DIGITAL DEFENCE - COMPLETE SECURITY BREACH PROTECTION

DIGITAL DEFENCE

ISACA 2017
Atlantic Provinces Chapter
Information Security & Risk Conference

Agile Incident Management (AIM): Making Incident Response Effective Again

Halifax, NS
07 November 2017

Overview

- Incident response: current methodology
- Principles of Agile Incident Management, AIM
- Strategic approach to AIM
- Tactical elements of AIM
- Key operations of a successful response

Data Security Incidents

Data security incident: the act of non-compliance with the corporate security policy or procedures, or any event that negatively impacts the confidentiality, integrity and availability of your corporate data

(or violation of criminal/civil law or relevant regulations)

Incident Response: Current Methodology

The Threat Has Radically Evolved

- Asymmetric warfare
- Financial and/or ideological motives drive improved skill level
- Multiple direct and indirect attack vectors – physical and cyber
- Fast attacks, long-term persistence
- “Attacks” replaced by “campaigns”

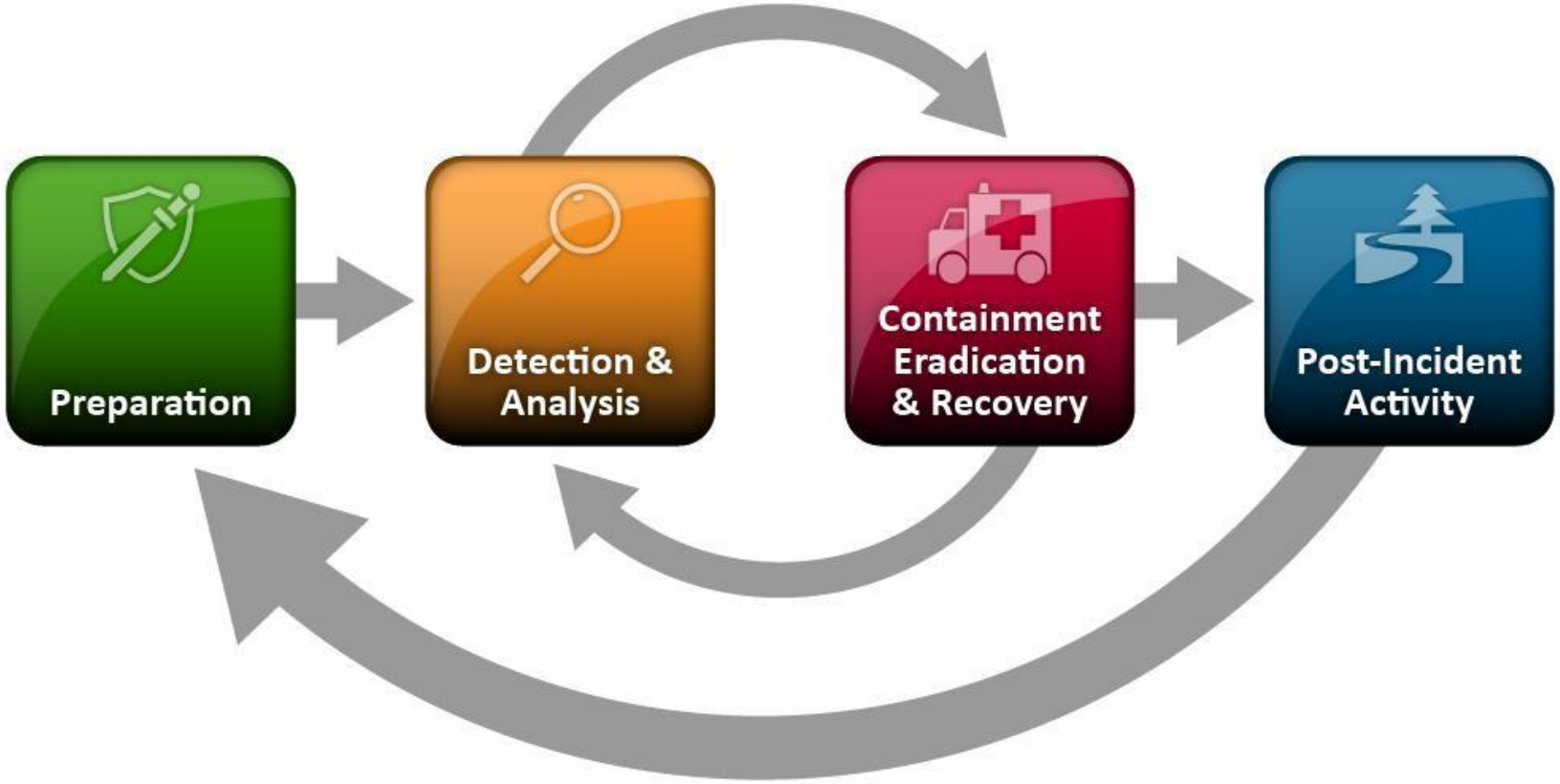
Adopt a military perspective

Implications of the Evolved Threat

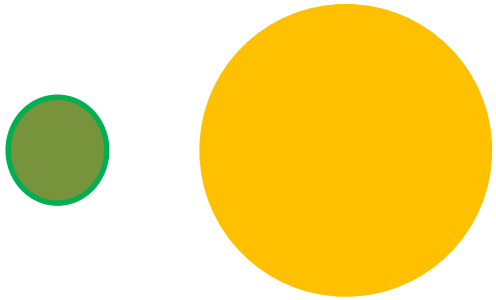
- All organizations are under attack
- At some point, the security controls of each organization will fail – there will be a security incident
- You can't control the failure
- You can only control your recovery

Fail gracefully, recover well

Incident Response – State of the Art

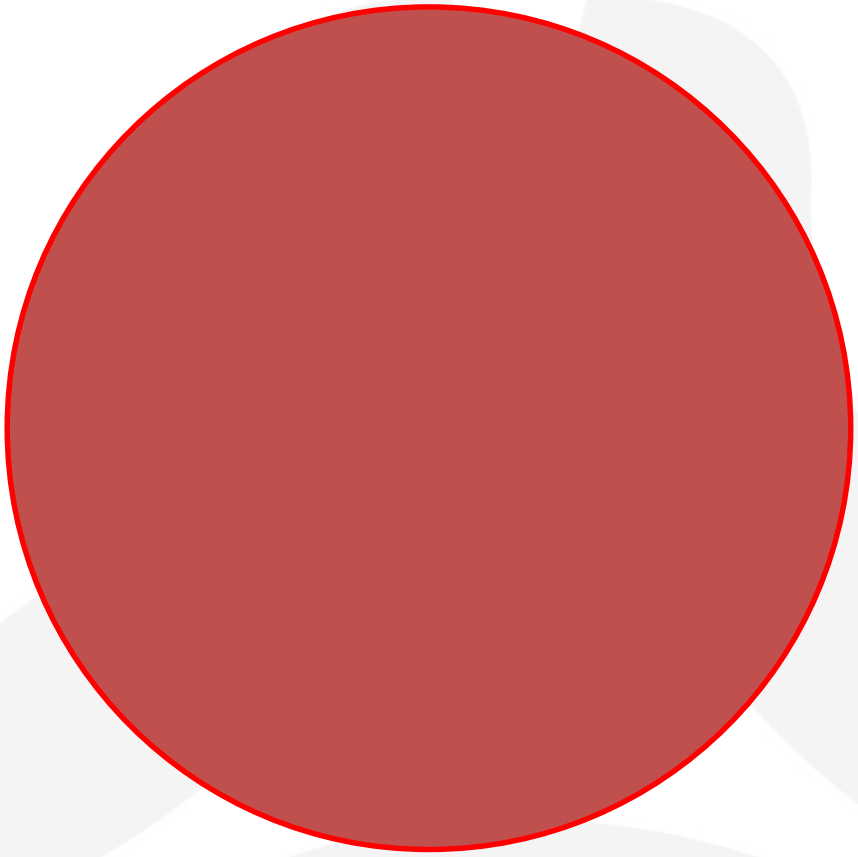


Incident Response – Work Effort



Preparation

Detection



Containment + Eradication

Post-Incident

Why Incident Response Fails

Corporate

- Not supported by business, execs
- Tactical approach
- Business vs. tech
- Failure to support
- Corporate secrecy
- No corporate memory

Technical

- Comms with execs
- Non-technical response required
- Competing priorities
- Internal, privileged attackers
- Lack training, tools

