plante moran | Audit. Tax. Consulting. Wealth Management.

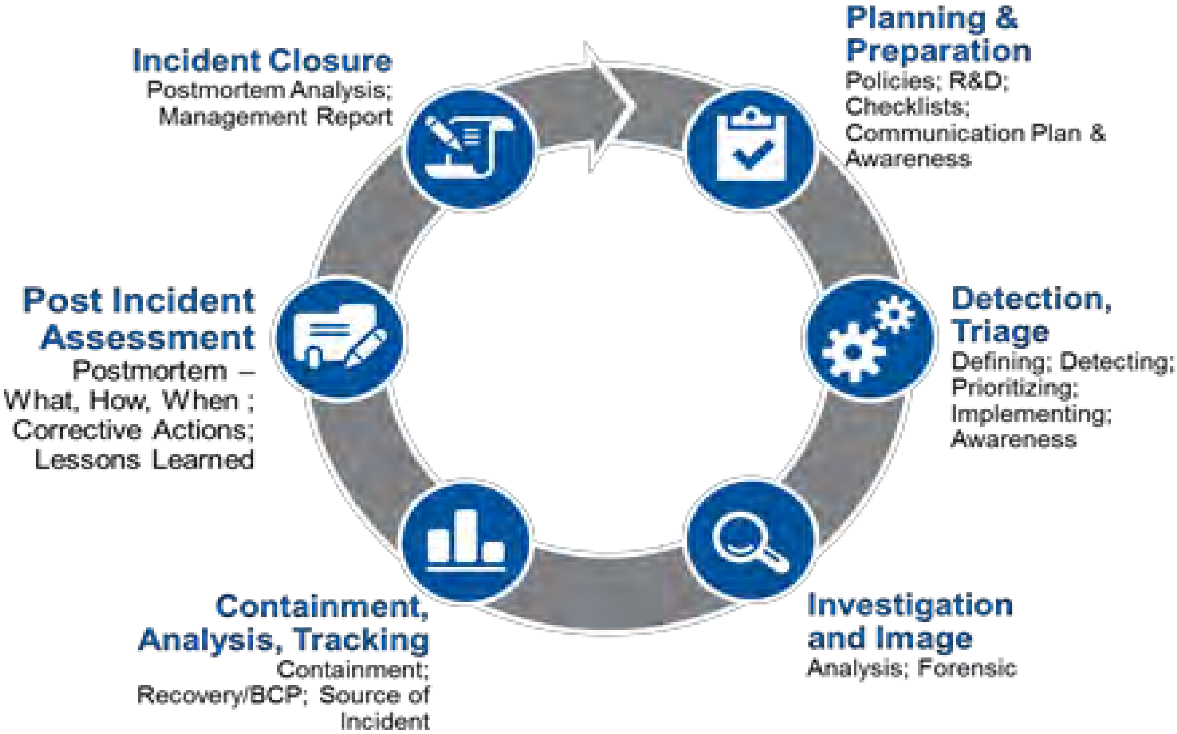
We’ve been hacked – now what?

Cybersecurity for the Public Sector

Overview of today's discussion

- We've been hacked!
  - Incident Response Triage – Where do we start?
  - Incident Evaluation – How did this happen?
  - Incident Prevention – How do we protect our organization?

Incident lifecycle



Planning & Preparation
Policies; R&D; Checklists; Communication Plan & Awareness

Detection, Triage
Defining; Detecting; Prioritizing; Implementing; Awareness

Investigation and Image
Analysis; Forensic

Containment, Analysis, Tracking
Containment; Recovery/BCP; Source of Incident

Post Incident Assessment
Postmortem – What, How, When ; Corrective Actions; Lessons Learned

Incident Closure
Postmortem Analysis; Management Report

Why is This Important?

2017	Statistics
$225	Average cost per record (Ponemon Institute: 2017 US Data Breach Study)
$7.35 mil	Average total cost per organization (Ponemon Institute: 2017 US Data Breach Study)
$.69 mil	Average customer notification cost (Ponemon Institute: 2017 US Data Breach Study)
206 days	Average time to detection (Ponemon Institute: 2017 US Data Breach Study)
55 days	Average time to address a breach (Ponemon Institute: 2017 US Data Breach Study)
82%	Breaches detected by outsiders (Verizon: 2017 Data Breach Report)
78%	Initial intrusions rated as low complexity (Verizon: 2017 Data Breach Report)

Incident Response Triage

Where do we start?

