What do Carnegie Hall and Good Security Incident Response Plans Have in Common? To get there you have to practice, practice, practice!

CYNERGISTEK

SMITH ANDERSON *expectexcellence*®

Presented by:

Marti Arvin
VP of Audit Strategy

Joe Dickinson
Partner

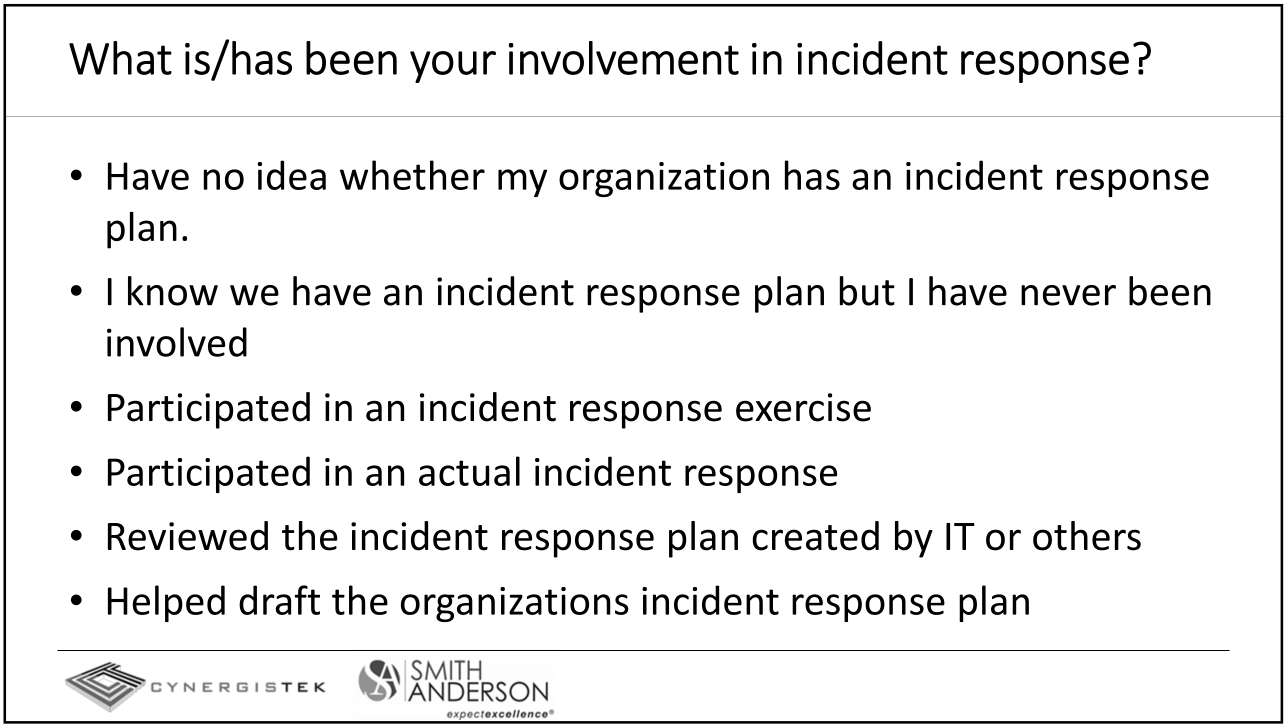
Agenda

1. The Incident Response Plan
2. Planning the Exercise
3. Preparing for the Exercise
4. Practicing Incident Response
5. Wrap-up

Getting to Know You and Incident Response

Who are you?

