtime of critical software or applications or even natural disasters.

How do these plans work together?

These types of plans all work together to protect your firm's data, IT infrastructure, and reputation. Incident Response Planning is a critical step within a Written Information Security, Disaster Recovery, and Business Continuity Planning. Depending on the incident, firms will likely look at all these together.



Conclusion

The most important thing to remember is that the first step in developing an Incident Response Plan is making the decision to develop and implement a formal plan.

- ✓ Assemble the proper team and begin developing the incident response plan.
- ✓ Promote internal awareness by testing and training employees to expedite the process if and when an incident occurs.
- ✓ Weigh the metrics that matter when considering an approach to incident response.

For more information on **Incident Response Planning, Managed XDR**, or to talk to one of our Cybersecurity Consultants, contact us at: eci.com/contact

About ECI

ECI is the leading provider of cloud services, cybersecurity, and digital transformation for alternative investment services organizations across the globe. With its unmatched platform of solutions, ECI provides assured business acceleration through technology, partnering with clients to drive innovation. More than 1,000 customers worldwide with over \$3 trillion of assets under management put their trust in ECI.

MAXIMIZE THE EFFECTIVENESS OF YOUR SECURITY



Identification

GAIN CLEAR VISIBILITY INTO KEY ASSET TRACKING AND INVENTORY MANAGEMENT INFORMATION



PROTECTION

PREVENT USER CREDENTIALS FROM BEING COMPROMISED AND STOP TARGETED ACCOUNT TAKEOVERS



Detection

SEARCH AND ANALYTICS TECHNOLOGY COMBINES THREAT INTELLIGENCE WITH HUMAN CYBERSECURITY THREAT HUNTERS



Response

24X7X365 MONITORING AND SUPPORT TEAMS TRAINED TO TAKE APPROPRIATE ACTION ON ALL ALERTS



Recovery

HANDS-ON TRAINING FOR INCIDENT RESPONSE AND REFINING YOUR RESPONSE STRATEGIES

[**www.eci.com/cyber-solutions**](https://www.eci.com/cyber-solutions)



Boston | Chicago | Dallas | Hong Kong | London | Los Angeles | Minneapolis | New York | San Francisco | Singapore | Stamford