Cyber Security Incident Response Mitigation & Response Strategies

Randy Romes
CISSP, CRISC, CISA, MCP, PCI-QSA, PCIP
Principal – Information Security
Randy.Romes@claconnect.com

October 2020

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Create Opportunities

Disclaimers

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

Learning Objectives

By the end of this session, you will be able to:

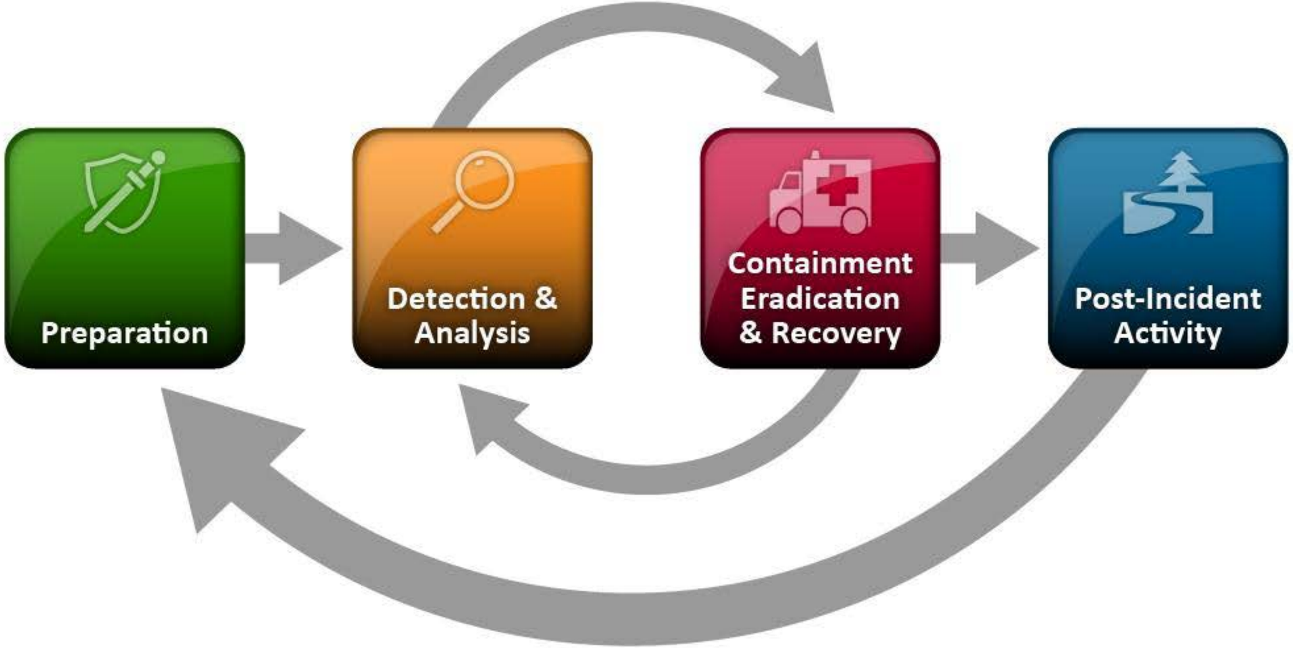
- Describe the latest developments in ransomware and account take over attacks
- Give examples from case studies about recent intrusions, breaches, and lessons learned from each case study
- Describe key risks and controls to mitigate and respond to breaches in Office 365
- Describe the aspects of the “Cybersecurity Kill Chain”
- Define key strategies to test the organization’s Incident Response program

Today’s Presenter

Randy Romes
CISSP, CRISC, CISA, MCP, PCI-QSA, PCIP
CLA (CliftonLarsonAllen LLP)

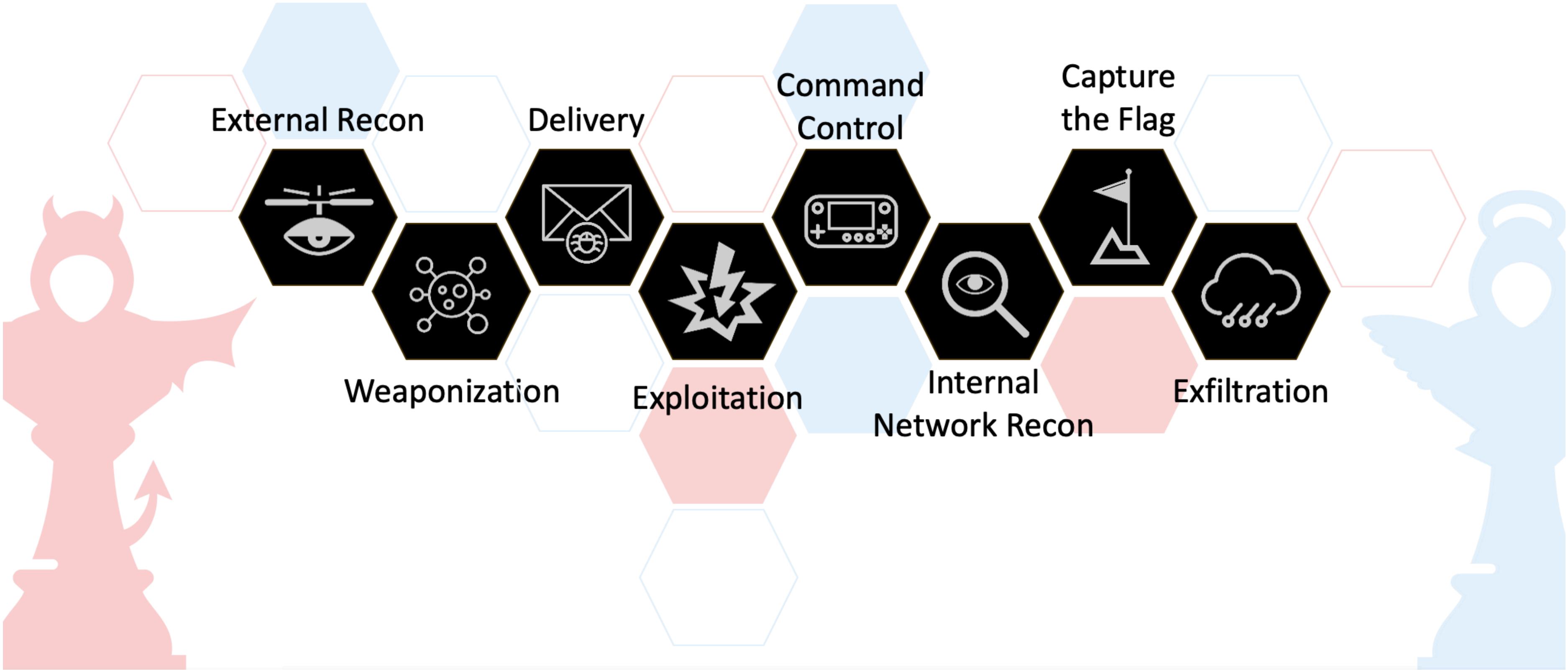
- “Professional Student”
- Science Teacher / Self Taught Computer Guy
- IT Consultant – Project Manager – IT Staff/Help Desk – Hacker
- Assistant Scout Master (Boy Scouts)

Incident Response Life Cycle (NIST 800-61)



Incident Response Life Cycle

The Cyber Kill Chain



External Recon

Weaponization

Delivery

Exploitation

Command Control

Internal Network Recon

Capture the Flag

Exfiltration

Current State of Cybercrime

What are the bad guys up to?