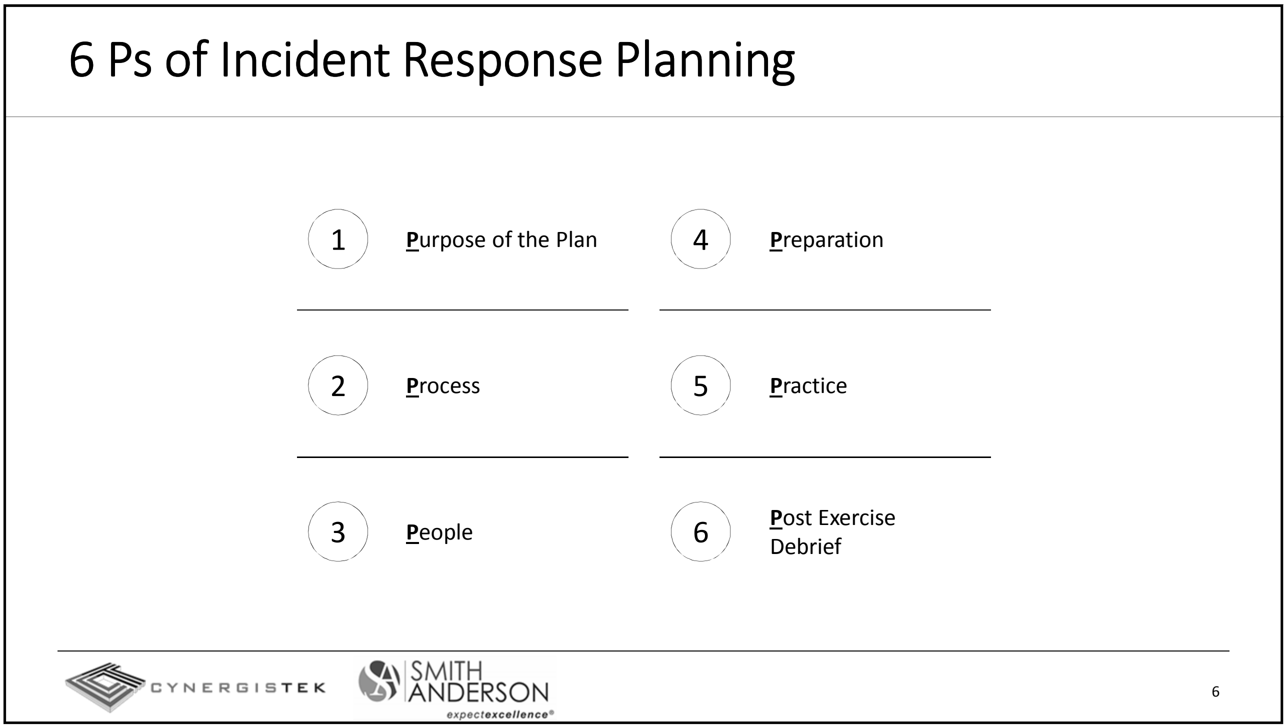
- CCO
- CPO
- CISO
- CIO
- Internal Audit
- General Counsel (internal)
- Counsel (external)
- Consultant
- Other



What is/has been your involvement in incident response?

- Have no idea whether my organization has an incident response plan.
- I know we have an incident response plan but I have never been involved
- Participated in an incident response exercise
- Participated in an actual incident response
- Reviewed the incident response plan created by IT or others
- Helped draft the organizations incident response plan

