CliftonLarsonAllen

Be Prepared: How to Recognize, React, and Respond to a Security Breach

Protecting your network from phishing and ransomware

Housekeeping

- If you are experiencing technical difficulties, please dial: **800-422-3623.**
- Q&A session will be held at the end of the presentation.
  - Your questions can be submitted via the **Questions Function at any time during the presentation.**
- The **PowerPoint presentation,** as well as the **webinar recording,** will be sent to you within the next 10 business days.
- For future webinar invitations, subscribe at CLAconnect.com/subscribe.
- Please complete our online survey.

CPE Requirements

- Answer the polling questions

- If you are participating in a group, complete the CPE sign-in sheet and return within two business days
  - Contact webmaster@CLAconnect.com

- Allow four weeks for receipt of your certificate; it will be sent to you via email

* *This webinar, once recorded, has not been developed into a self study course. Therefore, watching the recording will not qualify for CPE credit.*

About CliftonLarsonAllen

- A professional services firm with three distinct business lines
  - Wealth Advisory
  - Outsourcing
  - Audit, Tax, and Consulting
- More than 4,500 employees
- Offices coast to coast
- Serve more than 1,450 financial institutions

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC.

Speaker Introductions

Randy Romes

Principal, CliftonLarsonAllen

- Information Security Services Group
  - CISSP, CRISC, MCP, PCI-QSA

Chad Nordstrom

Manager, CliftonLarsonAllen

- Digital Forensic Investigator, Lead Incident Handler
  - CFCE, GCFE, GSEC

Learning Objectives

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

- Recognize how your credit union can be infected, and affected, by ransomware
- Identify ways to react and respond to a security breach
- Implement changes to your existing incident response plan, or develop a new plan

Sun Tsu – The Art of War

"If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle."