The Single Greatest Failure

- When discovery of the attack starts your response, you've lost the initiative

Principles of Agile Incident Management, AIM

Agile Incident Management, AIM ™

Agile Incident Management is the totality of proactive and reactive formal (documented, approved) measures undertaken to help prevent and manage data security incidents across an organization

Agile Incident Management ™ – The Essentials

- Agility = fast, focused, flexible
- Fast data collection, analysis
- Focused and appropriate response
- Focused formal documentation
- Flexible approach

- Push work effort to front; before the incident
- Adopt a military perspective (“campaign”)

Incident Response - STOP

- **S**TOP
- **T**HINK
- **O**BSERVE
- **P**LAN

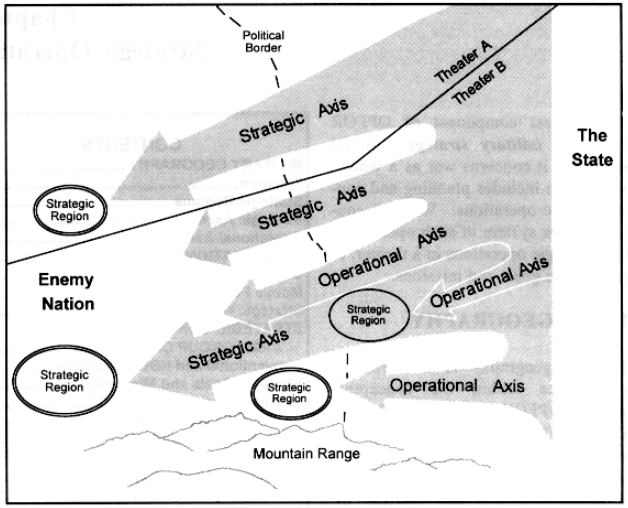
Incident Response – The Goal

- It does not matter what has happened in the past
- It does not matter who or what failed
- This “point” (in time and space) is the start
- Identify the critical path between the start and resolution of the incident
- Incident response is the movement on the path towards resolution; ignore or remove all other distractions

Agile Incident Management ™ - Framework

- Strategic approach
  - Engage the board; risk-based approach
  - Incident response strategy
- Drive strategy to tactics, operations
  - Incident response policy
  - Playbook
  - Table top exercises, other validation
  - Cyber insurance

Strategic Approach to AIM



General Principles

- IT exists to support the business
- An IT incident is a “business process”
- The business owns incident management; IT provides support
- Management of an incident is change control
- Rely on your established business processes

Strategy – Engage the Board

- Strategy originates here
- Attackers are focused on money; so is the Board
- Liability of Board members
- Issues of compliance and regulatory fines, corporate liability
- Mandatory breach reporting = impact stock price
- Contracts and cyber insurance for defence
- Need for collaboration

Strategy - Engage the Board ($$$)

PLANNING AHEAD

COST OF SECURITY INCIDENTS

	2001	2002	2003
Without IR Plan	$113,000	$90,000	$110,000
With IR Plan	$25,000	$14,000	$15,000

MEAN DAYS TO RECOVERY

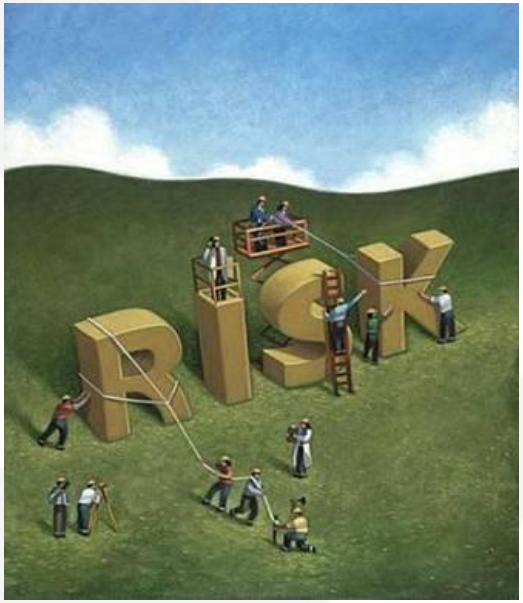
	2001	2002	2003
Without IR Plan	23	20	23
With IR Plan	10	4	4

SOURCE: Guardent (**www.guardent.com**); based on three-year review of 200 incidents at 125 companies.