Where are the breaches coming from?

Sun Zhu - The Art of War – "Know They Enemy"

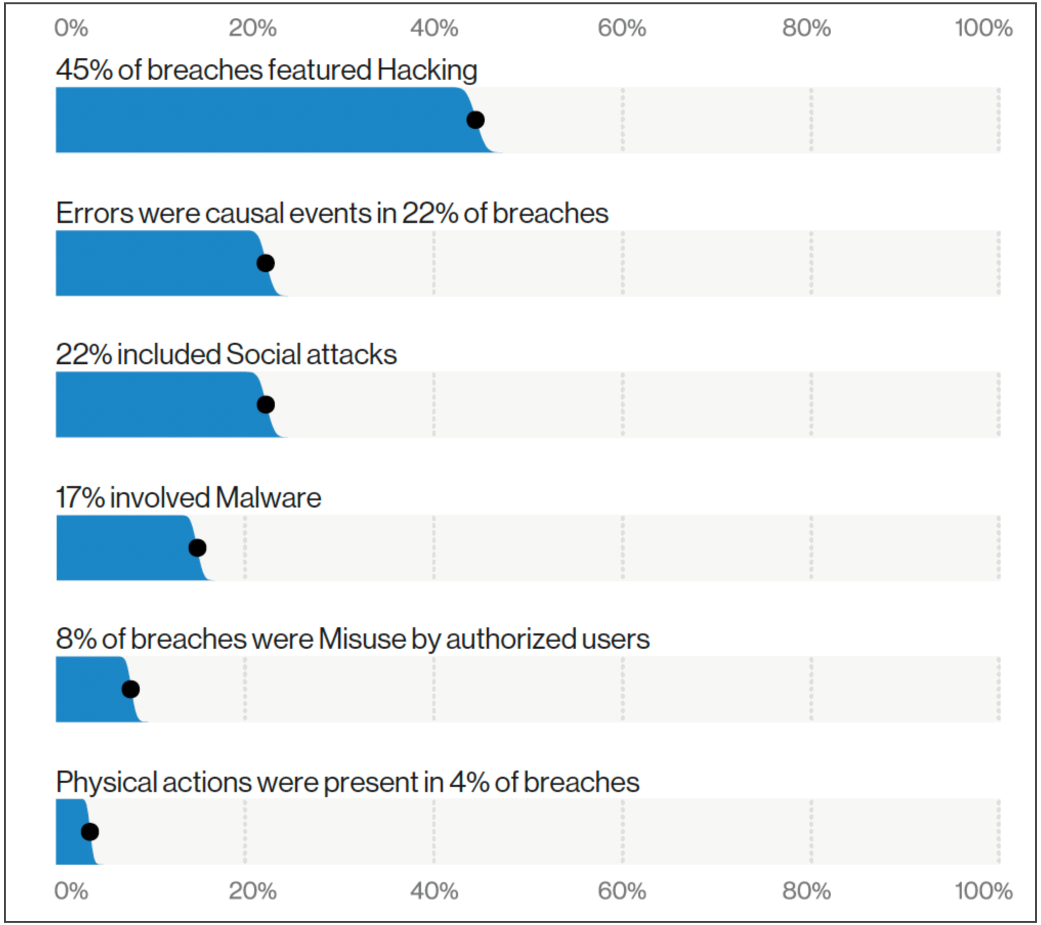
Current State of Cybercrime

- Hackers have monetized their activity
  - Theft of personally identifiable information (PII)
  - Payment fraud
  - Ransomware