How would your organization react?

A.

RUN
may be you
can escape
the issue

B.

IGNORE
it might go
away

C.

STAY
CALM
you have a
response plan

D.

BLAME
the IT guy
or gal

Step 1: Isolate Risk

Step 2: Assess damage

- Initial Entry Point
  - Email – Other recipients?
  - Compromised credentials – access to other systems?
- Breadth of Impacted Systems
  - Efficient log review process
  - OR
  - Compromised unless proven otherwise?
- Continue Isolating Risk

Step 2: Assess damage

- Availability
  - DDoS
  - Ransomware
- Integrity
  - Data Falsification
- Confidentiality
  - Data Loss

INTEGRITY
AVAILABILITY
INFORMATION SECURITY
CONFIDENTIALITY

What are Hackers After?

- Social Security Numbers
- Credit Card Numbers
- Banking Information
- Usernames and Passwords
- Address, Birthdate, other Personally Identifiable Information
- Email Lists

- ANY data the organization would consider confidential

Step 3: Notifications

- IT/Information Security
- Marketing/Public Relations
- Client-Facing Staff
- Legal
- Executives/Board
- Law Enforcement – Evidence maintained appropriately?
- Vendors

Incident Evaluation

How did this happen?

Levels of detection

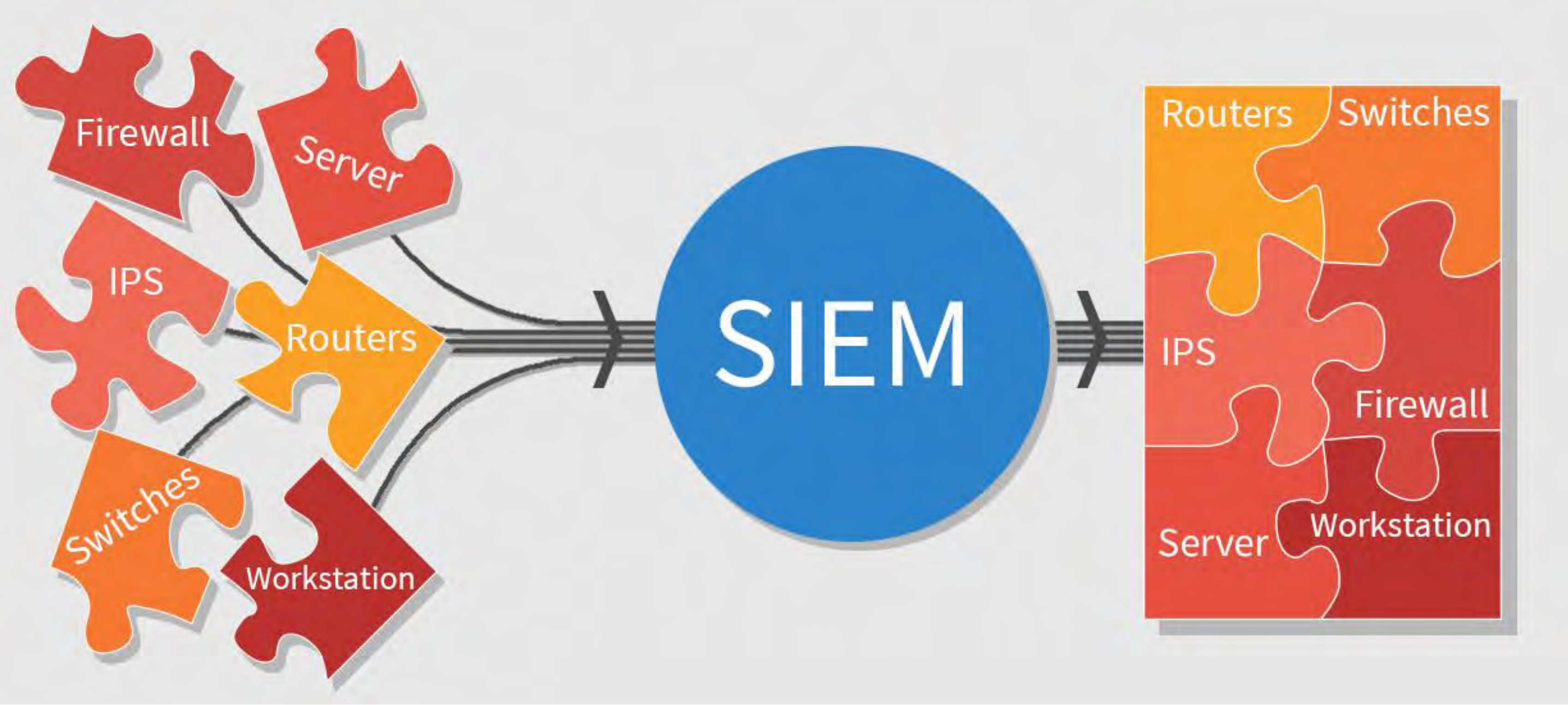
- Employees
  - Notify immediately or fear consequences

