Navigating Ransomware

Cyber & Analytics Unit Webinar

June 16, 2026

AGENDA

01 Welcome and Overview

02 Ransomware Fundamentals

03 Incident Response (Risks & Effective Practices)

04 Key Takeaways

05 Audience Questions

06 Feedback & Resources

FINRA Forward: Cyber Engagements

Strengthen Cyber Readiness

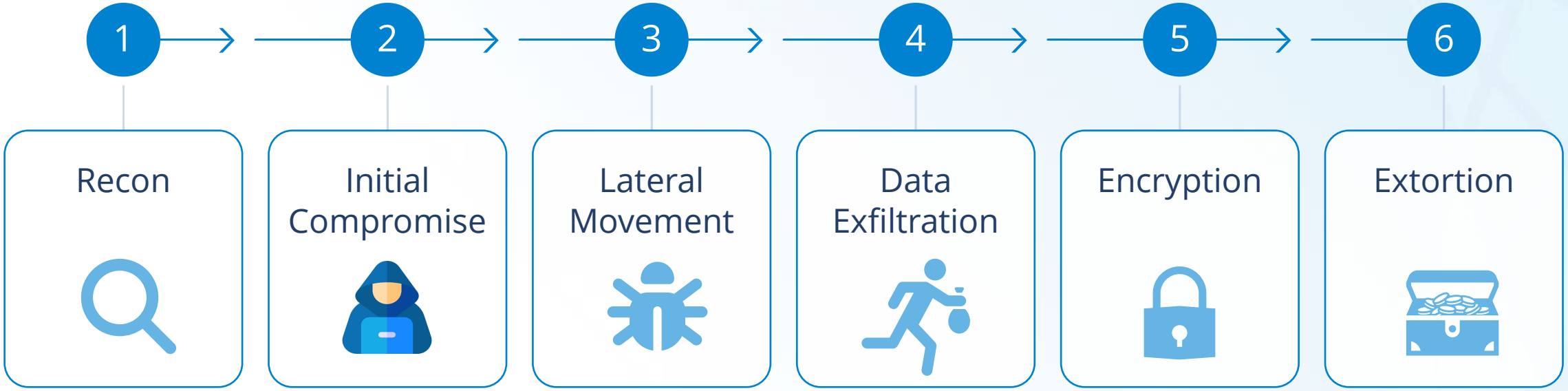
Reinforce Internal Controls

Safeguard Customer Data

Maintain Resilience

What is Ransomware?

Ransomware is malicious software (malware) that encrypts files, systems, or networks and demands payment to restore access.



Ransomware Evolution

FINRA

Initial Attacks

- Basic compromises and limited reach and scope

Age of Cryptocurrency

- Ease of payment provides acceleration

Targeting Businesses Instead of Individuals

- More lucrative targets

Ransomware-as-a-Service

- Anyone can be a potential threat actor

Age of AI

- Highly automated and adaptable-targeting via social engineering

How are Threat Actors Using Generative AI

FINRA

Phishing emails

Researching company organization models

Automating and accelerating attacks

Optimizing extortion efforts

Ransomware Attack Vectors

FINRA

Social Engineering

Attackers trick users into taking actions that grant attacker access

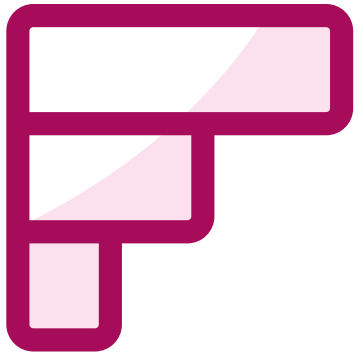
Remote Access

Compromised VPN/RDP credentials allow remote access to the network

Vulnerability Exploitation

Vulnerabilities in internet facing systems allow attackers to bypass authentication, run commands, extract credentials

Defense in depth is key



Which of the following social engineering techniques are you aware of, or have you experienced?