- Organized crime is highly involved

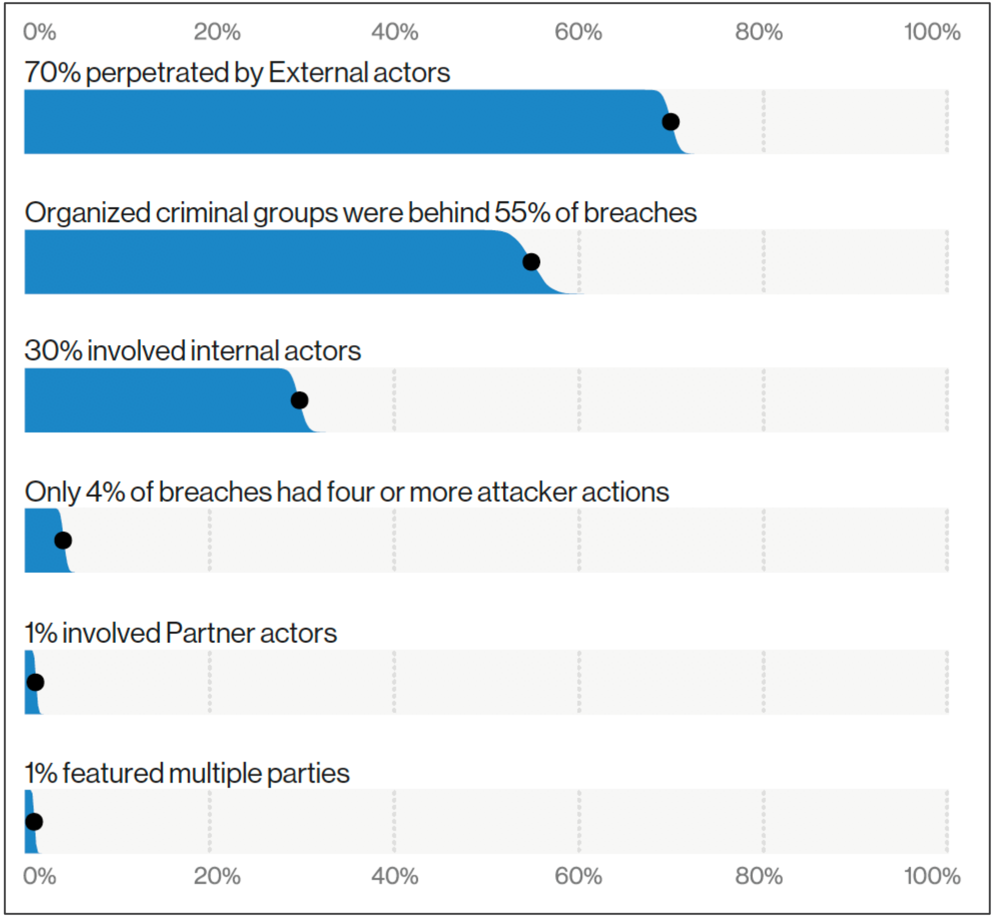
Across All Industries

Causes of Data Breaches



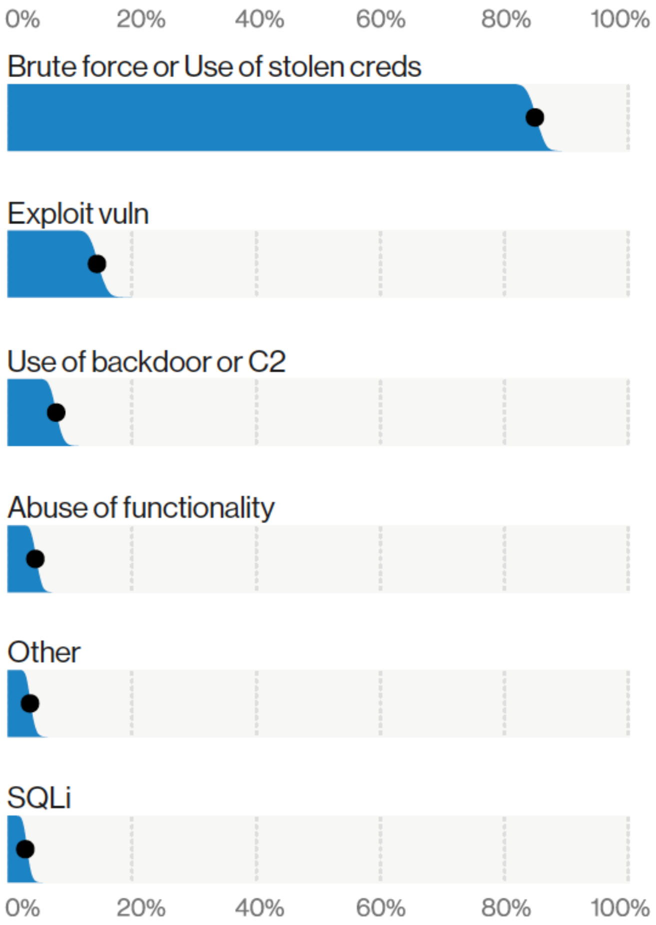
Across All Industries

Who’s Behind the Breaches



Compromised Email

- So much easier to steal passwords than exploit systems



Organized Crime

- Hacking is run like a business with specialization
  - Vulnerability Research
  - Writing malware and hacking tools
  - Operating and “renting” botnets
  - Stealing/acquiring/purchasing log in credentials
  - Stealing data
  - Selling data
    - ◊ (collect data from various sources/BIG DATA)
- Most attacks are largely automated / targets of opportunity

Theft of PII

- All this information has value
  - Submit fraudulent tax returns
  - Submit fraudulent insurance claims
  - Submit fraudulent unemployment claims
  - Set up fraudulent identities for credit
  - Purchase items with stolen credit card information
  - Use emails for phishing campaigns
- Attackers buy and sell data on cyber black market
  - Similar to amazon.com for stolen information

In the News

23 SEP 20

Govt. Services Firm Tyler Technologies Hit in Apparent Ransomware Attack

Tyler Technologies, a Texas-based company that bills itself as the largest provider of software and technology services to the United States public sector, is battling a network intrusion that has disrupted its operations. The company declined to discuss the exact cause of the disruption, but their response so far is straight out of the playbook for responding to ransomware incidents.

New Jersey hospital paid ransomware gang $670K to prevent data leak

By Lawrence Abrams October 3, 2020 10:15 AM 1

University Hospital New Jersey in Newark, New Jersey, paid a $670,000 ransomware demand this month to prevent the publishing of 240 GB of stolen data, including patient info.

7 JUL 2020 NEWS

Manufacturing Sector Paid Out 62% of Total Ransomware Payments in 2019

Defensive Strategies to Minimize and Mitigate the Risk of Breaches

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Create Opportunities

Strategies

Our information security strategy should have the following objectives:

1. Assume breach mentality
2. Defense in-depth – protect the crown jewels
   - Users that aware and savvy
   - Networks that are hardened and resistant to malware and attacks
   - Resilience capabilities: monitoring, incident response, testing, and validation
3. All of the above is supported by regular/periodic risk assessment

Assume Breach

It is not a matter of IF…

It is a matter of WHEN…

Assume Breach Approach

“Assume breach…”

Limits the trust placed in applications, services, identities, and networks by treating them all, both internal and external, ***as not secure and possibly already compromised***.

Old Model – Prevent Breach

- Focused on preventing a breach
  - Build the walls higher/thicker
  - *(hint… there are no more walls…)*

➢ Money went towards perimeter controls

  - “Next-gen” firewalls
  - Intrusion detection and prevention
  - Antivirus/antimalware software

Approach Comparison

Prevent Breach

- Firewall / Perimeter
- Static Defense
- “Set and Forget”
- Code Review
- Antivirus
- Threat Modeling

Assume Breach

- Constant Monitoring
- Logical Defense
- Awareness
- Testing
- Continual Improvement
- Red Team Simulation and response practice

Security Evolution

- Preventing breaches is critical, but does not adequately address modern threats

- Traditional controls are still necessary

- Practices must be continually tested and augmented to effectively address modern adversaries such as APTs, cyber criminals, etc.

Security Evolution

- Prepare for an “inevitable” breach
- Build and maintain robust, repeatable, and thoroughly tested security response procedures (playbook)
- Understand what normal looks like and continuously monitor for the presence of abnormal

Security Evolution

We do not expect firefighters to learn how to fight a fire when we call them!

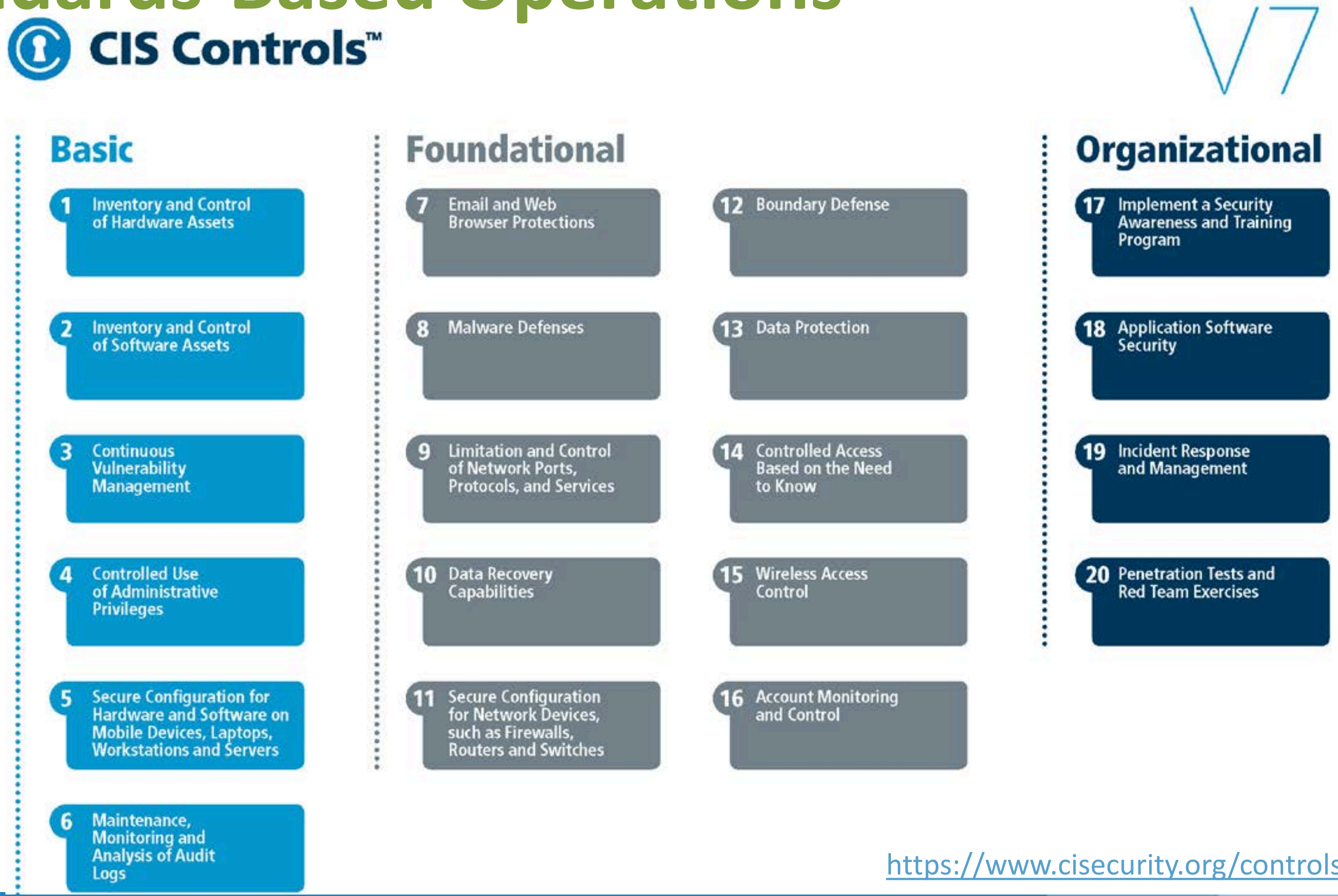
We should NOT expect our IT staff to handle incidents without training or proper tools.