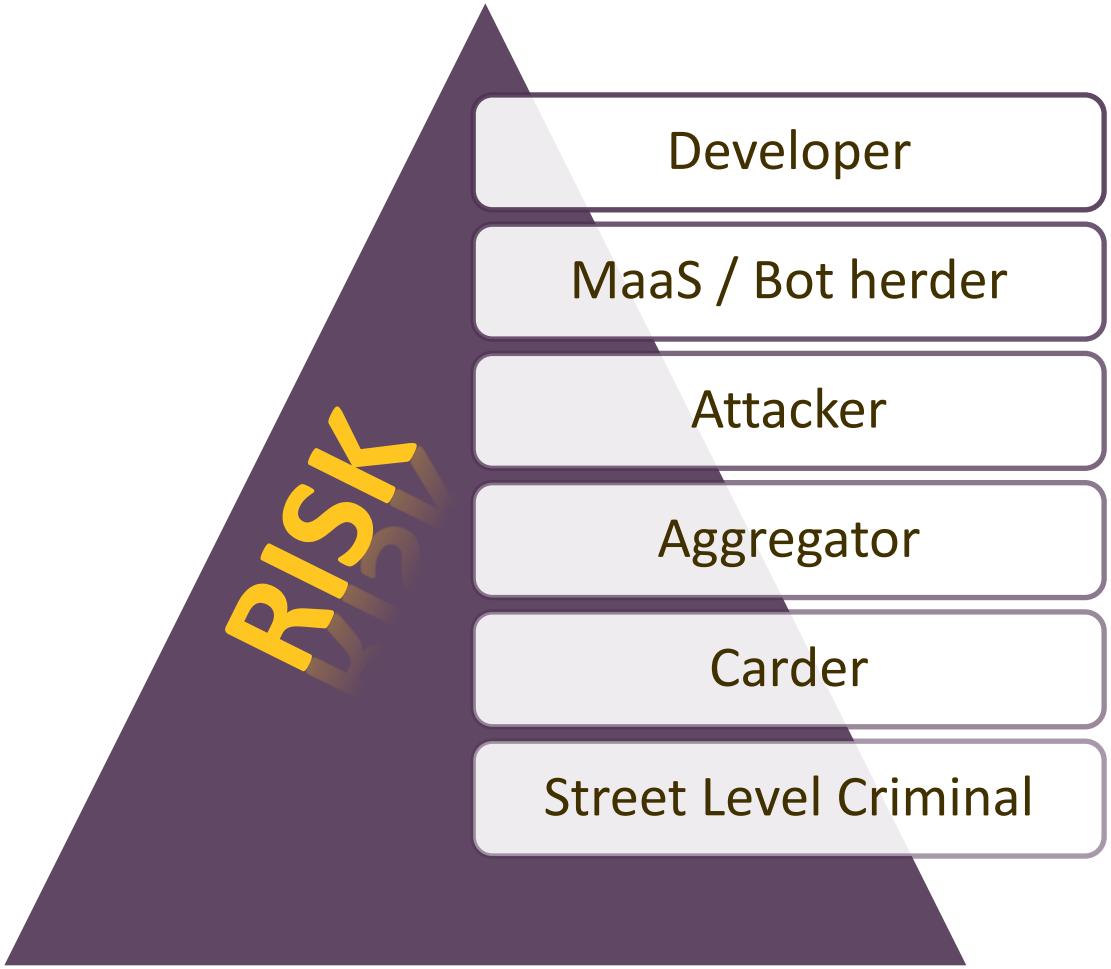
The Threat

Know your enemy

Threat Profile

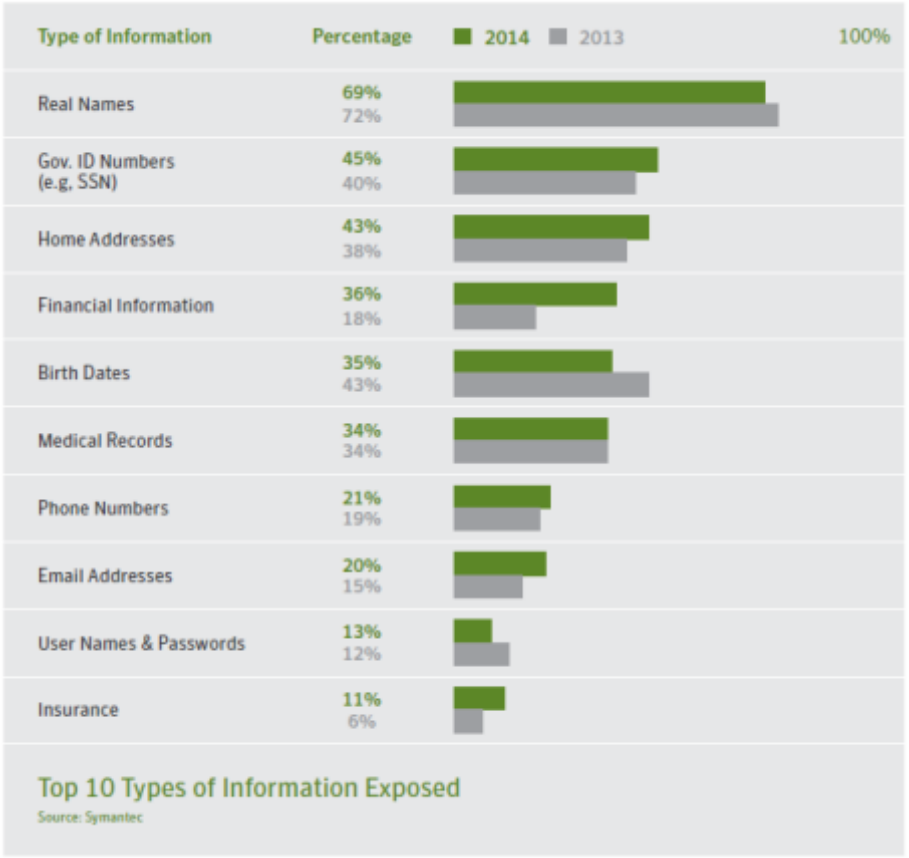
- More diversification
- More sophistication
- More “hands-on” effort
- Specialized targeting
- Increased specialization
- Cost / Benefit analysis

Specialization



What do they want?

- Social statement
- Notoriety
- Moonlighting
- Any data has value
- “Low hanging fruit”



How do they get in?

- Email Phishing
  - "Spear Phishing"
- Malware
  - targeted
  - ransomware
- Poor Configuration
- Social Engineering
- Employees

Email Phishing Objectives

Goals:

- Gain access to your network resources
- Get you to do something

Malware infection via:

- Links to malicious website containing drive-by malware
- Email Attachments (.exe, .zip, .doc, .pdf, etc…)
- Downloading a malware from a website

Gain information by:

- User credentials submitted into a compromised website
- Ask the user

Protecting Yourself

- Most breaches or malware infections start from one of two scenarios
  - Phishing email
  - Browsing to a compromised/malicious website

- It is important to learn how to identify if the email message or the website are legitimate and safe

Types of Email Phishing

Traditional Email Phishing

A hacker sends a email to a large amount of people (from hundreds to millions), hoping a few will take the bait.