Levels of detection

- System Logs
  - Firewall, IDS, network, application, DLP, etc.

Levels of detection

- Correlate Logs
  - SIEM solution



Key Questions to Answer

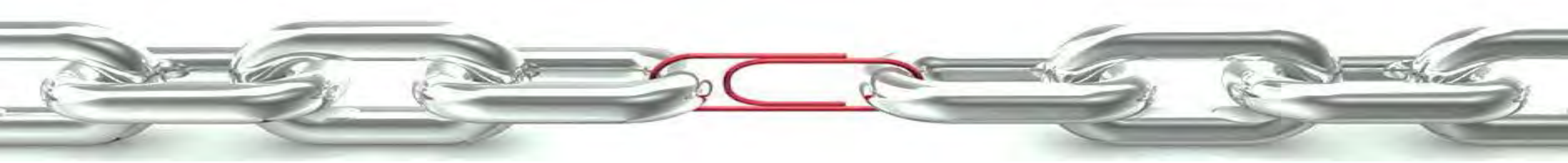
Key Questions to Answer

- Can you confirm the intrusion has ended?
- What was accessed?
- How much did this cost us financially and reputation?
- Was this something you trained or prepped for?
- What Lessons did you learn
- How did it happen….

How did this happen?

- Social Engineering

Most attacks begin socially. Employees are your greatest asset, but often your weakest link to security. Hackers know this, and have developed social scams by the thousands, hoping but one will fall victim

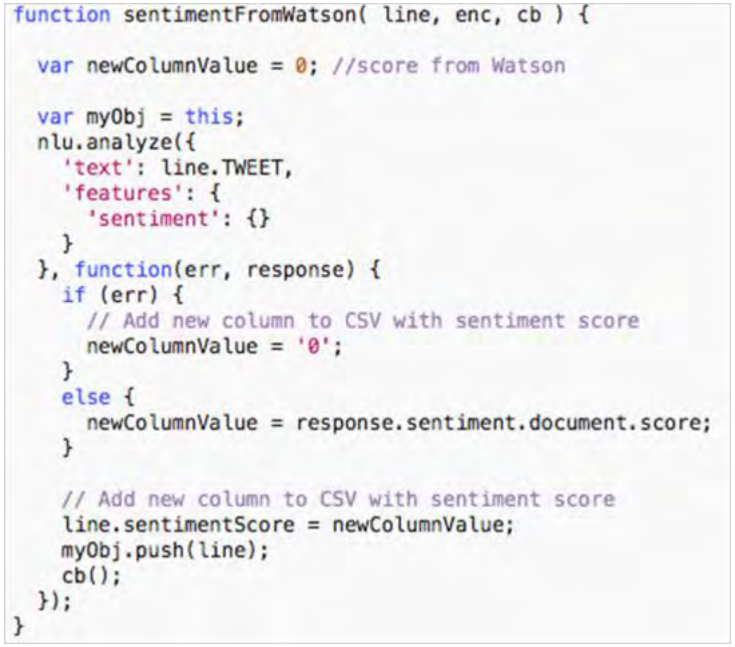


How did this happen?

- Mobile Device Management

How did this happen?