CYNERGISTEK SMITH ANDERSON expectexcellence®



6 Ps of Incident Response Planning

1 **P**urpose of the Plan

2 **P**rocess

3 **P**eople

4 **P**reparation

5 **P**ractice

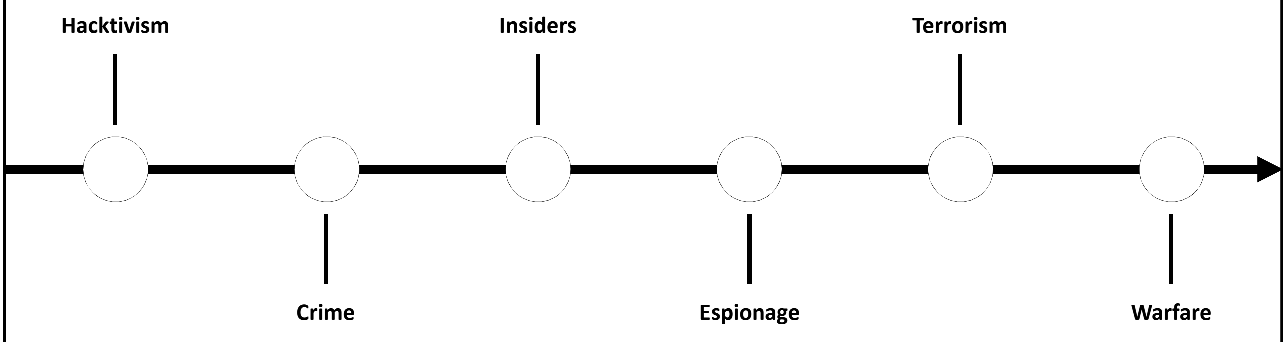
6 **P**ost Exercise Debrief

CYNERGISTEK SMITH ANDERSON expectexcellence®

6

Purpose of the Incident Response Plan

The Cyber Threat Spectrum



Hacktivism

Crime

Insiders

Espionage

Terrorism

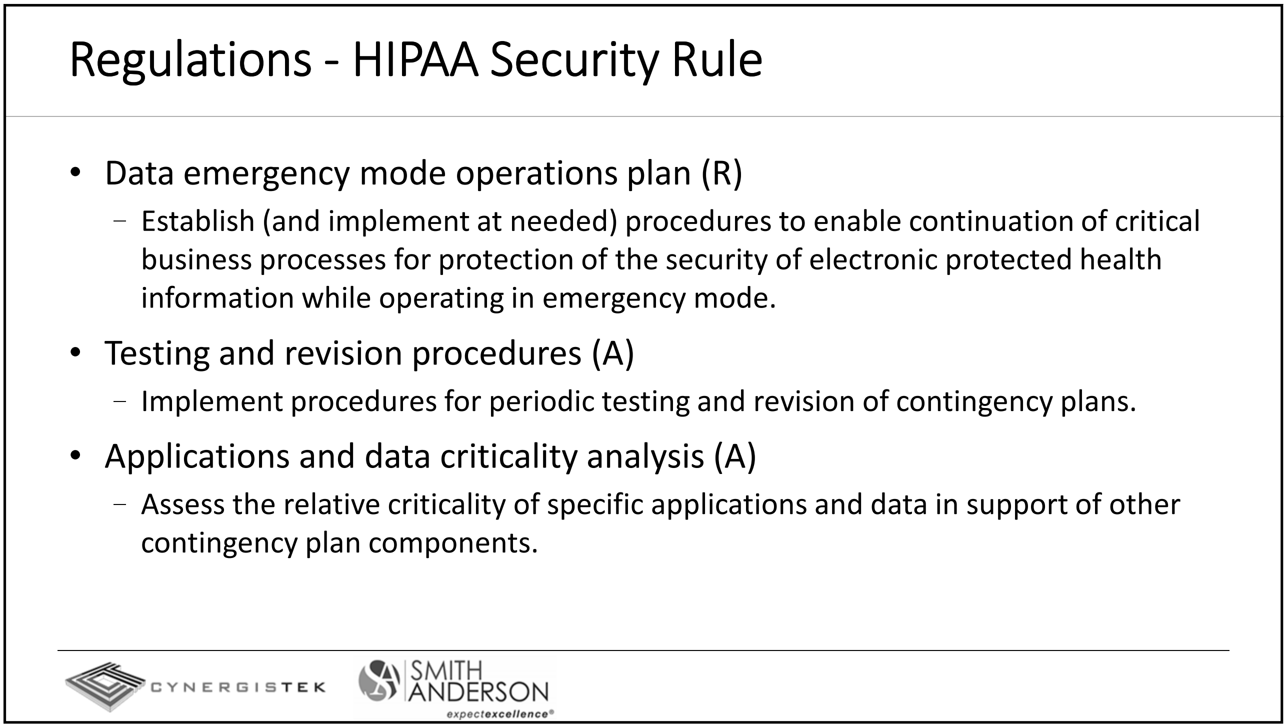
Warfare

Regulations - HIPAA Security Rule

- 45 CFR 164.308(a)(7)(i) Contingency plan
  - Requires P & Ps to respond to an emergency or other occurrence that damages a system containing ePHI including