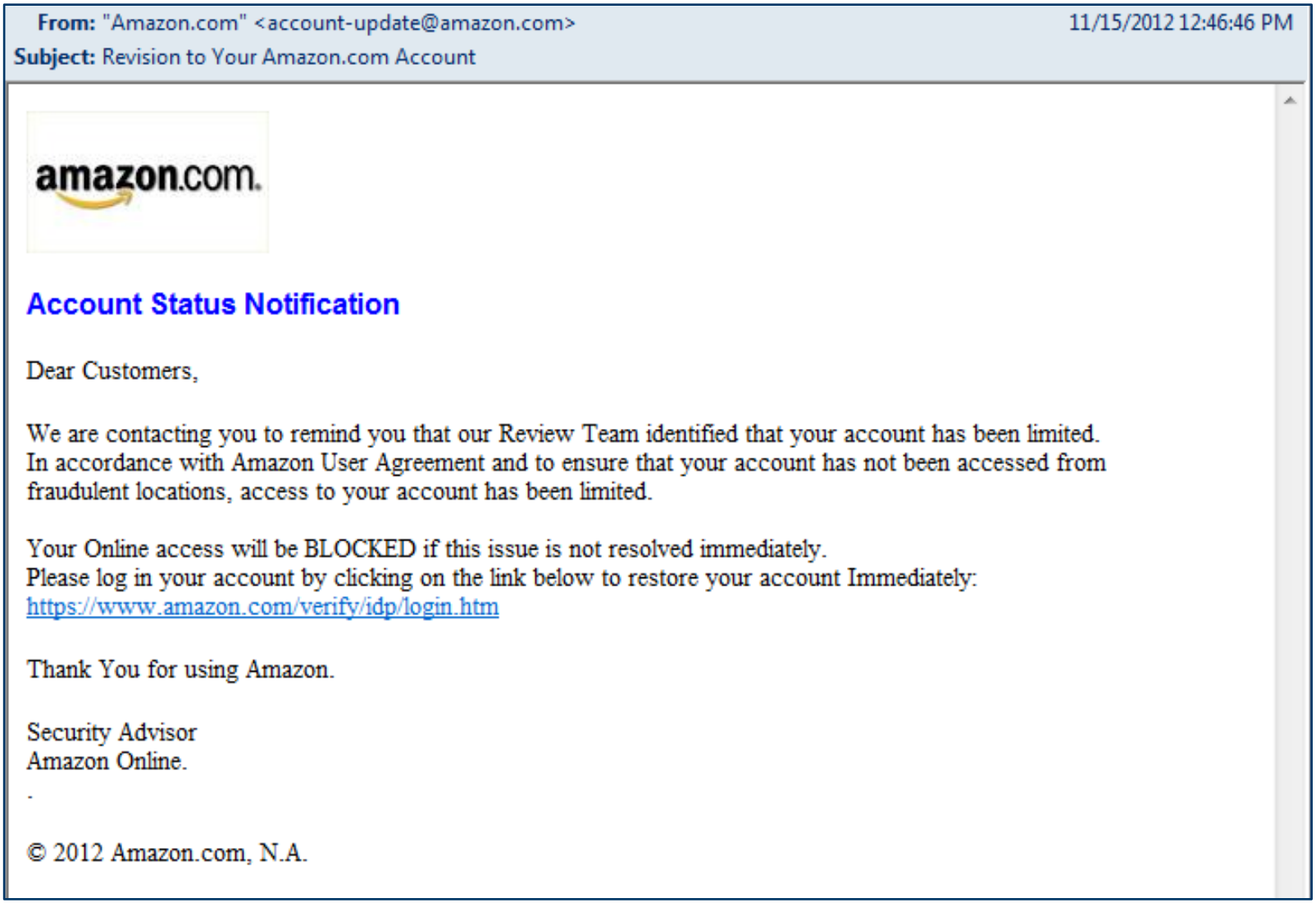
Spear Phishing

A specific target is identified and a custom message is sent.