- Weaknesses in Software



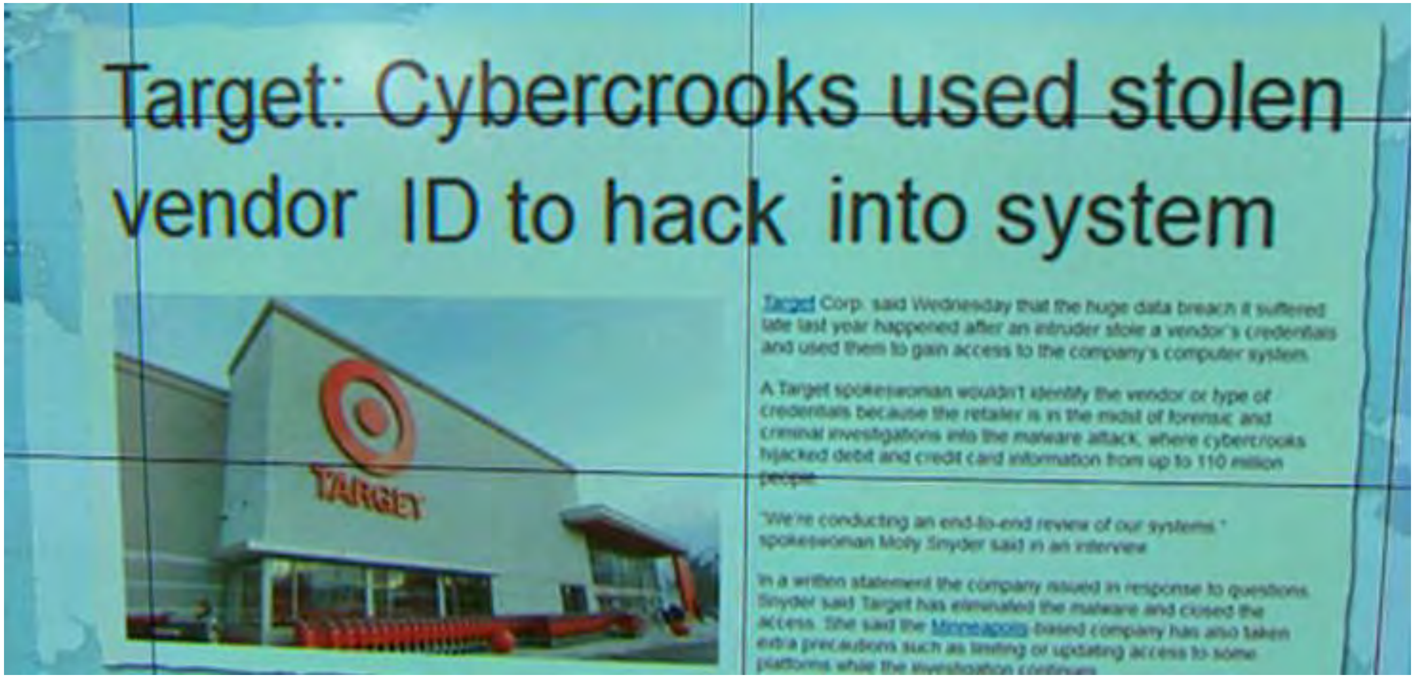
```
function sentimentFromWatson( line, enc, cb ) {

  var newColumnValue = 0; //score from Watson

  var myObj = this;
  nlu.analyze({
    'text': line.TWEET,
    'features': {
      'sentiment': {}
    }
  }, function(err, response) {
    if (err) {
      // Add new column to CSV with sentiment score
      newColumnValue = '0';
    }
    else {
      newColumnValue = response.sentiment.document.score;
    }

    // Add new column to CSV with sentiment score
    line.sentimentScore = newColumnValue;
    myObj.push(line);
    cb();
  });
}
```

How did this happen?

- Weak Passwords

How did this happen?

- Third Party Security



Target: Cybercrooks used stolen vendor ID to hack into system

Target Corp. said Wednesday that the huge data breach it suffered late last year happened after an intruder stole a vendor's credentials and used them to gain access to the company's computer system.

