Incident Management

RAY MURPHY

Ray Murphy

- Extensive information security and information technology experience

Public Company Accounting Oversight Board (PCAOB)
Chief Information Security Officer

Navy Federal Credit Union
Chief Information Security Officer
Vice President Fraud Management

LEO Cyber Security
CISO Advisor for small credit unions

Mobil Oil Corporation
All aspects of information technology

Incident Management Program

- Objectives of a Program:

  Recover quickly from an incident

  Protect the company's interests and assets

  Communicate with shareholders, employees third party providers, and regulatory agencies

Incident Management Program

- Documented program
- Defined roles and responsibilities
- Practice the entire program periodically
- Communication is the key, internally and externally

Detection and Prevention

- Although you must have a documented incident management program, the best way to avoid activating the program is through sound detection and prevention.
- Basic, fundamental cyber hygiene is the best way to prevent potential incidents.
- Key element is to know where the company assets are stored and who has access to these assets at all times.

NIST Cybersecurity Framework

Components of the Framework:

Identify

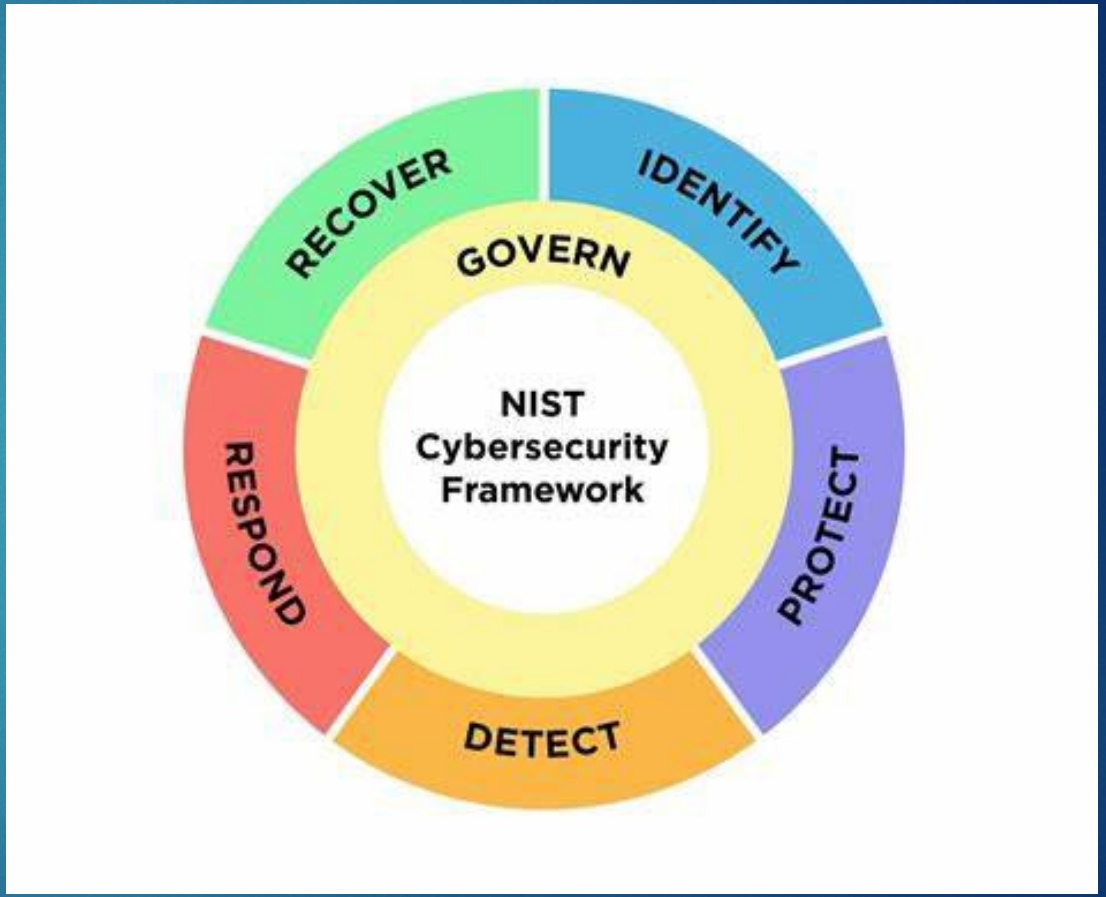
Protect

Detect

Respond

Recover

Govern



Incident Management Team

- Define who is on the team and clearly identity who the Team Chair is when an incident is identified
- This executive level team is convened once an incident has been declared
- The Chair of the team usually the CISO is responsible for all communications that are issued for the incident from the team
- This team will decide when certain activities will be initiated

Incident Response Team

- Combination of IT and Info Sec personnel who will provide the details and artifacts of the incident

  The Incident Manager leads this team and in consultation with the Incident Management Team Chair will determine the level of the incident

Incident Response Team

- identify a repository for all incident artifacts and documentation, i.e. Microsoft Teams

  Detailed playbooks should be created and updated as needed for various common incident scenarios:

  - Denial of Service Attack
  - Phishing Incident
  - Ransomware Incident
  - Insider Threat

Incident Response Team

- Phase of the Program once an incident is declared

  Determine the extent of the incident

  Develop a plan to contain the incident

  Once contained, develop a plan to eradicate the incident

  Once eradicated, restore the organization to full operations

Incident Management Communications

- Internal Communications

  Key component during an incident

  Periodic updates are given in meetings

  Chair and additional C Level executives will be responsible for providing updates to the CEO, COO, and Board as needed during an incident

Incident Management Communications

- External Communications

  Develop communication templates to issue to external sources, i.e., customers, media, etc.

  Identify a media spokesperson who will issue extremal media updates and/or interviews

Additional Services

- Cyber Insurance
  Full incident response team may be available
- Forensic Retainer Service
- For financial institutions, have credit monitoring service plan in place
- Crypto Payment service

Test The Program

- Important to test all aspects of the Program

Incident Response Team

Technical walk through for a specific incident type

Provides an opportunity to review what steps would be taken

Incident Management Team

Walk through an incident and discuss how the team would address the incident

Enterprise-Wide Exercise

Table Top Exercises

- Recommend that you participate in external organization tabletop exercises

  Financial Services Information Sharing and Analysis Center (FS-ISAC)

  US Department of The Treasury

  US Naval War College Critical Infrastructure Cyber War Games

Cyber Incident Examples

- Insider Threat – Departing Employee
  Transmitted proprietary information via email to Gmail account for next job

  Phishing Attempt – IRS Notice
  Email appearing to be from IRS advising recipient of delinquent taxes

  Phishing Attempt – Court Summons
  Email from a local court appearing to be a summons to appear in court

Cyber Incident Examples

- Phishing Attempt – Change Payroll Deposit information for the CEO
  Email sent to HR Payroll team requesting a change in the payroll deposit information for the CEO, email appears to be from the CEO

  Application Code Error – Sent Personally Identifiable Information (PII) to Incorrect recipient
  Application change sent information to incorrect third-party provider for processing

Thank You!

RAY MURPHY