http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss306_art542,00.html

Risk-Based Approach

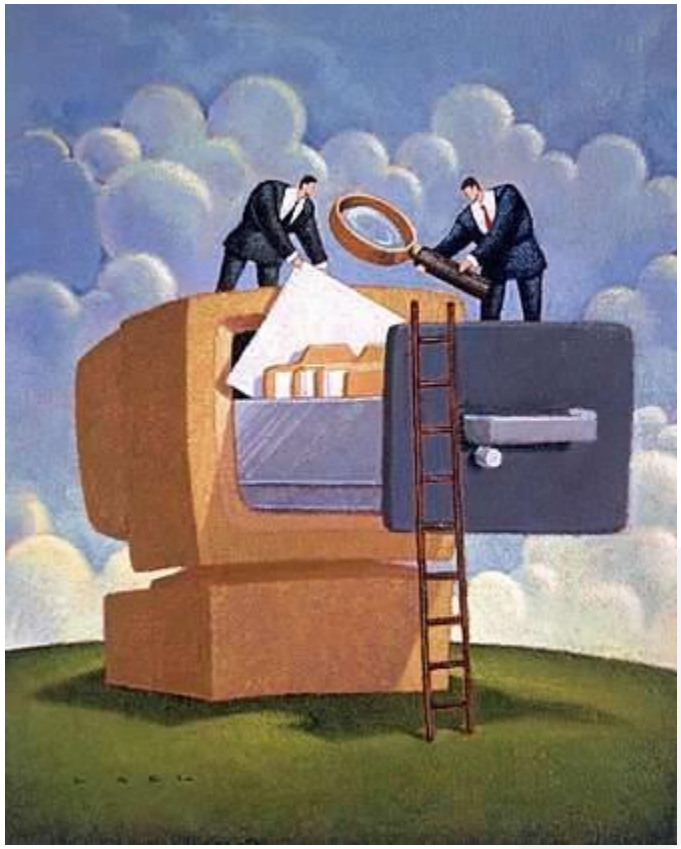
- Risk-based approach to incident management
- Risk / incident management is a business process; business owns the process
- Each business deals with risks differently (“risk appetite”)
- Documented (risk register)
- Consider all risks, including business, technical, HR, insider threat, etc.



Strategic Incident Management Plan

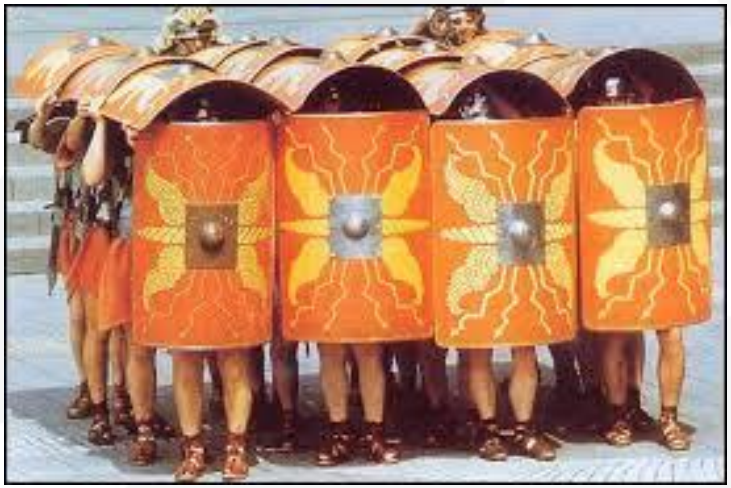
- Active endorsement from Board, executives
- Must be fully aligned with existing business strategy, BCP/DRP
- Supports compliance
- Statement of general principles
- Commitment of responsibility, resources
- Goals
- KPI to measure achievement