Defense in-Depth

Successive layers of preventative and detective controls

Supported by monitoring and incident response capabilities

Standards-Based Operations



CIS Controls™ V7

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols, and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

https://www.cisecurity.org/controls/

Defined Standards

- Secure standard configurations
  - ➢ "Every Windows workstation will have the following"
  - ➢ All wireless systems will be configured as follows…
- Harden your systems and applications
  - ➢ Principal of minimum access and least privilege
  - ➢ Turn off the services/components you do not need
  - ➢ Change or remove the defaults

Resources – Hardening Checklists

Hardening checklists from vendors

- CIS offers vendor-neutral hardening resources

  http://www.cisecurity.org/

- Microsoft Security Checklists

  http://technet.microsoft.com/en-us/library/dd366061.aspx

Most of these will be from the “BIG” software and hardware providers

Operational Discipline

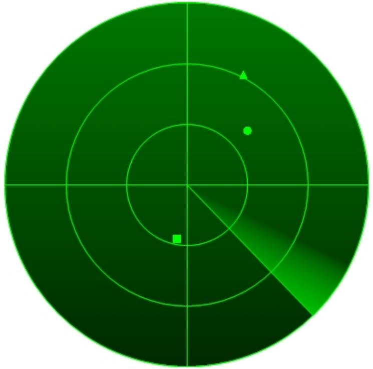
- Disciplined change management
- Consistent exception control and documentation
  - Should include risk evaluation and acceptance of risk
  - Risk mitigation strategies
  - Expiration and re-analysis of risk acceptance

Vulnerability & Patch Management Standards

- Define your standard
  - Internet-facing critical updates will be applied within **<u>hours</u>**
  - Internal system critical updates will be applied within **<u>days</u>**
- Manage to your standard
- Document and manage your exceptions
  - Don’t forget the expiration date

Vulnerability Management Monitoring

- Monitoring
  - System logs and application “functions”
  - Accounts
  - Key system configurations
  - Critical data systems/files
- Scanning
  - Patch Tuesday and vulnerability scanning
  - Rogue devices
  - Recognize abnormal



Disaster Recovery & Business Continuity

- Inventory of assets and results of risk assessment are crucial
  - Hardware and software
  - Critical data elements (“the crown jewels”)
  - Critical business processes
- Business impact analysis with definition of recovery point objectives
  - Defines priority for restoration
- Disaster Recovery is periodically practiced
  - Need to make sure it works the way you expect

Incident Response Preparedness

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

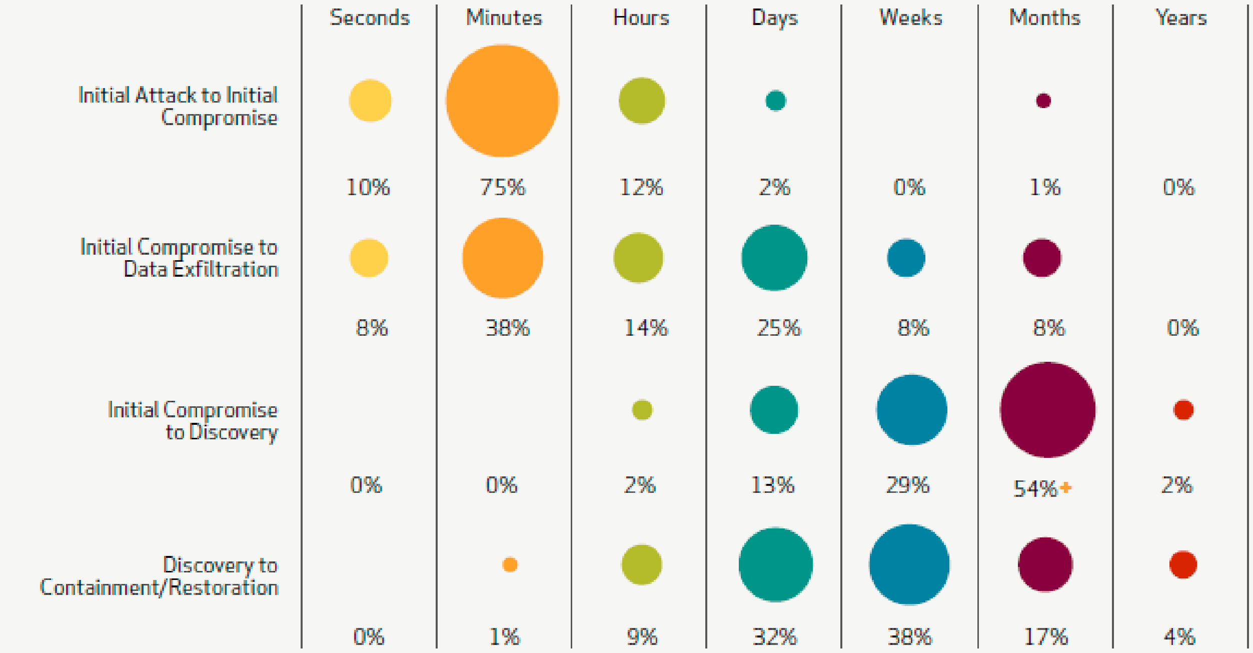
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Create Opportunities

Intrusion & Breach Timelines

Figure 40. Timespan of events by percent of breaches

Source: 2012 Verizon Breach Investigation Report



	Seconds	Minutes	Hours	Days	Weeks	Months	Years
Initial Attack to Initial Compromise	10%	75%	12%	2%	0%	1%	0%
Initial Compromise to Data Exfiltration	8%	38%	14%	25%	8%	8%	0%
Initial Compromise to Discovery	0%	0%	2%	13%	29%	54%+	2%
Discovery to Containment/Restoration	0%	1%	9%	32%	38%	17%	4%