Social Engineering Ransomware Attack Vectors

FINRA

Phishing

Smishing & Quishing

Vishing

Helpdesk Fraud

ClickFIX Fraud

Ransomware Extortion Schemes

FINRA

1x

SINGLE EXTORTION

- Files are locked and inaccessible
- Payment requested for the encryption key

🎯 **Target: System Availability**

2x

DOUBLE EXTORTION

- Files are locked, sensitive data stolen
- Demand payment to prevent data leakage

🎯 **Dual Threat: System Availability & Data Theft**

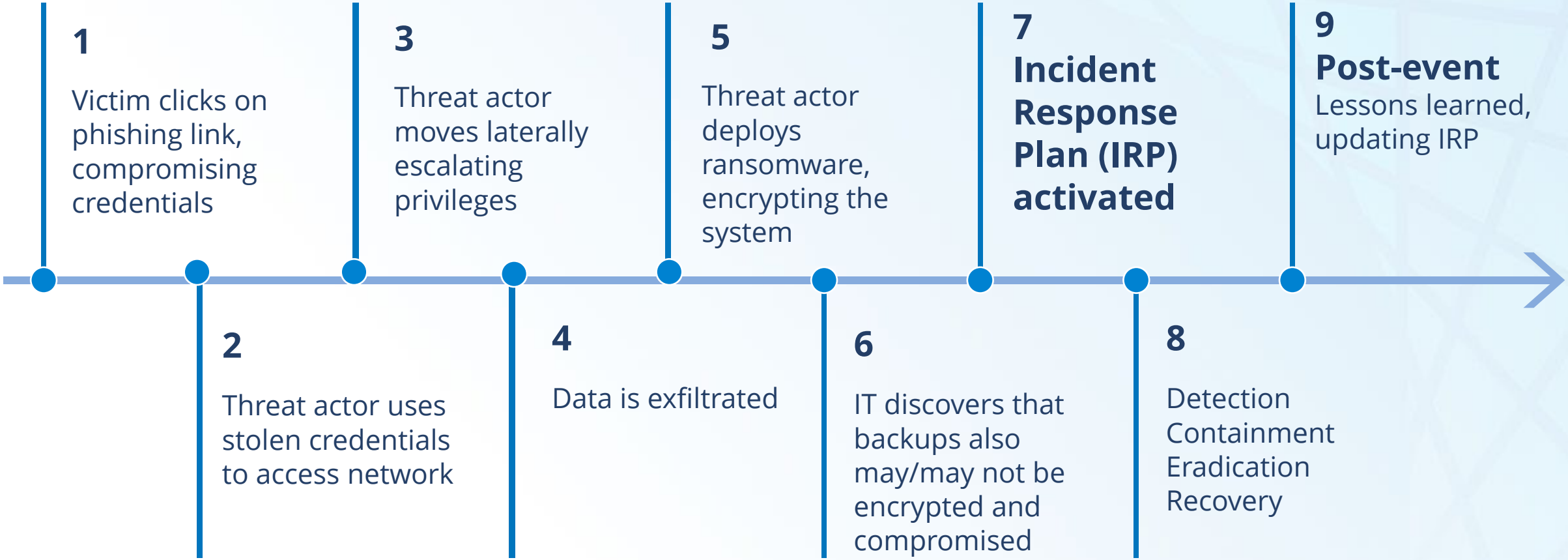
3x

TRIPLE EXTORTION

- Encryption, data leaks, DDoS attacks, notifying third parties

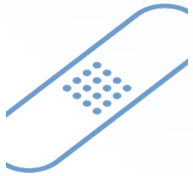
🎯 **Triple Threat: System Availability Data Theft & Third Parties**

Case Study: Ransomware Incident



Effective Practices to Prevent Ransomware

FINRA



1. Vulnerability patching

2. Multifactor authentication (MFA)

3. Security awareness training

4. Endpoint and managed detection and response (EDR & MDR)

5. Zero trust implementation

6. Immutable backups

7. Regular testing of Incident Response Plan

8. Key Partners

FBI, Regulators and Partners

- The FBI may be able to provide:
  - Threat intelligence about the attacker
  - Decryption keys for certain ransomware variants
- Law enforcement may be able to seize the data stolen from your firm