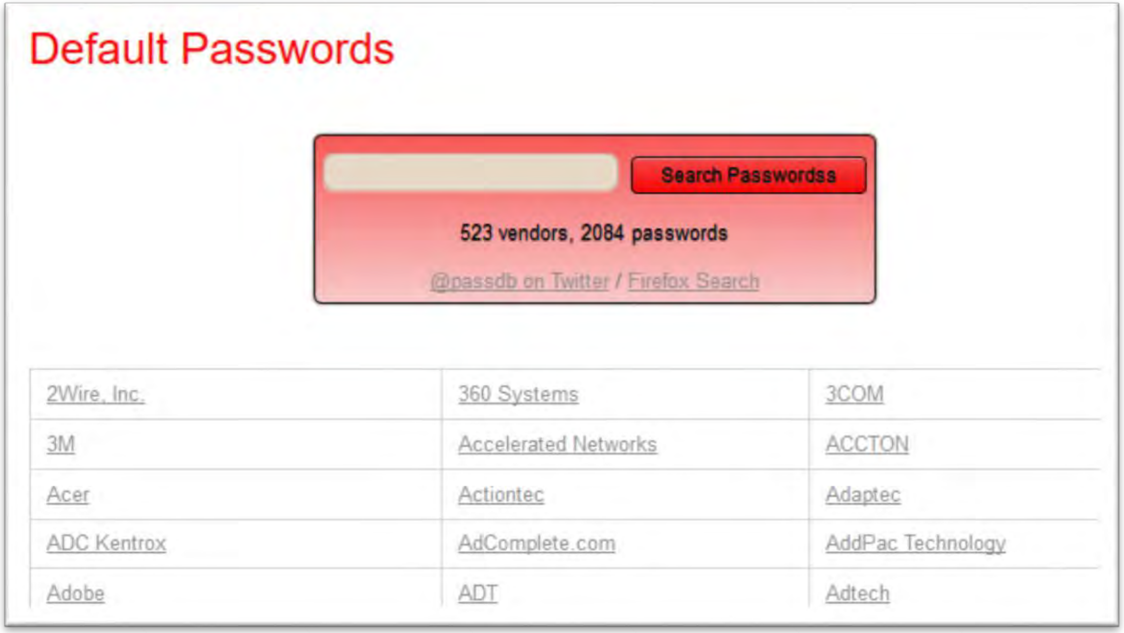
A Target spokeswoman wouldn't identify the vendor or type of credentials because the retailer is in the midst of forensic and criminal investigations into the malware attack, where cybercrooks hijacked debit and credit card information from up to 110 million people.

"We're conducting an end-to-end review of our systems," spokeswoman Molly Snyder said in an interview.

In a written statement the company issued in response to questions, Snyder said Target has eliminated the malware and closed the access. She said the Minneapolis-based company has also taken extra precautions such as limiting or updating access to some platforms while the investigation continues.

How did this happen?

- Misconfigurations
  - Device hardening
  - Segmentation – Internet facing confidential server



Default Passwords

523 vendors, 2084 passwords

@passdb on Twitter / Firefox Search

2Wire, Inc.	360 Systems	3COM
3M	Accelerated Networks	ACCTON
Acer	Actiontec	Adaptec
ADC Kentrox	AdComplete.com	AddPac Technology
Adobe	ADT	Adtech

Incident Prevention

How do we protect our organization?