Whaling

A specially crafted message is sent to the executives or upper management of a business.

Spotting a Malicious Link



From: "Amazon.com" <account-update@amazon.com> 11/15/2012 12:46:46 PM
Subject: Revision to Your Amazon.com Account

amazon.com.

Account Status Notification

Dear Customers,

We are contacting you to remind you that our Review Team identified that your account has been limited.
In accordance with Amazon User Agreement and to ensure that your account has not been accessed from fraudulent locations, access to your account has been limited.

Your Online access will be BLOCKED if this issue is not resolved immediately.
Please log in your account by clicking on the link below to restore your account Immediately:
https://www.amazon.com/verify/idp/login.htm

Thank You for using Amazon.

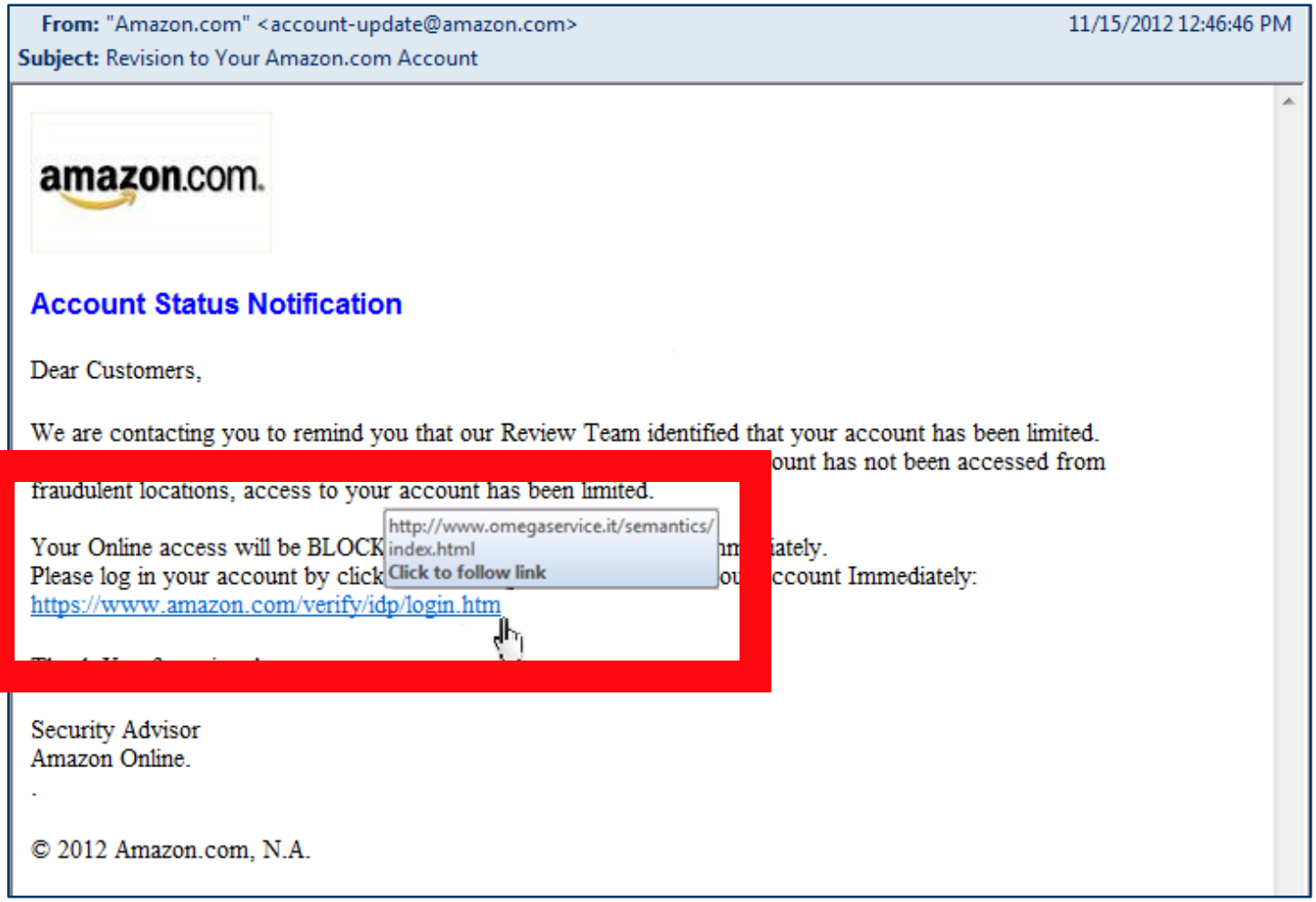
Security Advisor
Amazon Online.
.