Incident Response & Forensic Resilience

- Your Program
  - Proactive components
    - ➢ The Boy Scouts Motto: Be Prepared
    - ➢ Protect and detect
    - ➢ Know what normal looks like
  - Reactive components
    - ➢ NOT a chemistry experiment…
    - ➢ Recognize abnormal
    - ➢ Respond and Remediate

The Program…

- Establishes incident response program and policies
  - Commitment
  - Org structure and capabilities
- Creates an incident response plan focused on
  - Defense in-depth
  - Intelligently protect your “crown jewels”
  - Maintaining C.I.A.
    - ◊ Confidentiality
    - ◊ Integrity
    - ◊ Availability

Purpose

- Prepare for unscheduled computer (security) incidents (people, rules, and tools)
- Identify potential threats and vulnerabilities
- Develop best responses and reduce damage
- Apply critical thinking to solve problems
- Improve over time…

Purpose

- How can an IR plan mitigate risk?
  - Clearly defined roles and responsibilities for response
  - Enhanced understanding of needed skills
  - Enhanced understanding of needed controls, processes, and technology
  - Quick and focused response to incidents
  - Enhanced ability to respond to threats and remove risks

Purpose

- Understand and define the difference between an intrusion event and a breach
  - "Know what normal looks like" as your baseline
  - Define indicators of compromise
    - ◊ What does abnormal look like?
  - Understand and apply relevant state laws related to breach notification

Incident Response Resources

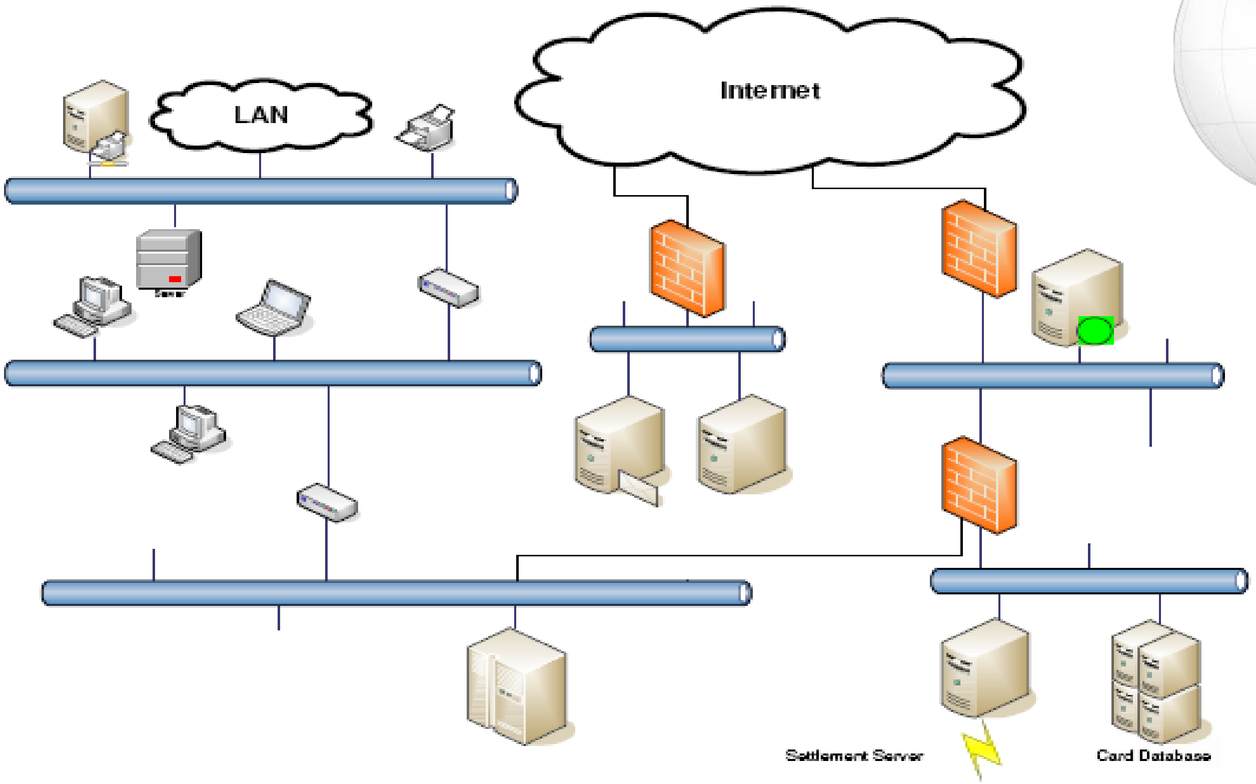
Examples for definition of incidents

15 indicators of compromise

http://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/d/d-id/1140647

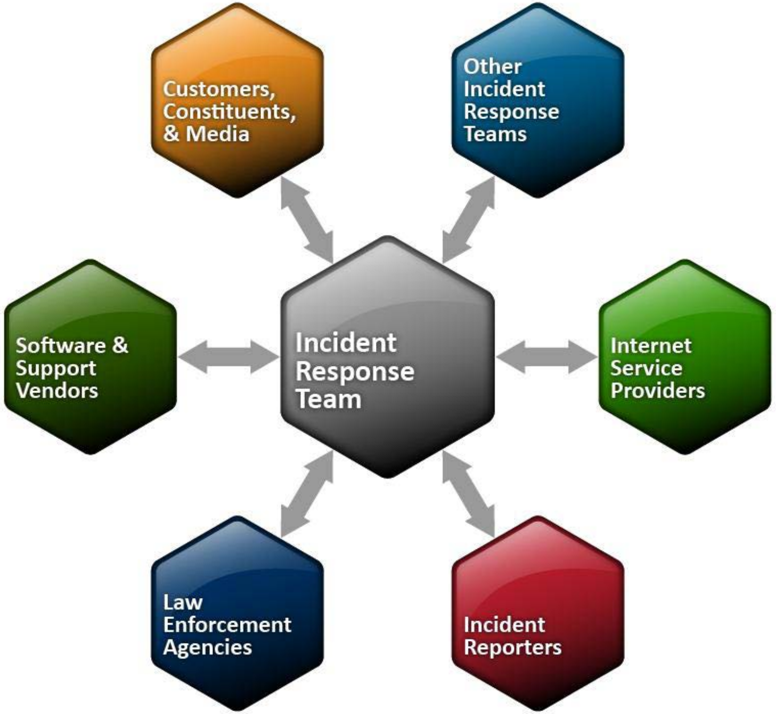
1. Unusual outbound network traffic
2. Anomalies in privileged user account activity
3. Geographical irregularities
4. Other log-in red flags
5. Swells in database read volume
6. HTML response sizes
7. Large numbers of requests for the same file
8. Mismatched port-application traffic
9. Suspicious registry or system file changes
10. DNS request anomalies
11. Unexpected patching of systems
12. Mobile device profile changes
13. Bundles of data in the wrong places
14. Web traffic with unhuman behavior
15. Signs of DDoS activity