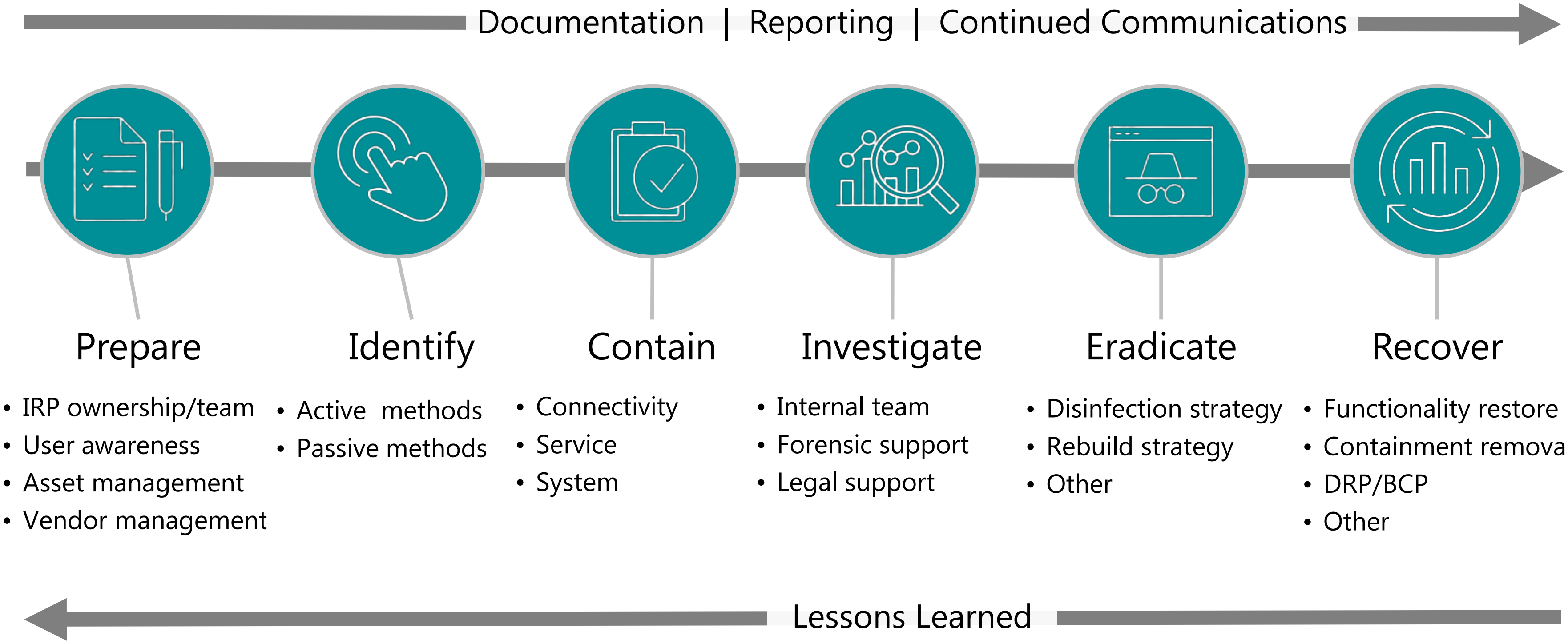
Compliance ≠ Security

No regulation or standard alone will keep your organization safe!

CJIS
FISMA
ISO 2700x
PCI
NIST
State Privacy
HIPAA
GDPR
FERPA

Planning

A defined response framework is important!