© 2012 Amazon.com, N.A.

The link requests the user to visit a website to perform account maintenance.

Uncovering a Malicious Link

1. Hovering over a link with your mouse will show the true path of an email link.



2. This link appears to go to Amazon but is actually going to a malicious site.

Spoofed Internal Source

- Hackers are becoming more sophisticated with their email phishing attacks everyday.

- It is becoming more common for an email phishing message to appear to come from a trusted internal source.

Staff Security Awareness

Learning how to identify phishing emails and malicious websites is key to protecting yourself online:

- Don’t trust attachments
- Don’t trust links
- Ensure you are visiting the website you think you are visiting
- Don’t browse the web/check email as an administrator
- If something looks odd…

CHECK IT BEFORE YOU CLICK IT!

Inevitable

It is not a matter of IF… only WHEN

Boy Scouts Motto: ***Be Prepared!***

The goal is to quickly:

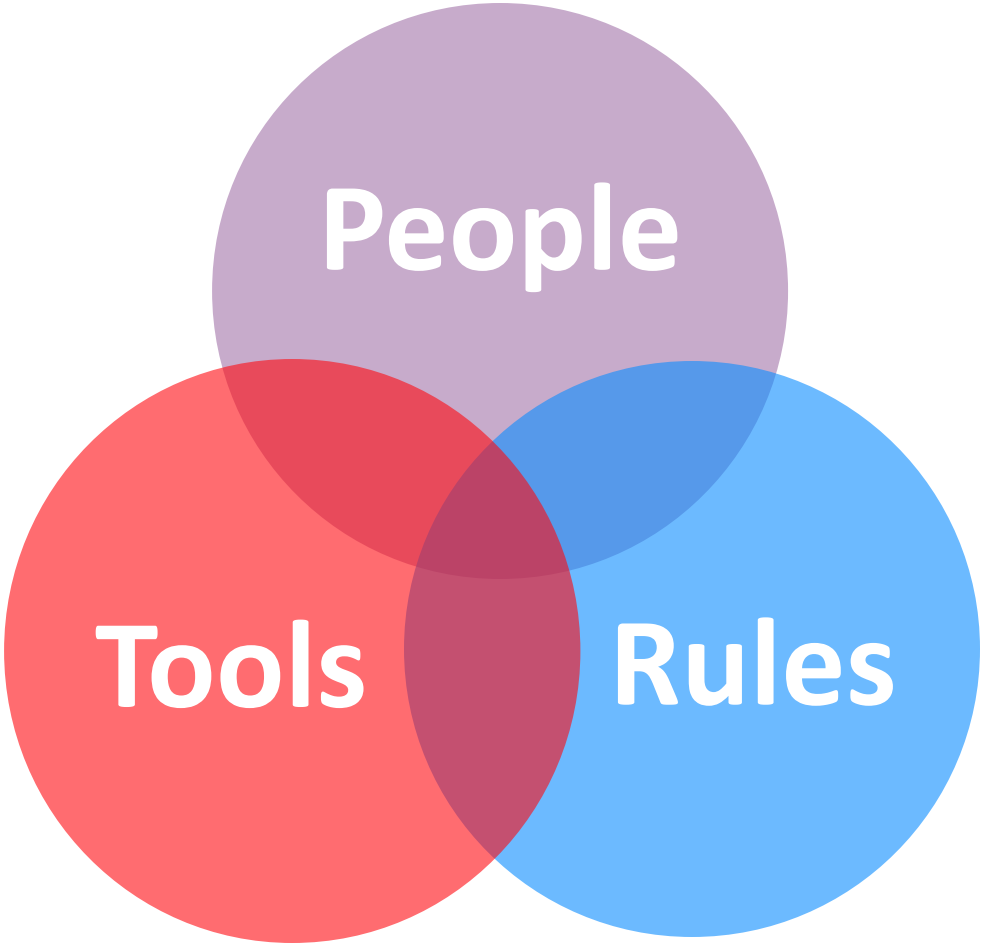
- Detect
- Remove
- Remediate

Preparation

Know yourself

How well do you know your network?