- Potential recovery of ransom payments to threat actors
- Information you provide to law enforcement can help thwart threat actors, and lead to the prosecution of the criminals

Find your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices
Report ransomware incidents to FBI via www.ic3.gov

NIST CSF 2.0 Incident Response Lifecycle

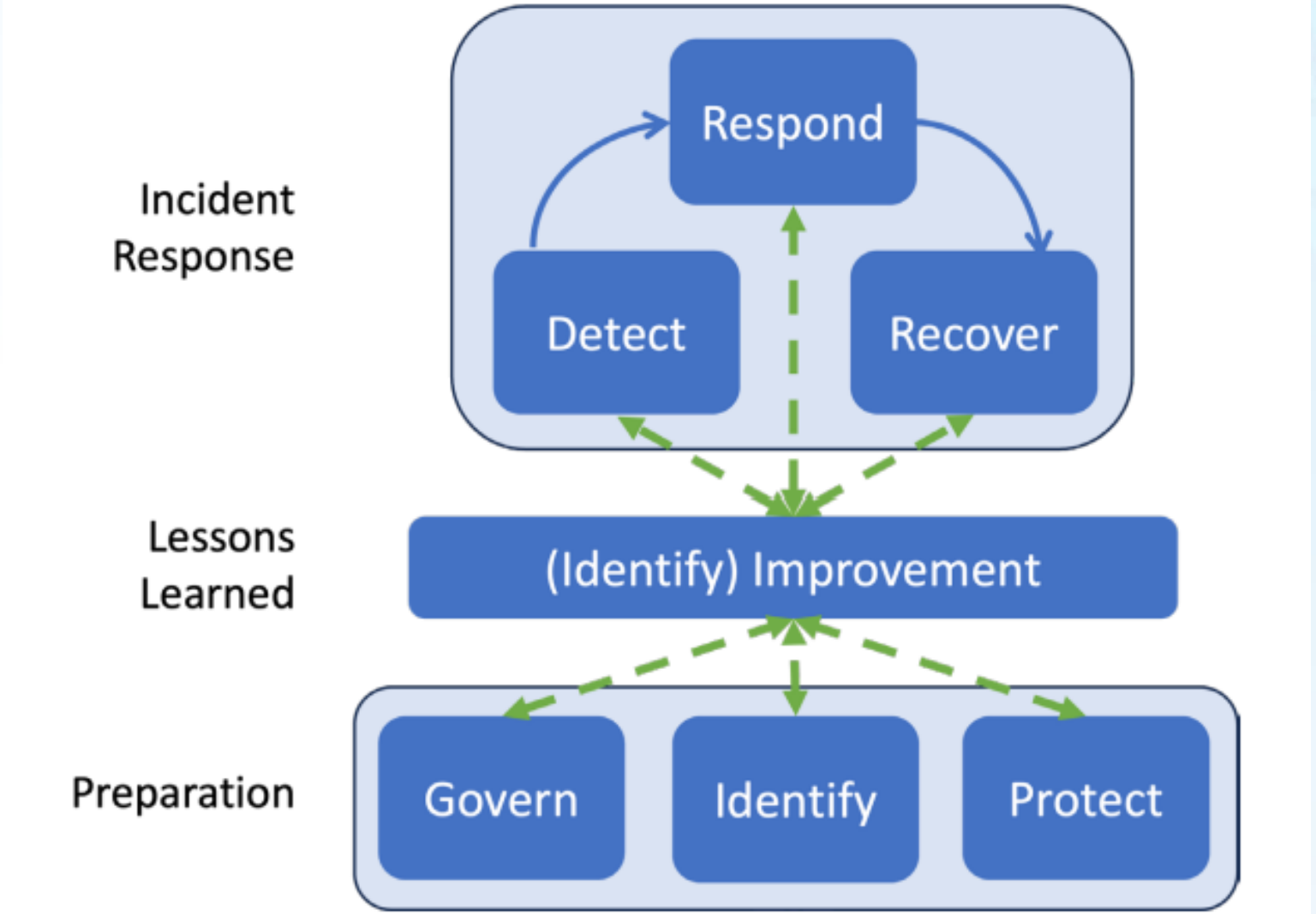
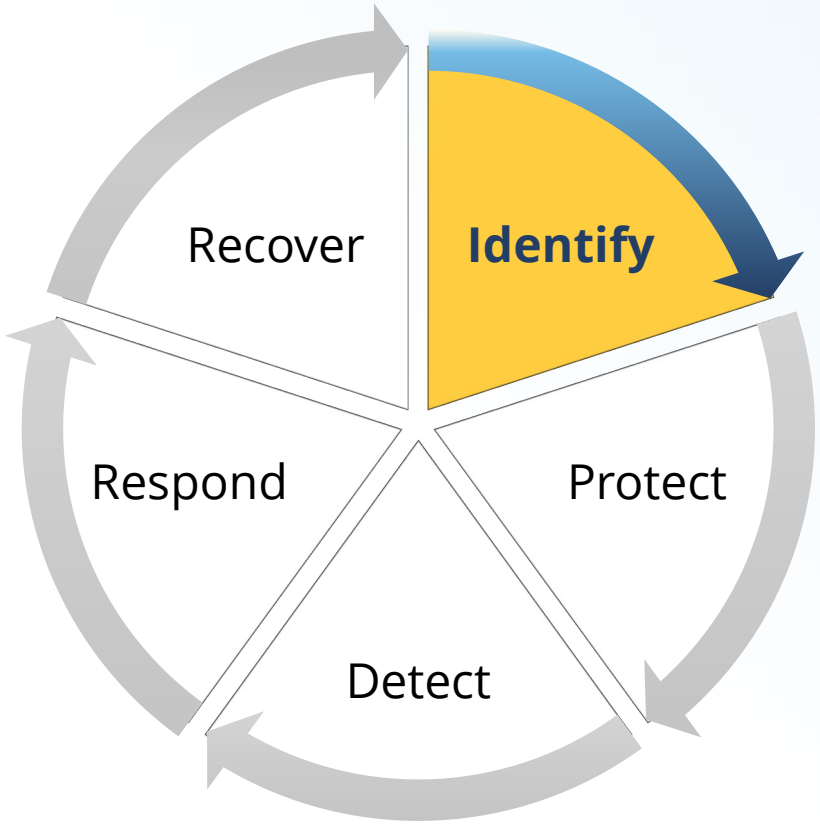