Incident Response Policy



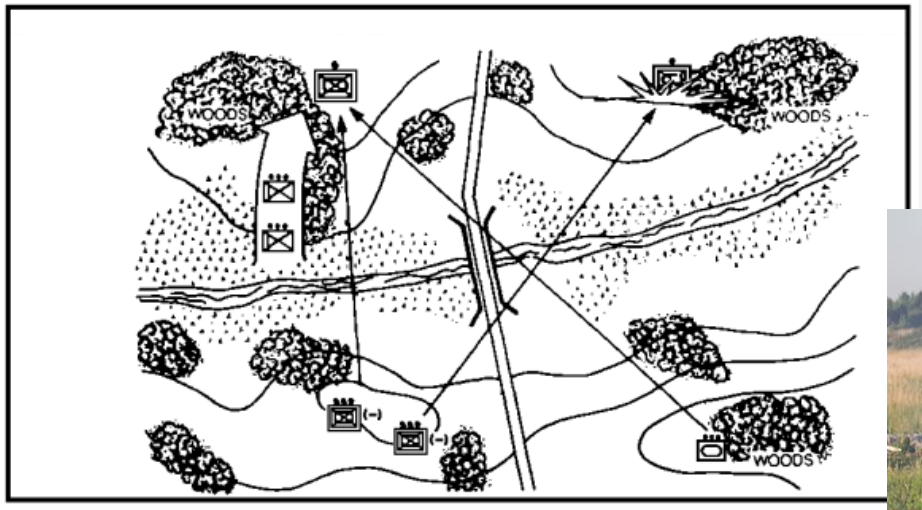
- Connects strategy to tactics, operations
- Business and technical
- Definition of incident
- Who defines the incident
- Flexible incident response
- SOPs “plug into” policy
- Post-incident follow-up
- Keep them up to date

Tactical Elements of AIM



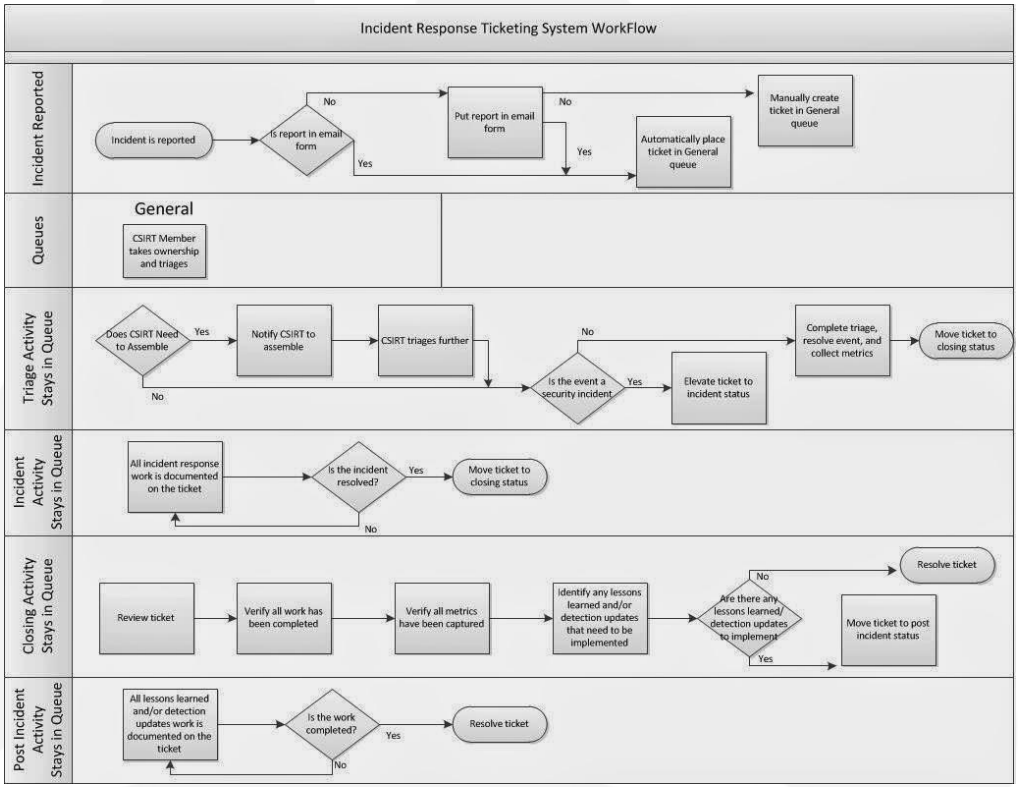
SOPs – The Operational Response

- Formal process drives flexible response - irony!