Preparation



Security = Culture

*Security is a **BUSINESS** issue, NOT a technical issue!!*

- *Administrative Policies / Procedures*
- *Physical Access Controls*
- *Technical Security Controls*

PEOPLE

Who is on the wall?

Are they prepared?

Do they understand their role?

Incident Response

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

Why do we expect our IT staff to handle incidents with no training or tools?

Fire Team Paradigm

Concepts

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

Does this look like your team?

Does it feel like this?

Or is this more of the reality?

RULES

- Do our policies and procedures support our:
  - Mission?
  - Vision?
  - Reality?

- Do our staff understand them?

- Are they being followed?

Incident Definition

Criteria:

1. Natural definition
2. Easy to conceptualize
3. Efficient
4. Effective
5. Easy to implement with a small IT department
6. It has to work!

“Incident”

*“An **incident** is any thing that potentially impacts the, Confidentiality, Integrity, or Availability of your network resources.”*

Incident Continuum

Help Desk | Incident | BCP

Incidents can be further subdivided based on the impact.

- Minor
- Major
- Critical

Categorization allows for analysis by management for strategic planning

Communication

Incident Command System

- A standardized approach to the command, control, and coordination of emergency response
- Able to adapt to any complexity and scale
- Cost effective with no duplication of work
- Responders are left to focus on the incident
- Incident Commander coordinates and updates
- Timely and accurate information for management
- Documentation is key

TOOLS

- Do they have the tools to respond?
  - Do they know how to use them?
  - Do they use them enough to be efficient and effective?
- Do they have the knowledge to respond?
  - Do they understand the threats to the network?
  - Are they learning the latest strategies and techniques?

Cyber Insurance

- Increasing in popularity
- Details are important
- What is covered?
  - ✓ 1st Party losses
  - ✓ 3rd Party losses
- Should end up being like health insurance

