Cyber Imitation Game

Harshad Mengle

Expectations

- ?? Disruptive Technologies
- Cyber Security
- ??Imitation Game
- ??Incident

Cyber Security

What strangers think I do

What my family thinks I do

What my friends think I do

What Government thinks I do

What I think I do

What actually I do

Team A – Approach to Incident

Alfa TEAM

Scenario 1

The company's web server slows down then stops responding. High network traffic causes you to suspect a Denial of Service attack.
Points to address:

- How will you identify the source of the traffic?
- Should you shutdown the corporate web server?
- How will you stop the traffic?
- How will you prevent it from reoccurring?

Scenario 2

The organization starts receiving complaints about spam originating from its network
The administrator identifies the source as the company's web server

Points to address:

- How would you validate the source of the spam?
- How would you respond to complaints regarding the spam?
- How would you isolate and repair the web server?
- How would you prevent reoccurrence?

Bravo Team

Scenario 3

A new Trojan/worm is released on the Internet - it distributes itself through Email attachments and downloads malicious code from an Internet FTP server. A number of people in your organisation have opened such attachments.
Points to address:

- How do you identify infected systems?
- How could you prevent the malware entering the enterprise before antivirus signatures were updated?
- How would you prevent further spread?

Scenario 4

An employee at your site mentions that his bank account has been cleaned out by hackers in Arendelle. He has been using online banking from his company workstation.
Points to address:

- Could you confirm whether or not his password was stolen?
- How would you report this incident?
- Would you warn other employees?

Approach

Assessing the situation

- what is the business impact of the incident?
- if the affected system(s) are isolated then what is the impact to business?
- how much effort will it take to resolve?
  - this estimate can be re-evaluated later
  - estimate for repair-in-place
  - estimate for offline rebuild from scratch
  - estimate to recover from backups (you do have backups, don't you?)
- is there enough people with enough expertise available?
  - if not, think about calling someone - either additional internal resources, or external providers
- document everything
  - include dates and times, include contact information

Approach

Identifying the people to handle the incident

- An incident team for a small to medium enterprise is almost always two people. One will be the technical lead who will perform the bulk of the remedial work, and the other will be a backup person reporting to management and recording the actions taken. Further people may be involved depending on the size of the organisation, usually in the reporting chain rather than in direct involvement. These may include:
  - the IT manager
  - the CEO/CIO/CTO
  - Media relations
  - Legal
  - Law enforcement
- Always get help if you feel the situation is getting out of hand. For example, in one case an incident involving malware infection dragged on for two weeks before someone was called in to diagnose the problem and resolve it within an hour. Get equipment and software tools if required. For example:
  - new workstations, servers, switches/routers, firewalls
  - IDS tools
  - Anti-virus, Anti-spam tools
- Preparation is the key to saving time here. It is always good to have an incident toolkit ready with software tools on a CD or USB stick.

Approach

Forming a plan for resolution

- Make a plan, not necessarily written, but at least well communicated. Include the following basic steps:
- **1. Contain the problem**
  - Potentially by isolating the affected systems
- **2. Do No Damage**
  - make backups of the affected system(s)
  - decide if preservation of evidence or critical data is required, if so then backups and correct procedures are critical
- **3. Resolve the problem**
  - rebuild systems from scratch?
  - load backup data?
  - re-secure the affected system(s) as soon as possible
- These steps may be reiterated as the resolution process continues. During resolution the following must be continuously performed:
  - record all actions taken, and document as much as practical
  - updated estimated RTO times
  - report to management and other interested parties
- Keep other people in the organisation up to date with expected RTO times and any issues that are outstanding. Discretion needs to be applied here : avoid public dissemination of sensitive information (such as what type of system failed), and be very cautious as to attributing blame.

Approach

Return to Operation

- After the incident has been resolved the systems can be returned to operation, but only after they have been tested and re-secured to prevent any re-occurrence.
- Identify and mitigate all vulnerabilities that were exploited
- After return to operations, monitor the system closely to make sure all systems are restored to normal.
- Report to management and other interested parties that the system has been restored.

Preventing Reoccurrence

- This is by far the most crucial area, unfortunately it is often overlooked. Many problem would not occur if prevention measures had been put in place following the first occurrence.