What Is "Normal" – IoC's



Communication Strategies

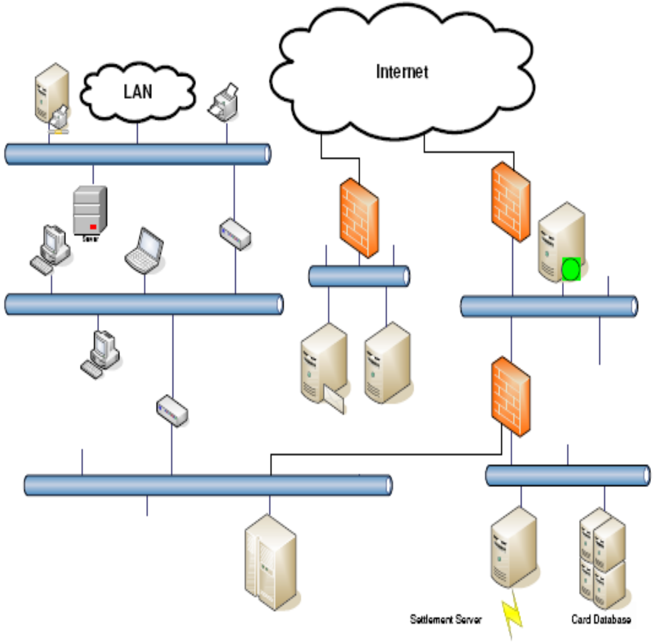
- Internal
  - Staff
  - Management
  - Board
- External
  - Service providers
  - Law enforcement
  - Regulatory
  - Media


Customers, Constituents, & Media
Other Incident Response Teams
Software & Support Vendors
Incident Response Team
Internet Service Providers
Law Enforcement Agencies
Incident Reporters

Know Your Network – What Is “Normal”?

Alignment of centralized audit logging, analysis, and automated alerting capabilities (SIEM) and DLP

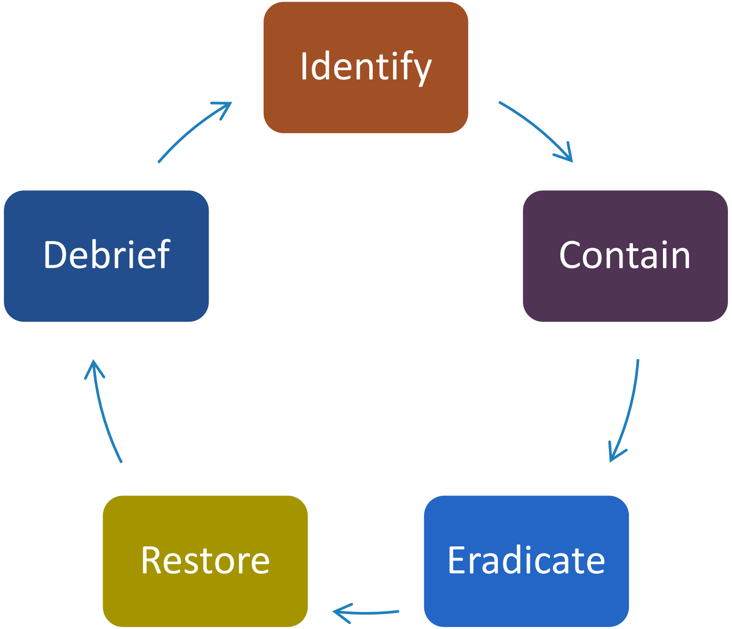
- Infrastructure
- Servers and applications
- Archiving vs. Reviewing



➢ **Know your Network, Systems, DATA**

➢ **Monitor and review of service providers**

Reactive Defense Strategy



Fire Department/Team Paradigm

Concepts

- Specialized gear
- Specialized training
- Tools are tested
- Simple repeatable tasks
- Fast response is expected
- Communicate effectively

Boy Scouts – Be Prepared?

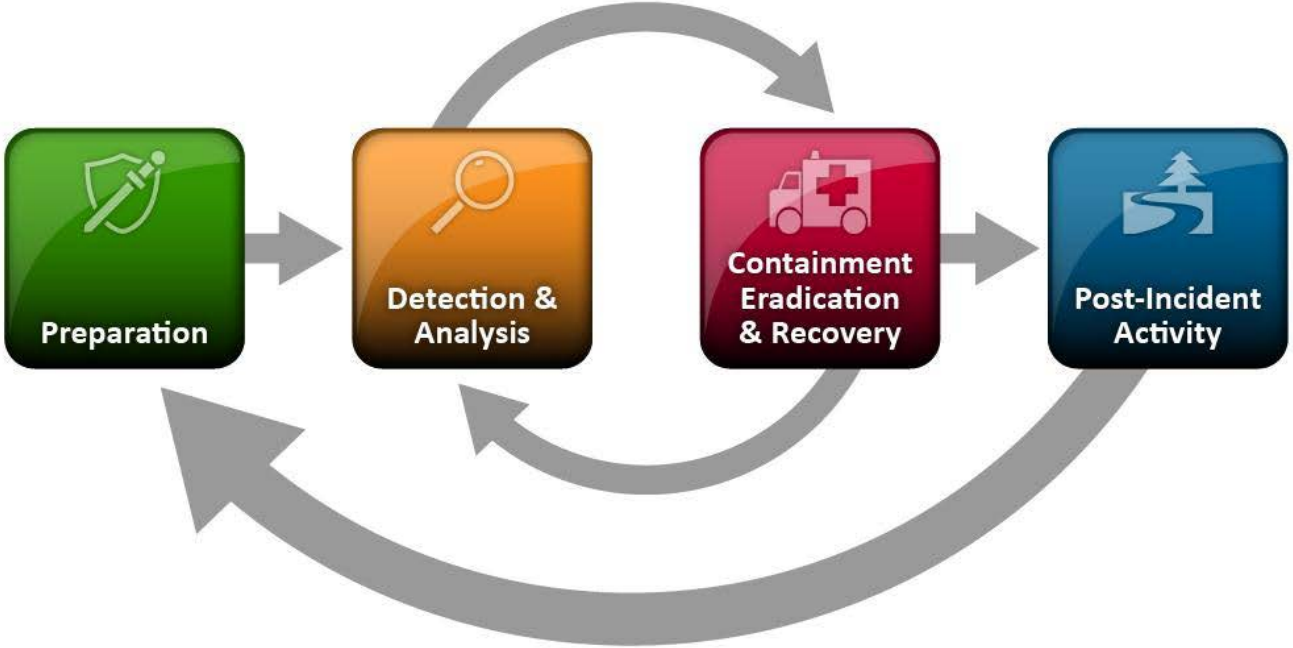
- Documentation…
  - Network diagrams
  - **Critical information/data inventory**
  - Configuration files (routers/firewalls)
  - System build/configuration standards
  - Sources of key data (logs)
  - System baselines/normal behavior
  - Business partner/vendor inventory
    - ◊ Responsibility Matrix

Boy Scouts – Be Prepared?