Ransomware

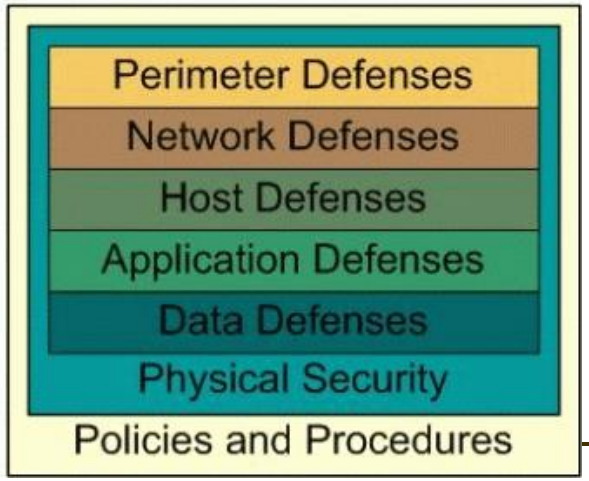
Mitigation Techniques

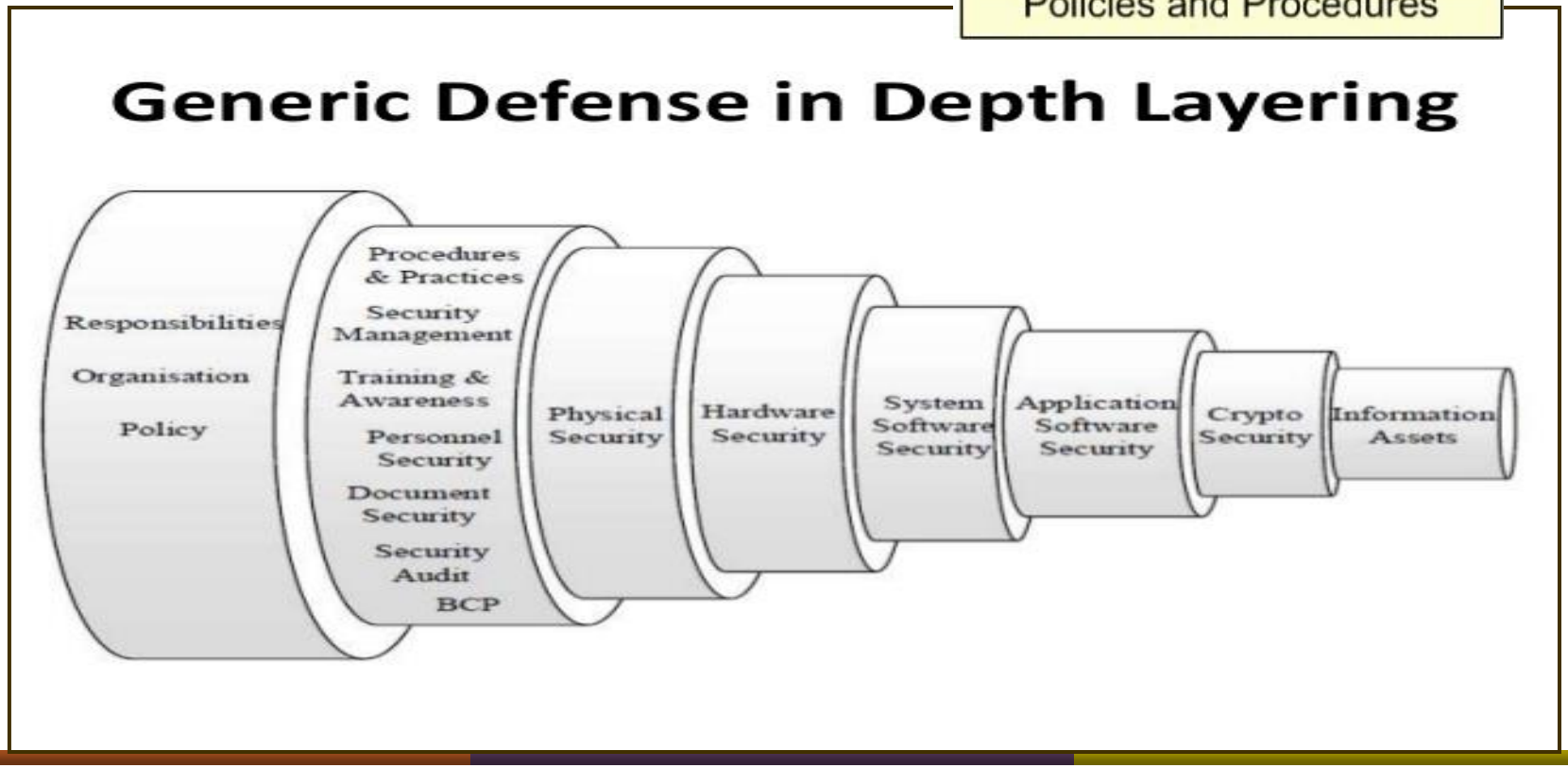
Ransomware

- Attack on the **Availability** of network data
- Easier to do than exfiltration of the data
- Uses strong encryption to render victims files unreadable
- Payments are often in Bitcoin
- Cyber criminals attempt to delete host and network backups
- User credentials are used for network access
- Many variants and constant evolution

Defense in Depth

- Castle Defense
- Layered Defenses
- Applied many ways





Defensive Strategies

- Staff Awareness
  - Education strategies
  - In-service training
- Email Spam Filters
  - Setup
  - Tested
  - Examine spam that gets through
- Removal of ads from the network
  - Webproxy

Defensive Strategies (cont.)

- Software Restriction Policies
  - Not allowing files/DLLs to run in AppData
  - https://technet.microsoft.com/en-us/library/cc759648(v=ws.10).aspx
- Applocker
  - Similar to SRP
- EMET
  - https://technet.microsoft.com/en-us/security/jj653751

Backups

- Best effective response
- Secure your backups
  - Service account
  - Network connection only allowed for backup
  - “Read only”
  - Test your backups

Mitigation

- Employees that are aware and savvy
  - Training
  - Testing
  - Simplify policies
- Resistant and resilient network
  - Defense in Depth
  - More resources for “crown jewels”
  - Backups are the best
- Active Monitoring
  - Understand what is “normal”
  - Detection is critical