Approach

Review the Causes

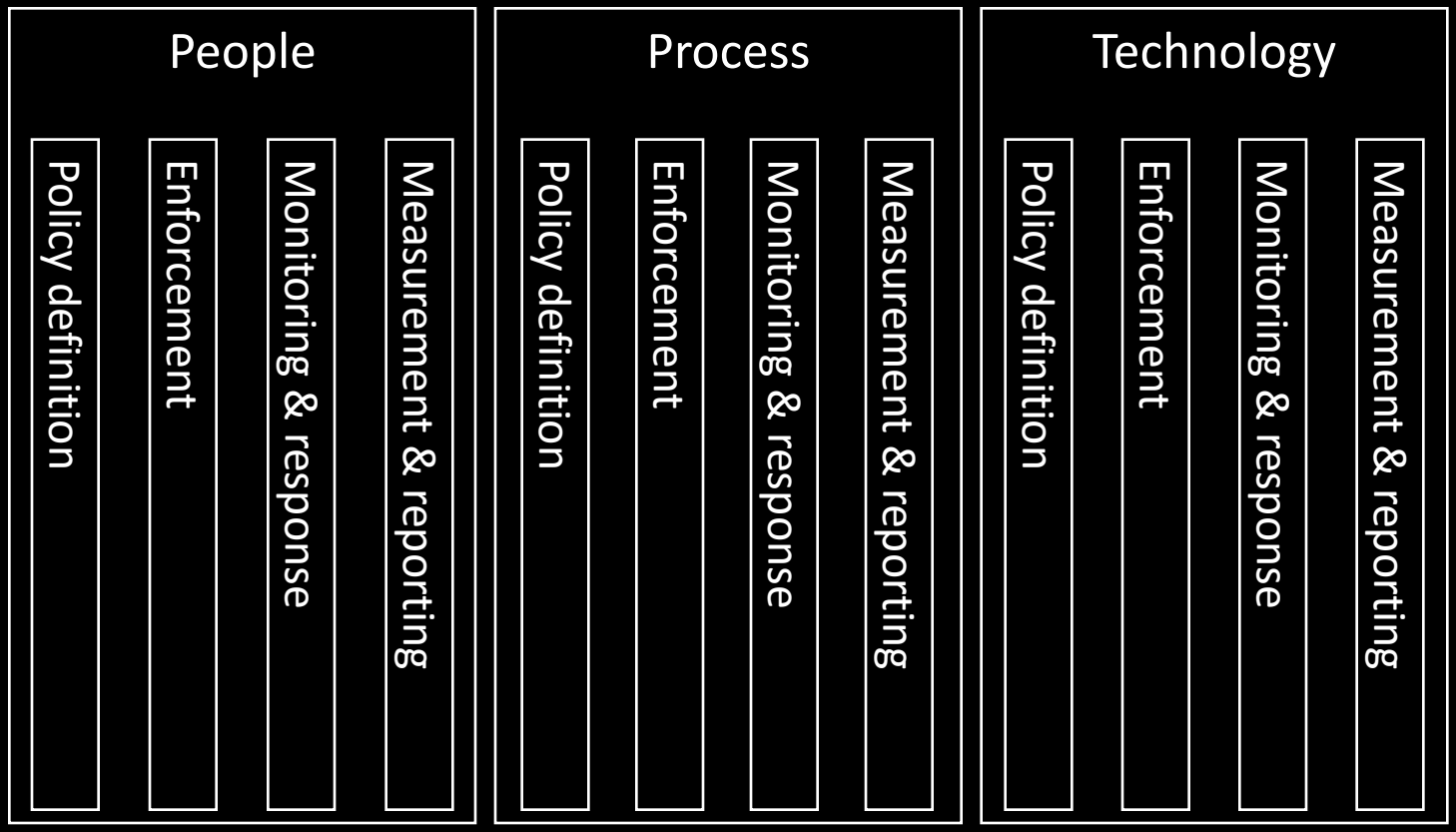
- Was the incident caused by a failure in one or more of the following?
- Technical controls?
- Environmental systems?
- Human factors?
- Management & budget constraints?

