Incident Response

Domain 4.0

The Importance of the Incident Response Process

Chapter 15

Episode 15.02

IR Roles and Responsibilities

Objective: 4.1 Explain the importance of the incident response process.

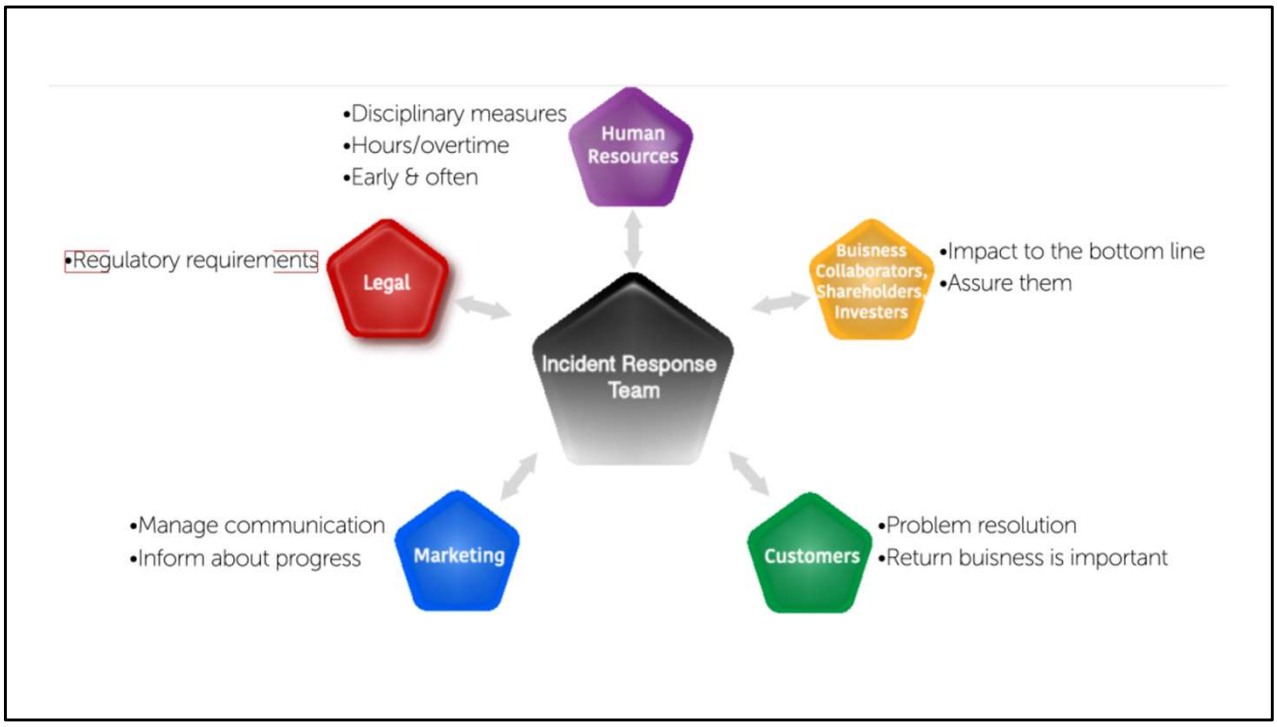
- Communication plan
  - Limiting communication to trusted parties
  - Disclosing based on regulatory/ legislative requirements
  - Preventing inadvertent release of information
  - Using a secure method of communication
  - Reporting requirements
- Response coordination with relevant entities
  - Legal
  - Human resources
  - Public relations
  - Internal and external
  - Law enforcement
  - Senior leadership
  - Regulatory bodies

IR Process Key Roles

- Senior leaders
  - Include in decision-making process
  - Visibility & support
  - Address regulatory issues
  - Buffer between IR team & personnel/leaders

IR Process Key Roles

- Team composition
  - Response based on scope of incident management
  - Bring in the right knowledge & experience to meet the problem
  - Outside resources need coordination & pre-set parameters
- Escalated IR
  - Need strict guidelines, policies, & notification requirements
  - May by subject to penalties or legal ramifications


•Disciplinary measures
•Hours/overtime
•Early & often
Human Resources
•Regulatory requirements
Legal
Buisness Collaborators, Shareholders, Investers
•Impact to the bottom line
•Assure them
Incident Response Team
•Manage communication
•Inform about progress
Marketing
Customers
•Problem resolution
•Return buisness is important

Team Structure

- Central response team
  - Organic
  - Address incidents as they come up
- Distributed response team
  - Larger organizations
  - Geographically separate teams that address incidents
- Outsourced response team
  - Outside the organization
  - Responds to incidents as a service

Communications Process

- Circle of trust
  - Key staff, internal & external partners
- Disclosure
  - Based on regulatory or legislative requirements
  - Need-to-know
- Damage control
  - Let employees know about incident
  - Policy of talking about the incident
- Secure communications
  - Avoid leaks

Responsibilities & Coordination

- Clearly defined
- Understandable
- Portable

Episode 15.02

IR Active Preparation

Objective: 4.1 Explain the importance of the incident response process.

• Factors contributing to data criticality

- Personally identifiable information (PII)
- Personal health information (PHI)
- Sensitive personal information (SPI)
- High value asset
- Financial information
- Intellectual property
- Corporate information

Preparation

- Prevent incidences to begin with
  - People
  - Process
  - Technology
- Network & host hardening
- Patches & updates

Active Security Measures

- Know Your Attack Surface
  - Attack surface analysis
    - Main point: identify key parts of system to test for vulnerabilities
    - Help security team prepare for attacks & protect assets
    - Help developers make better products

Attack Surface Analysis

- Conducted by security architects & pen testers
- Helps to identify:
  - Parts of a system to review & test for vulnerabilities
  - High risk areas that need to be defended
  - When attack surface changes

Detection & Analysis – Know the Signs

- Indicators of compromise
  - Unusual outbound traffic
  - Anomalous admin account activity
  - Geographic irregularities
  - Login irregularities
  - High database read volume
  - HTML response size
  - High requests on the same file
  - Mismatched port application traffic
  - Suspicious registry and system file changes
  - DNS request anomalies

Detection & Analysis

- Prepare your sources
  - SIEM
  - IDS/IPS
  - Alerts & logs

Determining Severity

- Scope of impact
  - Downtime
    - What is the maximum tolerable downtime?
  - Recovery time
    - Time is money
  - Data integrity
    - Tampering or deleting
  - Economic
    - Value & cost
  - Business process criticality

Types of Data

- PHI (Protected Health Information)
- PII (Personally Identifiable Information)
- Corporate secrets & intellectual property
  - Patents
  - Trademarks & copyright
  - Mergers & acquisitions
  - Accounting
  - Trade secrets
- Payment card information

Know Your Threat

- Know vulnerabilities & landscape
  - What type of data?
  - What do systems look like?
  - What are the threat actors?