Fig. 2. Incident response life cycle model based on CSF 2.0 Functions

Incident Response - Identify

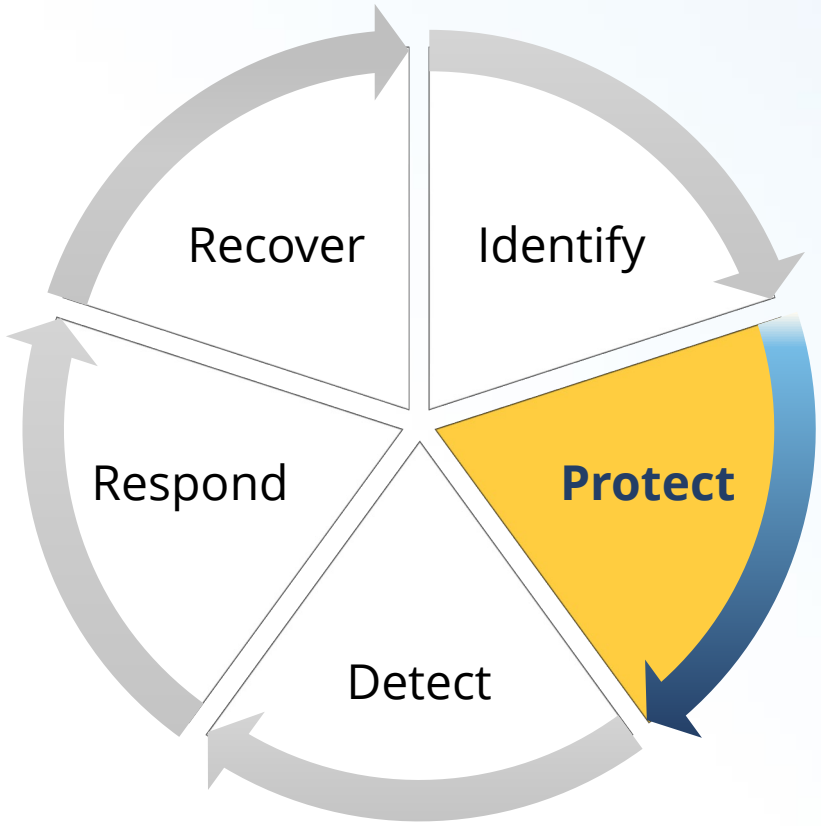


The time to prepare for ransomware is before it occurs: Identifying assets, connections, and processes saves critical time

- **Maintain hardware and software inventories**
- **Document information flows**
- **Identify the external system connections**
- **Identify critical enterprise processes and assets**
- **Establish cybersecurity policies that spell out roles and responsibilities**

Is it useful to have documented incident response capabilities?

Incident Response - Protect



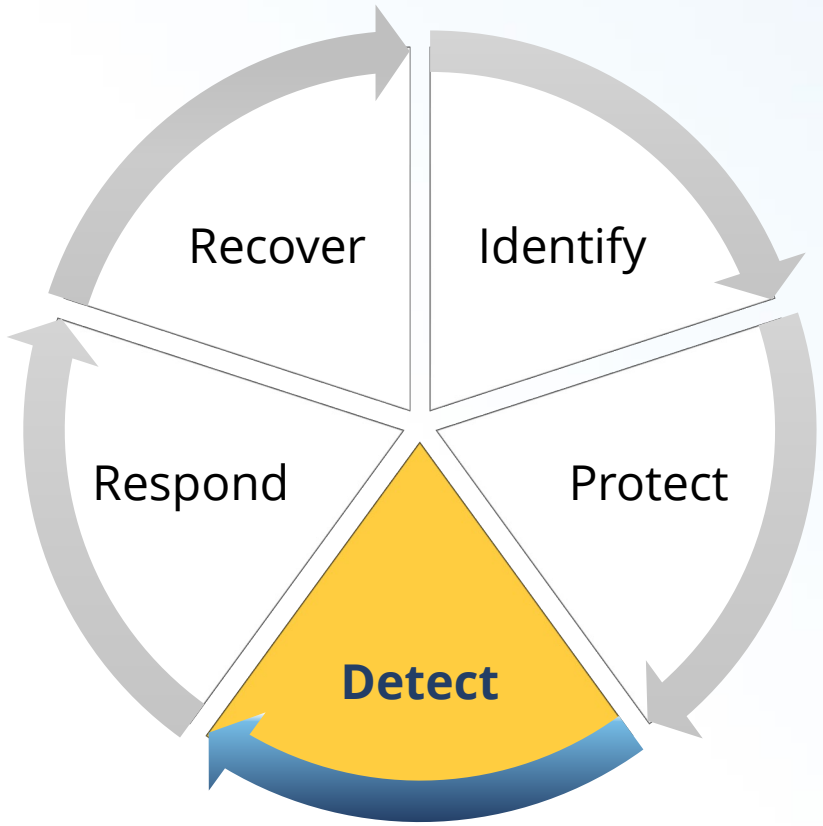
Pre-defined isolation criteria help contain ransomware while minimizing disruption

- **Manage access to assets and information**
- **Manage device vulnerabilities**
- **Educate and train workforce**
- **Secure all devices**
- **Protect sensitive data**
- **Conduct regular backups**

Role of Zero Trust in Ransomware Defense

- ✓ **Device health verification**
- ✓ **Network segmentation**
- ✓ **Least privileged access**
- ✓ **Continuous identity checks**