Review Resolution

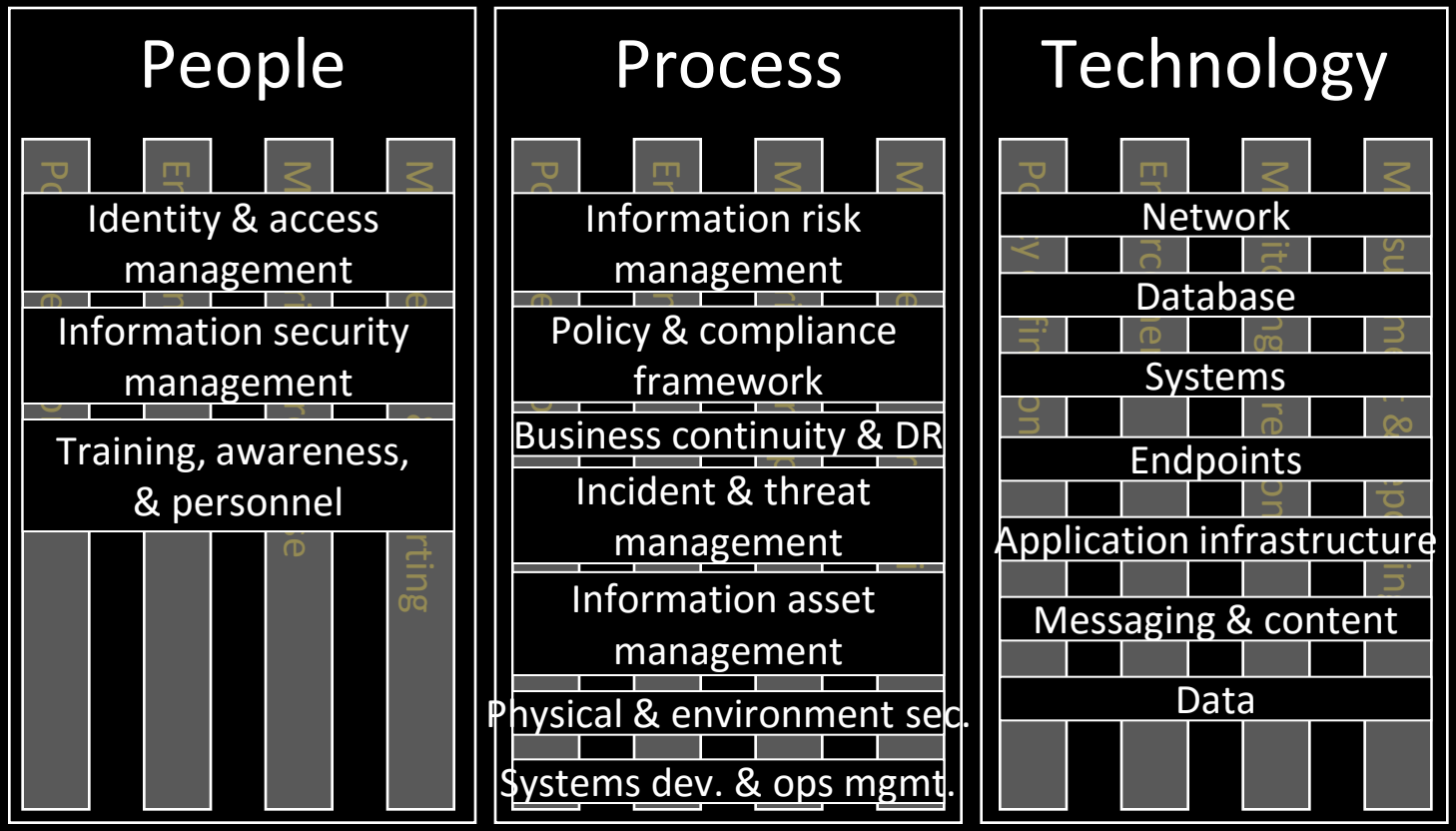
- Could the incident have been detected earlier?
- Could the incident have been resolved quicker?
- Did you need more resources?
- Was reporting adequate?
- Would simulations and rehearsals help in resolving similar incidents?
- Would it help to have better incident response plans?

Create a Final Report

3 Principles



Framework


People
Identity & access management
Information security management
Training, awareness, & personnel
Process
Information risk management
Policy & compliance framework
Business continuity & DR
Incident & threat management
Information asset management
Physical & environment sec.
Systems dev. & ops mgmt.
Technology
Network
Database
Systems
Endpoints
Application infrastructure
Messaging & content
Data

Reference

- NIST SP800-61 Computer Security Incident Handling Guide
  Tim Grance, Karen Kent, Brian Kim
  http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

- NIST SP800-83 Guide to Malware Incident Prevention and Handling
  Peter Mell, Karen Kent, Joseph Nusbaum
  http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf

- NIST SP800-86 Guide to Network and Computer Data analysis: Applying Forensic Techniques to Incident Response
  Tim Grance, Suzanne Chevalier, Karen Kent, Hung Dang
  http://csrc.nist.gov/publications/drafts/Draft-SP800-86.pdf

Thank You