Documentation | Reporting | Continued Communications

Prepare

- IRP ownership/team
- User awareness
- Asset management
- Vendor management

Identify

- Active methods
- Passive methods

Contain

- Connectivity
- Service
- System

Investigate

- Internal team
- Forensic support
- Legal support

Eradicate

- Disinfection strategy
- Rebuild strategy
- Other

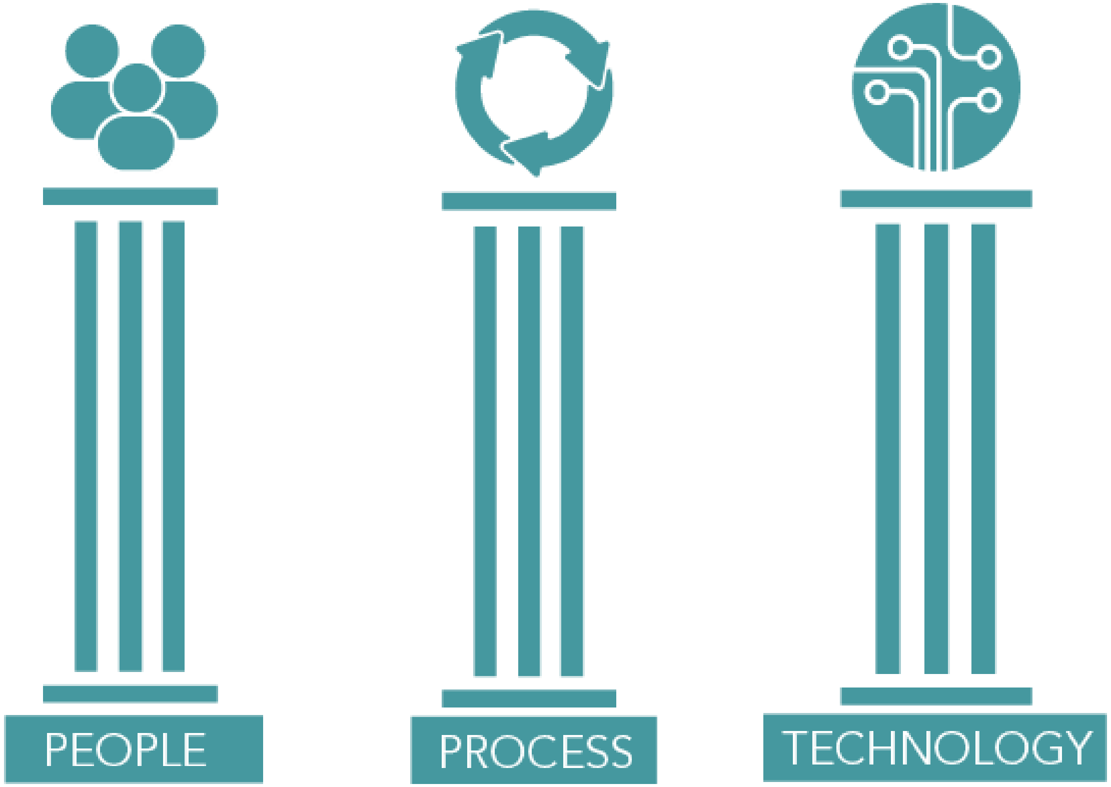
Recover

- Functionality restore
- Containment removal
- DRP/BCP
- Other

Lessons Learned

Who’s responsible?

Information security is not an IT issue



Building around People, Process, and Technology

Identify
what you have

Protect
what you identify

Detect
direct and indirect attacks

Respond
accordingly (IRP)

Recover
appropriately (BCP/DRP)

Identify What You Have

- Asset Inventory
- Application Inventory
- Access Needs – Logical and Physical
- Vendor Inventory

Protect What You Identify

- End User Training
- Network Segmentation
- Patch Management
- Access Management
- Mobile Device Management
- Vendor Management
- Information Security Program

Detect Direct and Indirect Attacks

- Event Logging
  - Firewall
  - IDS/IPS
  - Network
  - Application
- Activity Reviews
  - Alerts and Reports
  - Independent
  - Baselines

Respond Accordingly

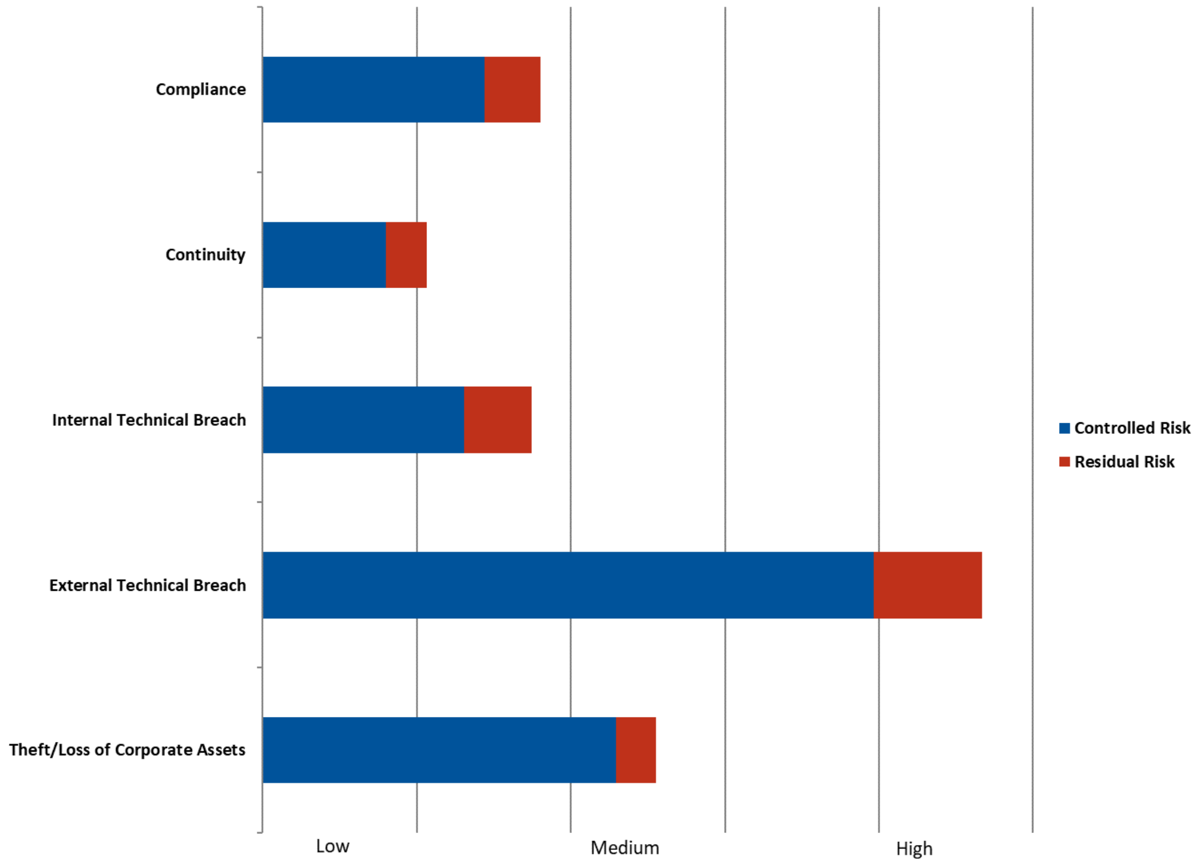
- Incident Response Plan
  - Vendor/Regulator Communications
  - Senior Management Communications
- Cybersecurity Insurance
- Plan Training and Testing