SOPs – Identify Likely Incidents and Workflow

- Lost, stolen device
- External attack
- Malicious insider
- Malicious software
- Physical intrusion
- Social engineering or phishing
- Policy violation



SOP - Documentation

SOP 01: Malicious Software			
Item	**Action**	**Date / Time**	**Signature**
1	Receive notification from Help Desk		
2	Isolated suspect system(s) from network – physically ensure network cables are removed. Contact duty system (duty_admin@company.com) administrator for all infected servers, network devices		
3	Document identified malicious software in IR ticketing system		
4	Identify AV present on infected system(s) using AV.bat		

Table Top Exercises

- Validate feasibility of strategy, IR policy, SOPs
- Business and technical participation
- Non-practical
- Scenario-based; must be realistic
- Walk through / act out the correct response to an incident
- Debrief to identify success factors, gaps
- Most cost-effective approach

Cyber Insurance

- Increasingly common
- Covers:
  - Losses due to cybercrime
  - Costs of remediation
  - Liability
  - Compliance penalties
  - Legal costs
- May receive discounted insurance rates if incident response program in place

Key Operations of a Successful Response

Key Operations

- Simplify communications
- Roles and responsibilities: business vs. technical, role of legal counsel
- Provide proper training
- Validate existing controls
- Adopt new methodologies
- Data forensics are integral
- “Every man a rifleman”

Simplify Communications

- The military requires brief, effective communications – e.g.: “fire mission”

A. Enemy grid

B. Direction

C. Target

D. Ammo

E. Time, duration

Simplify Communications – Mail Template

A. Is this a “new” or “ongoing” incident being reported?
B. Is the incident “open”, or is it “closed”?
C. What is the severity of the incident?
D. Give a description of the incident?
E. What is the data known to be affected – financial, PI, credit card data, etc?
F. What devices and data are known to be affected? Ensure that source IP addresses and targets of the attack are identified
G. When did the incident occur (date, time)
H. When was the incident reported (date, time)?
I. Who reported the incident?
J. What containment and remediation steps have been completed?
K. What containment and remediation steps are in process, or happening in the future?

Simplify Communications - Internal

- May or may not have a “war room”
- Have a phone bridges reserved for incident management team
- Pre-defined times for management, technical meetings
- Control the internal message (e.g. chat, twitter)

Simplify Communications- External

- Define what information can be shared, and with who (and how!)
- Encourage information sharing
- Collaborate with professional organizations (government, FIRST), other companies in your industry and with vendors (software, hardware)
- Use trusted 3rd parties to provide specialist support (alarm and monitoring, legal, investigative, technical, training)

"Fools you are . . . who say you like to learn from your mistakes ...
I prefer to learn from the mistakes of others, and avoid the cost of my own.“ O. v Bismark

Roles and Responsibilities – “Business” vs “Technical”

- Teamwork - eliminate the business vs. technical bottleneck / warfare
- The incident response team lead is from the line of business
  - Liaise with internal executive management
  - Liaise with partners, media, third parties
  - Make decisions that don’t involve IT (pay ransom?)
  - Let managers manage … and tech folk work!
  - (Role of the team lead is to keep other business managers away from the technical team)