- Proactive
  - Standards based IT Ops
  - Harden your systems
  - Exception management
  - Monitoring and Threat Intelligence
  - Test and Practice

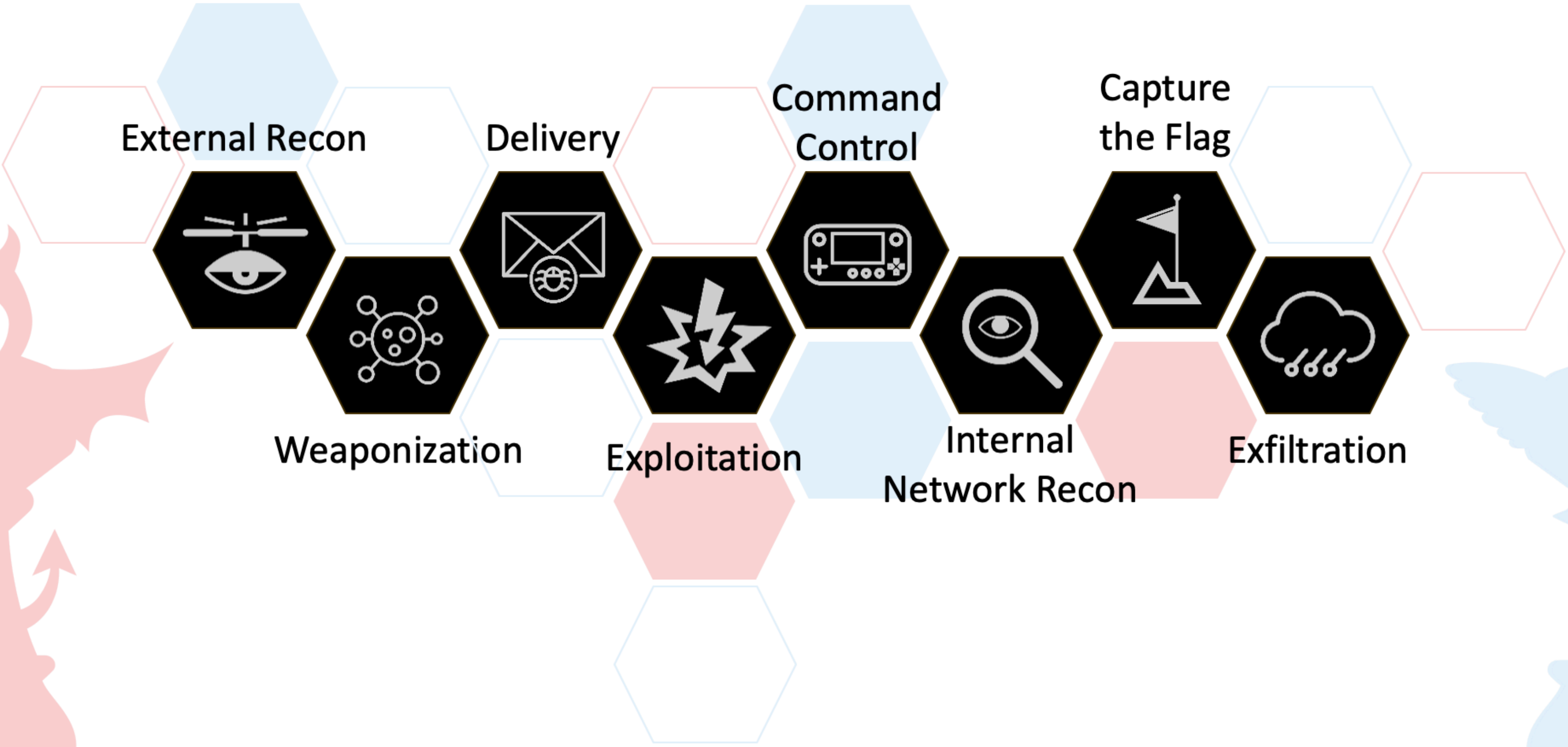
- Reactive
  - Playbook ready
  - Up to date documentation
  - Tuned monitoring and alerting
  - Defined communication and escalation

Incident Response Life Cycle (NIST 800-61)



Incident Response Life Cycle

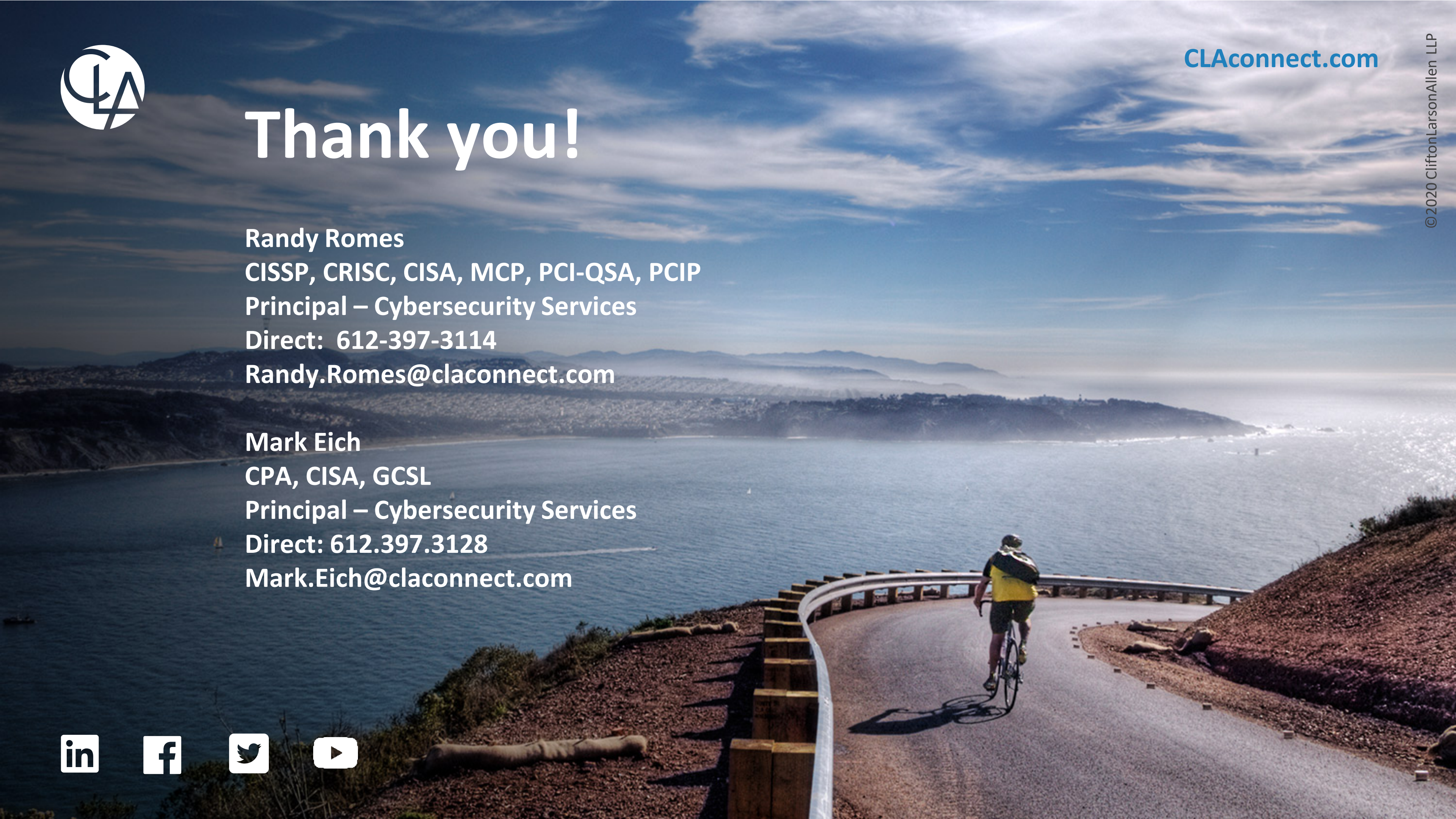
The Cyber Kill Chain



Boy Scouts – Be Prepared?