Incident Response - Detect

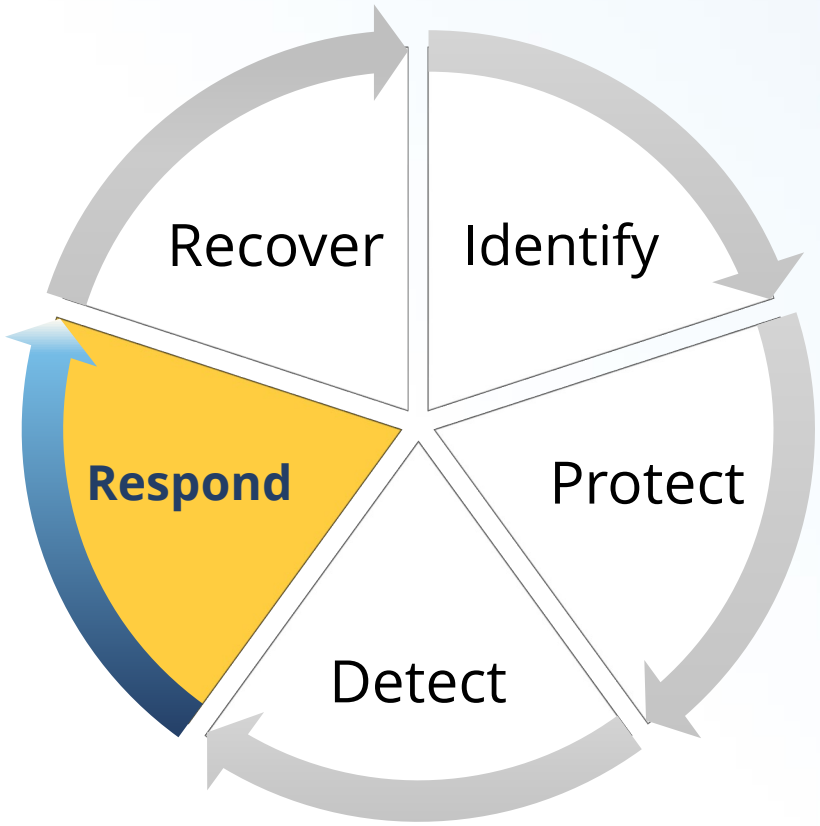


Rapid incident assessment requires tested detection, trained staff, and mapped data flows

- **Test and update detection processes**
- **Train staff**
- **Map expected data flows**
- **Assess and communicate incidents rapidly**

Is it important to identify outside expertise you may need before experiencing an incident?