Assign Roles and Responsibilities

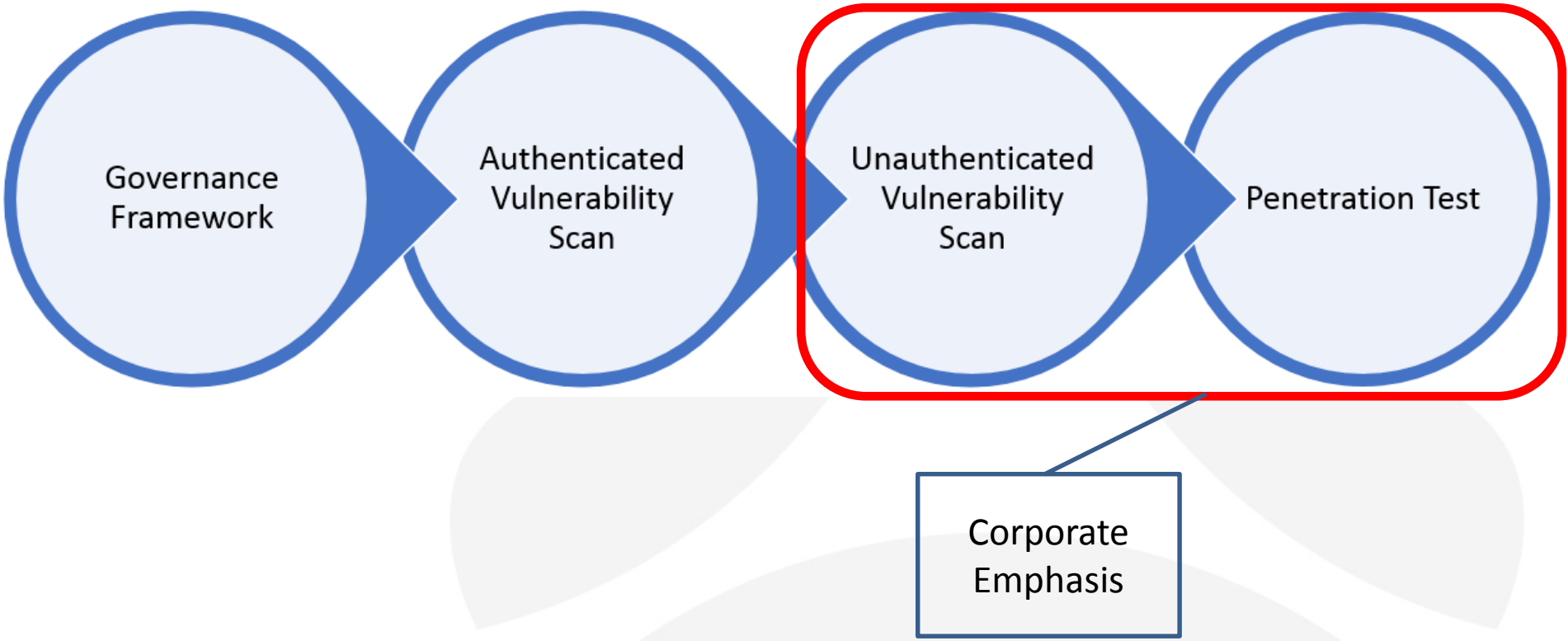
- Managers need clearly defined roles
  - Who is responsible for declaring an incident?
  - At what point do “recovery needs” outweigh “investigative needs”?
- Responders need clearly defined roles
  - Usually have full-time duties in addition to their response role
  - How will conflicts be resolved?
  - How will burn-out be avoided?

Provide Proper Training

Provide Proper Training

- Train as you fight
- Adequate technical training
  - Ethical hacking
  - Indicators of compromise (logging, SIEM)
  - Response and data forensics
- Training can exceed $20K / person; consider 3rd party augmentation
- Employ scenario-based training
- Integrate business into IM training with structured walkthroughs, table top exercises

Validate Existing Controls



Validate Existing Controls - Governance Framework

- Who supports and endorses security testing?
- Who signs the contract?
- Do you have an information security policy?
- Who is managing the testing process?
- What will be done with the results?
- Will there be a retest?
- How will you address the root cause(s) of vulnerabilities?
- How will you learn from the testing?

Vulnerability Assessment and Penetration Testing

- Start = inventory + baseline
- Vulnerability assessment relies largely on automated scanning
- Authenticated vs unauthenticated
- Penetration testing is interactive – additional techniques (social engineering, phishing)
- Focus is on proving vulnerabilities by demonstrating exploits

Validate Existing Controls

Purple Team Assessments

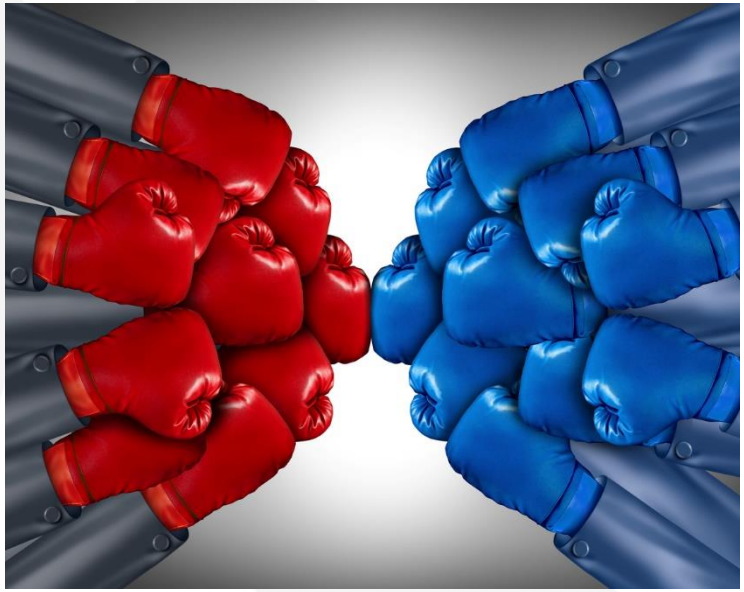
- Defender = blue
- Attacker = red
- The attacker and defender will work together throughout the test:
  - Attacker: “I’m about to send you an obsfucted powershell macro embedded in a Word document”
  - Defender: “Okay, we’re ready”
  - Attacker: “It’s sent … did you detect it”
  - Defender: “Uhhhh … nope …. Try again when we’ve fixed the firewall rules”