- Not IF, but WHEN…practice, practice, practice…
  - Test incident response periodically (just like DRP testing)
    - Tabletop exercises (NIST 800-61 is your friend!)
    - Penetration testing (NOT vulnerability scanning)
    - Red team/blue team activities
- Feed results of testing back into improvement process
- Include general staff awareness training
  - How to recognize
  - Who to call

Questions?



CLAconnect.com

Thank you!

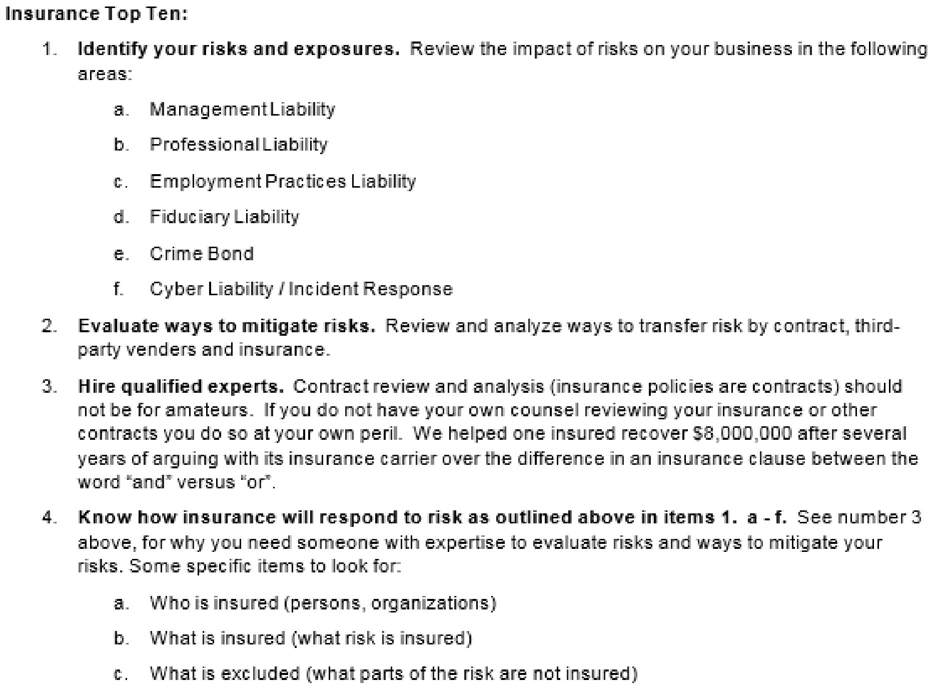
Randy Romes
CISSP, CRISC, CISA, MCP, PCI-QSA, PCIP
Principal – Cybersecurity Services
Direct: 612-397-3114
Randy.Romes@claconnect.com

Mark Eich
CPA, CISA, GCSL
Principal – Cybersecurity Services
Direct: 612.397.3128
Mark.Eich@claconnect.com

Incident Response Resources

Examples and feedback from insurance industry

One example of “Insurance Top Ten”



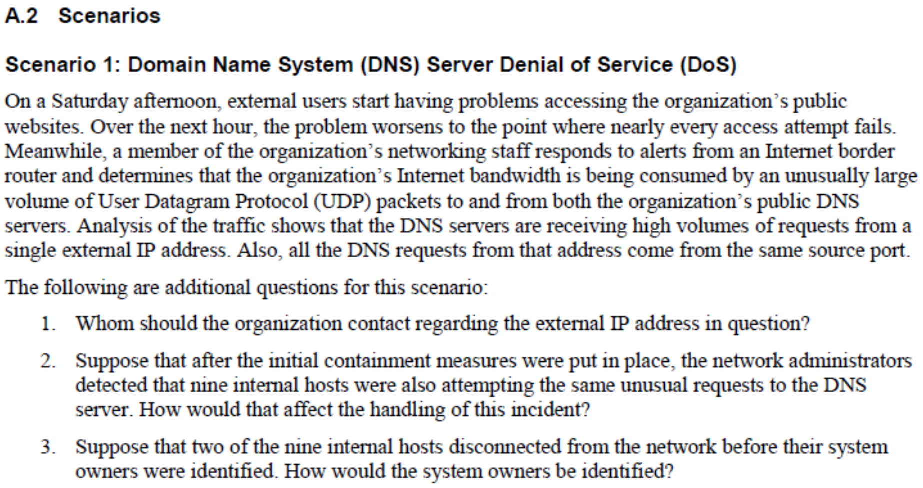
Insurance Top Ten:

1. **Identify your risks and exposures.** Review the impact of risks on your business in the following areas:
    a. Management Liability
    b. Professional Liability
    c. Employment Practices Liability
    d. Fiduciary Liability
    e. Crime Bond
    f. Cyber Liability / Incident Response
2. **Evaluate ways to mitigate risks.** Review and analyze ways to transfer risk by contract, third-party venders and insurance.
3. **Hire qualified experts.** Contract review and analysis (insurance policies are contracts) should not be for amateurs. If you do not have your own counsel reviewing your insurance or other contracts you do so at your own peril. We helped one insured recover $8,000,000 after several years of arguing with its insurance carrier over the difference in an insurance clause between the word "and" versus "or".
4. **Know how insurance will respond to risk as outlined above in items 1. a - f.** See number 3 above, for why you need someone with expertise to evaluate risks and ways to mitigate your risks. Some specific items to look for:
    a. Who is insured (persons, organizations)
    b. What is insured (what risk is insured)
    c. What is excluded (what parts of the risk are not insured)

Incident Response Resources

Examples for tabletop exercise

- Incident handling scenario questions
- Incident handling table top examples
- Eleven examples/samples in NIST 800-61



A.2 Scenarios

Scenario 1: Domain Name System (DNS) Server Denial of Service (DoS)

On a Saturday afternoon, external users start having problems accessing the organization's public websites. Over the next hour, the problem worsens to the point where nearly every access attempt fails. Meanwhile, a member of the organization's networking staff responds to alerts from an Internet border router and determines that the organization's Internet bandwidth is being consumed by an unusually large volume of User Datagram Protocol (UDP) packets to and from both the organization's public DNS servers. Analysis of the traffic shows that the DNS servers are receiving high volumes of requests from a single external IP address. Also, all the DNS requests from that address come from the same source port.

The following are additional questions for this scenario:

1. Whom should the organization contact regarding the external IP address in question?
2. Suppose that after the initial containment measures were put in place, the network administrators detected that nine internal hosts were also attempting the same unusual requests to the DNS server. How would that affect the handling of this incident?
3. Suppose that two of the nine internal hosts disconnected from the network before their system owners were identified. How would the system owners be identified?

Sources for Standards & Guidelines

- FFIEC IT Handbook

  http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/other-policies,-standards-and-processes/incident-response.aspx

- NIST 800-61: Computer Security Incident Handling Guide

  https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

- PCI Requirements

  https://www.pcisecuritystandards.org/documents/PFI_Program_Guide.pdf

- State laws

  http://www.privacyrights.org/data-breach#10

  https://www.steptoe.com/images/content/1/4/v2/140143/SteptoeDataBreachNotificationChart.pdf