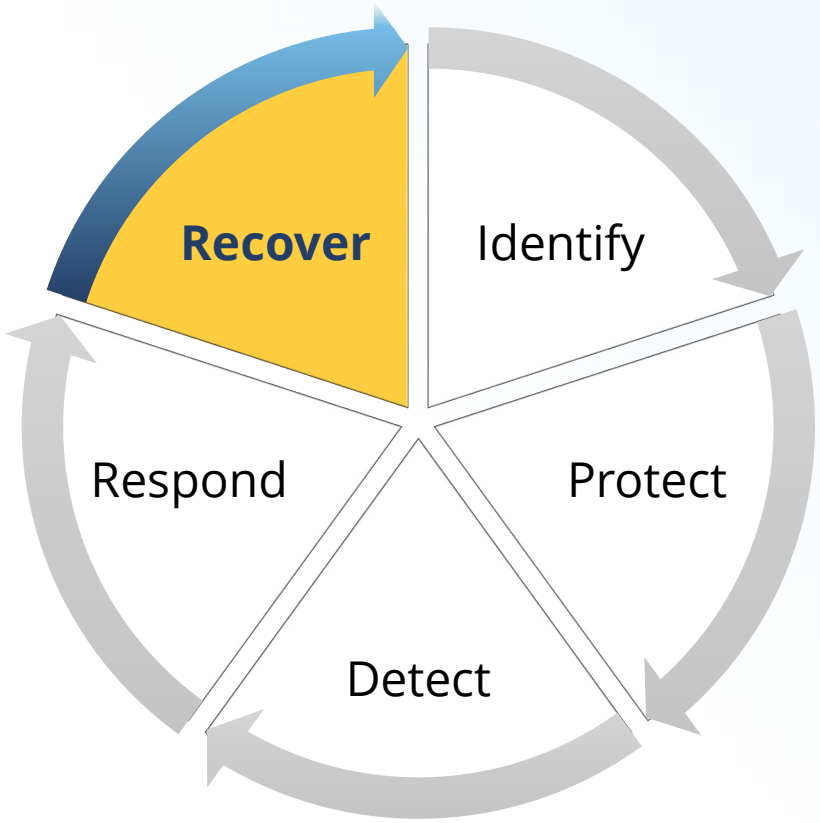
Incident Response - Respond



Pre-identified response vendors enable faster evidence collection and incident containment

- **Develop response plans**
- **Coordinate with stakeholders**
- **Test response plans**
- **Update response plans**