Post-Compromise Assessment

- A PCA is the “new penetration test”
- If I told you there was a 40% chance that your network has an APT on it, right now … could you find it?
- If I gave you the indicators of attack, could you search your logs to find the infection point?
- If I gave you the indicators of compromise, could you find all instances of the APT?

Red Team Assessment

- Originated in military
- No scope: no-holds barred; physical and logical attacks
- Long test cycle (preparation + attack phase)
- Not integrated with blue team activities



Adopt New Monitoring Methodologies

- Traditional logging (what you're not doing enough of)
  - What you log is set by policy, SOPs
  - Monitor all activity (automated processes, employees, privileged users)
  - Establish a baseline (the "normal good")
  - Look for anomalies, exceptions – but keep a record of legitimate and approved activities as well
- Most important – increase monitoring after a security event occurs – it's a "campaign"

New Monitoring Methodologies - Honeypots

- Case study: manufacturing
- Logging was difficult (old devices, complex network, no storage capabilities)
- Concerned with access to HR and ICS devices
- Deployed monitored honeypots
- Identified 2 employees attempting to access HR systems within 5 days

Data Forensics are Integral

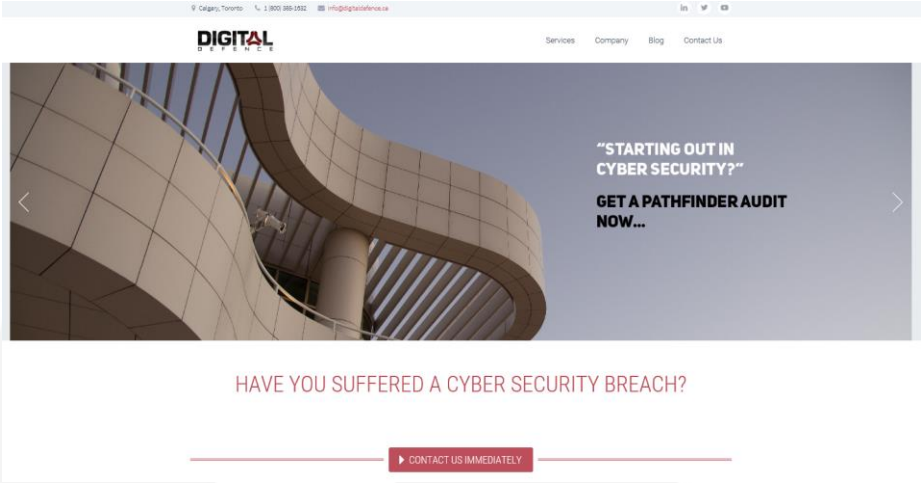
- Data forensics closely tied to IM process
- Design, construct and configure policies, SOPs, and data systems to support future forensics requirements
- Pre-emptive forensics
- Non-traditional forensics: “sniping”, live system analysis, memory analysis

Your Employees are the “First Responders”

- Non-IT employees are the first to spot 70% of all security incidents
- They are usually closest to a system that is being attacked
- Employees can be taught basic response skills
  - Recognize an attack
  - Disconnect the system from the network
  - Don’t change anything
  - Call the IT support number
- “Every employee a responder”

DigitalDefence (www.digitaldefence.ca)

- Specialize in penetration testing, incident response, data forensics
- Training provider



Robert W. Beggs, CISSP

Connect with: https://www.linkedin.com/in/robertbeggs

Check out: Canadian Information Security Professionals

robert.beggs@digitaldefence.ca