Incident Response

Effective and Efficient Response Strategies

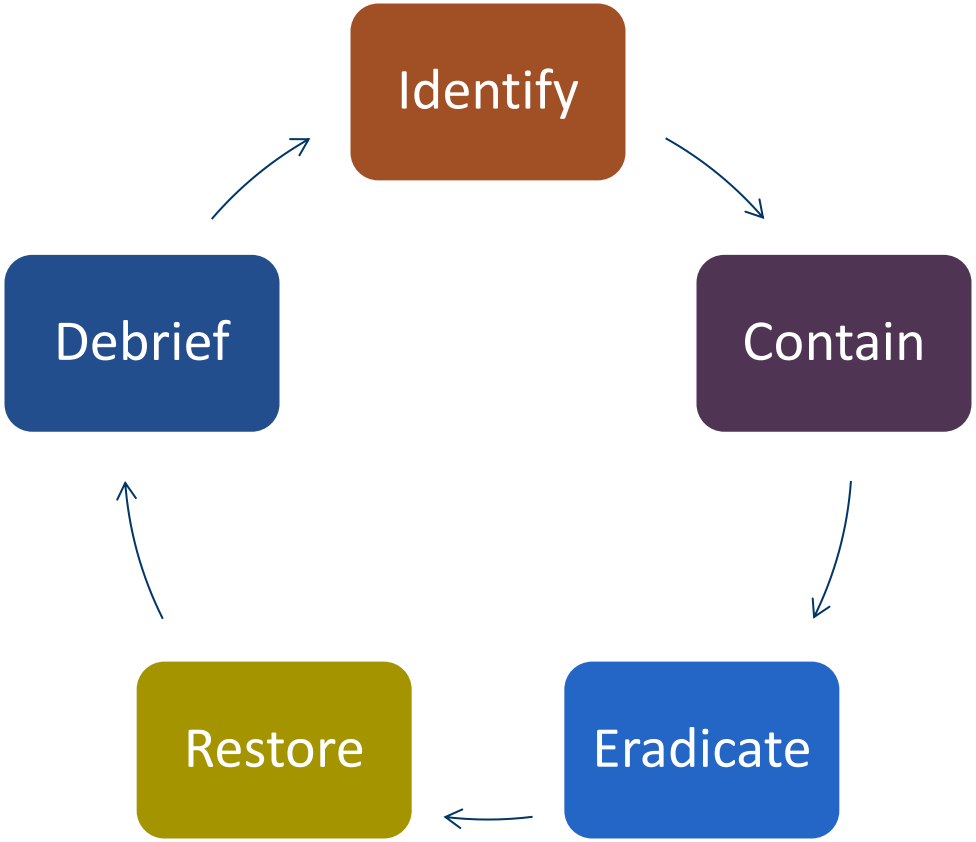
Incident Response Goals

- Plan
- Protect network resources
  - Confidentiality
  - Integrity
  - Availability
- Remediate
- Audit

Plan

- Create an incident response plan
- Establish incident response policies
- Defense in Depth
- Intelligently protect your “crown jewels”
- C.I.A.
  - Confidentiality
  - Integrity
  - Availability

Defense Strategy



Ransomware Investigation

- Remove computers from network
  - Teach staff to remove ethernet jack
- Identify Source
  - Interview the victim
  - Email
    - ◊ Identify others who got the email and delete them
  - Website
    - ◊ Block the IP address from your network
- Review logs for abnormal outbound traffic

Ransomware Analysis

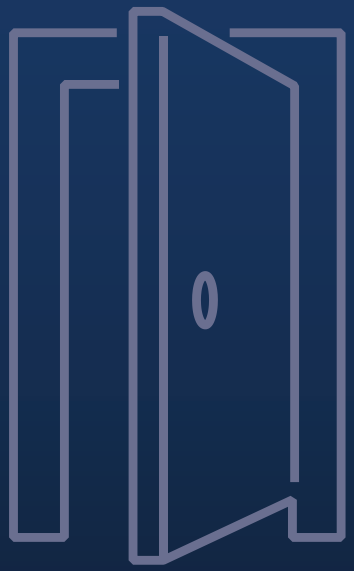
Analyze malware in a test environment

- Regshot
  - ◊ Snapshots the registry (before and after)
- Process Monitor
  - ◊ Records all processes
- Process Explorer (with Symbols and signing set up)
  - ◊ Observe and review processes
- Wireshark
  - ◊ Record and analysis of network traffic

Use that information to respond and remediate

Questions?

Thank you!



Chad Nordstrom, CFCE, GCFE, GSEC
Manager
Information Security Services
chad.nordstrom@CLAconnect.com
888-529-2648

Randy Romes, CISSP, CRISC, MCP, PCI-QSA
Principal
Information Security Services
randy.romes@CLAconnect.com
888-529-2648

CLAconnect.com