Recover Appropriately

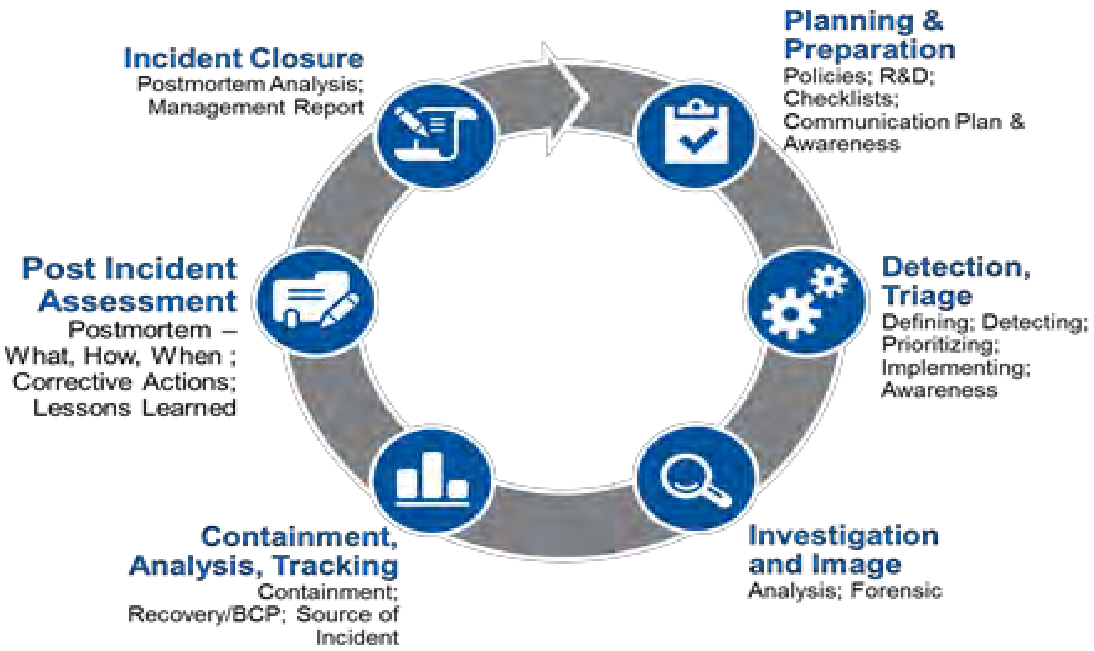
- Disaster Recovery Plan
  - Data Recovery
  - Redundant Connectivity
  - Vendor Failover
- Business Continuity Plan
  - Business Process Workarounds
  - Recover Normal Operations
- Plan Training and Testing

Where Do We Focus Efforts

Risk Based Decisions



Incident lifecycle



Incident Closure
Postmortem Analysis; Management Report

Planning & Preparation
Policies; R&D; Checklists; Communication Plan & Awareness

Detection, Triage
Defining; Detecting; Prioritizing; Implementing; Awareness

Investigation and Image
Analysis; Forensic

Containment, Analysis, Tracking
Containment; Recovery/BCP; Source of Incident

Post Incident Assessment
Postmortem – What, How, When ; Corrective Actions; Lessons Learned