Incident Response - Recover

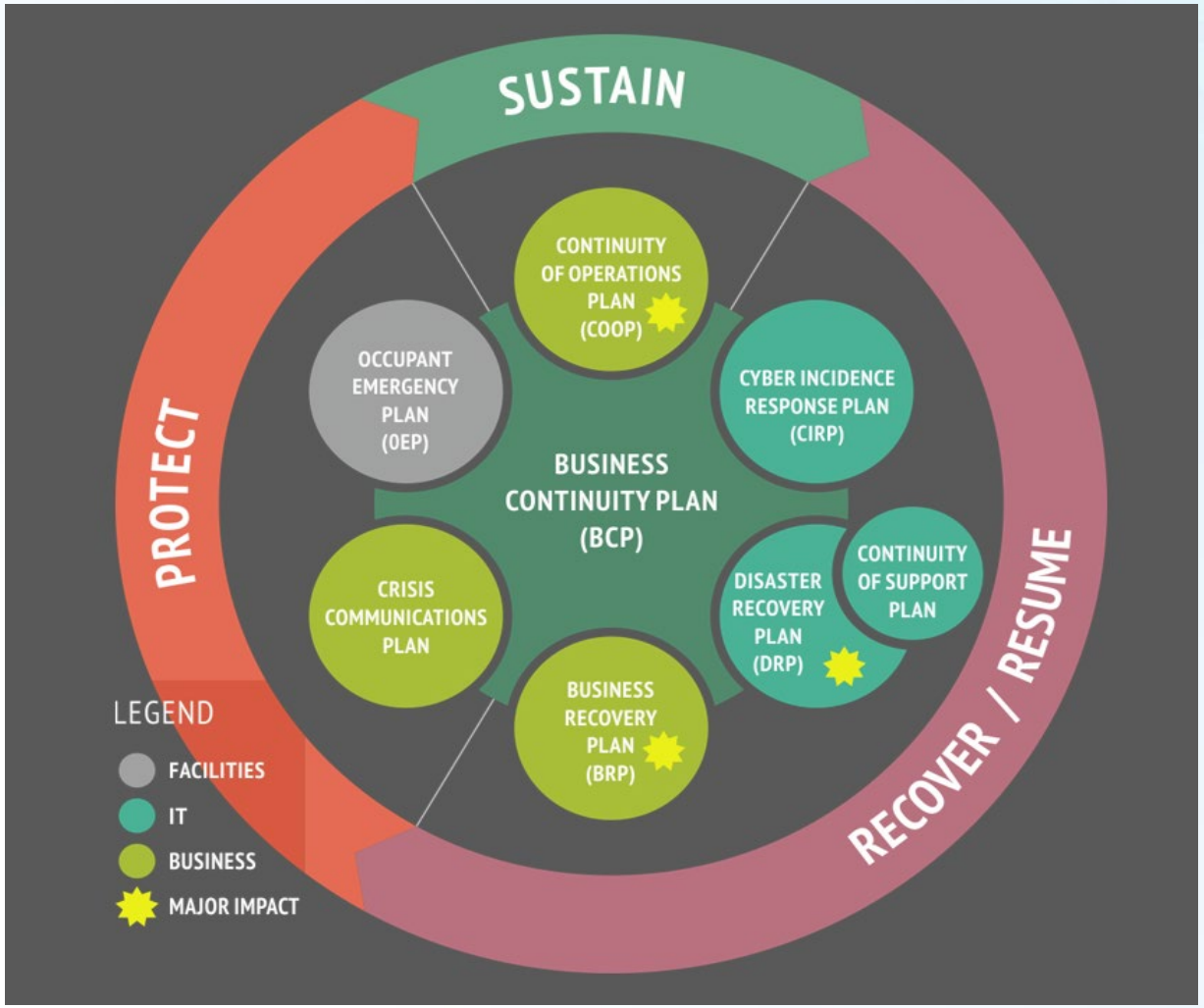


Backup validation is performed in isolated test environments prior to production restoration

- **Develop contingency plans**
- **Communicate with stakeholders**
- **Manage organizational reputation**
- **Test and update recovery plans**

Should Incident Response and Business Continuity Plans be tested together?

The Business Perspective: How It All Works Together



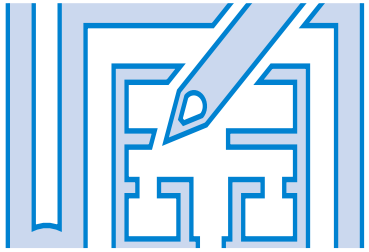
Combating Ransomware

Validate your Incident Response Program

- Verify and develop ransomware-specific procedures

Establish relationships

- Contact your local FBI office for assistance



Business continuity

- Test your BCP
- Operational resilience depends on readiness

Coming Soon

Ransomware Decision Simulation
June 30, 2026

- Simulated scenarios
- Incident response training
- Improve problem solving
- Enhance collaboration
- Learn how to mitigate risks

Register at
FINRA.org/events

Survey QR Code

THANK YOU

If you have any follow up questions or comments, please contact the Cyber and Analytics Unit

CAU@finra.org

Linked Resources

Resources Available on FINRA.org

- FINRA Cybersecurity
- FINRA Financial Intelligence Fusion Center (FIFC)
- FINRA Small Firm Checklist
- FINRA Firm Checklist for Compromised Accounts
- Non-FINRA Cybersecurity Resources
- FINRA Risk Monitoring Program

External Resources: Federal Government

- Department of Homeland Security – Ready.gov Testing Exercises
- Cybersecurity and Infrastructure Security Agency (CISA)
- CISA Tabletop Exercise Packages
- Internet Crime Complaint Center (IC3)
- Local FBI Field Office

External Resources: NIST

- NIST Cybersecurity Framework
- NIST SP 800-61r2 - Computer Security Incident Handling Guide
- NIST SP 800-30 - Guide for Conducting Risk Assessments
- NIST SP 800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

External Resources: Other

- Center for Internet Security Critical Security Controls (CIS CSC)
- SANS Security Policy & Form Templates
- Backdoors & Breaches, an Incident Response Card Game
- FinCEN Advisory - FIN-2016-A005

Regulatory Considerations

FINRA Rules to Consider

- **FINRA Rule 3110 – Supervision**
  - Each member shall establish and maintain a system to supervise the activities of each associated person that is reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules

- **FINRA Rule 2010 – Standard of Commercial Honor and Principles of Trade**
  - A member, in the conduct of its business, shall observe high standards of commercial honor and just and equitable principles of trade

- **FINRA Rule 4530 – Reporting Requirements**
  - Requires firms to report specified events
    - Quarterly statistical and summary information regarding written customer complaints
    - Copies of specified criminal and civil actions

SEC Rules to Consider

- SEC Reg S-P
  - Requires registered broker-dealers, investment companies, and investment advisers to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information“
- SEC Reg S-ID
  - The rule requires institutions to develop and implement a written identity theft prevention program designed to detect, prevent, and mitigate identity theft in connection with certain existing accounts or the opening of new accounts
- SEC Reg SCI
  - Reduce the occurrence of systems issues
  - Improve resiliency when systems problems do occur
  - Enhance the Commission's oversight and enforcement of securities market technology infrastructure