    - Data back-up plan (R)
    - Disaster recovery plan (R)
    - Emergency mode operation plan (R)
    - Testing and revision procedures (A)
    - Application and data criticality analysis (A)

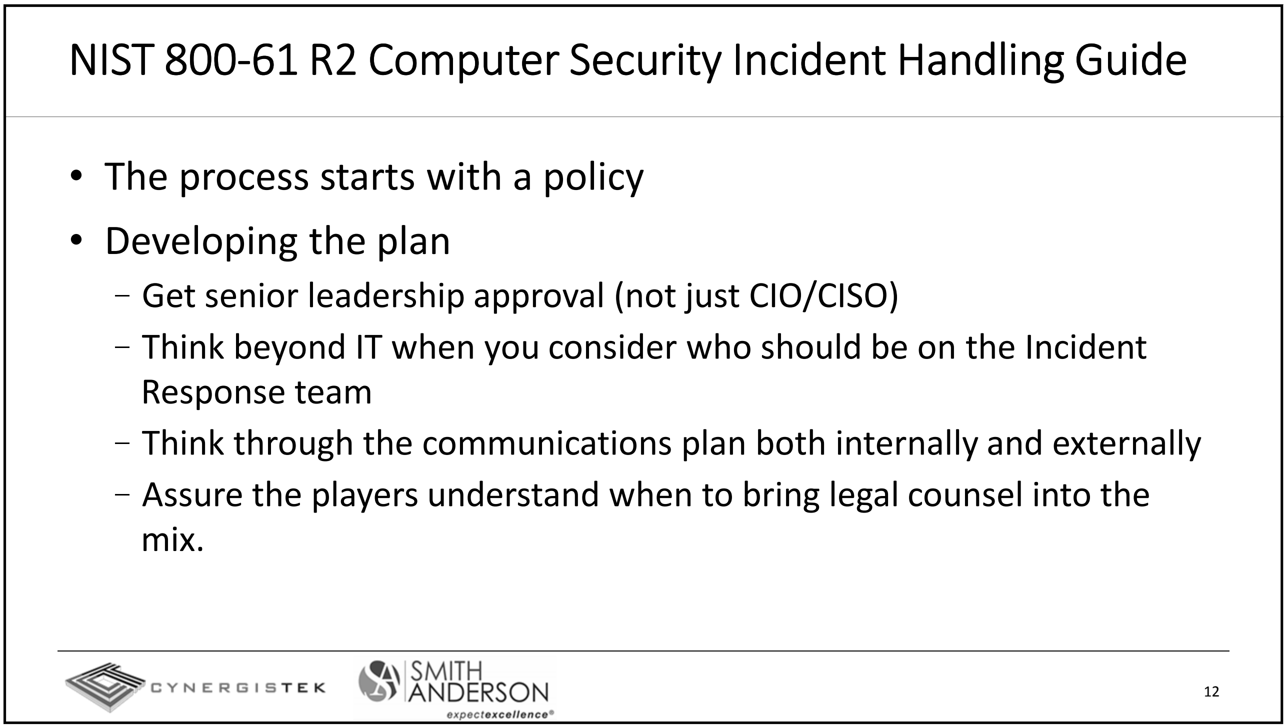
Regulations - HIPAA Security Rule

- Data back-up plan (R)
  - This requires more than just documentation on paper
  - The organization must ”establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.”
- Disaster recovery plan (R)
  - Establish (and implement as needed) procedures to restore any loss of data.



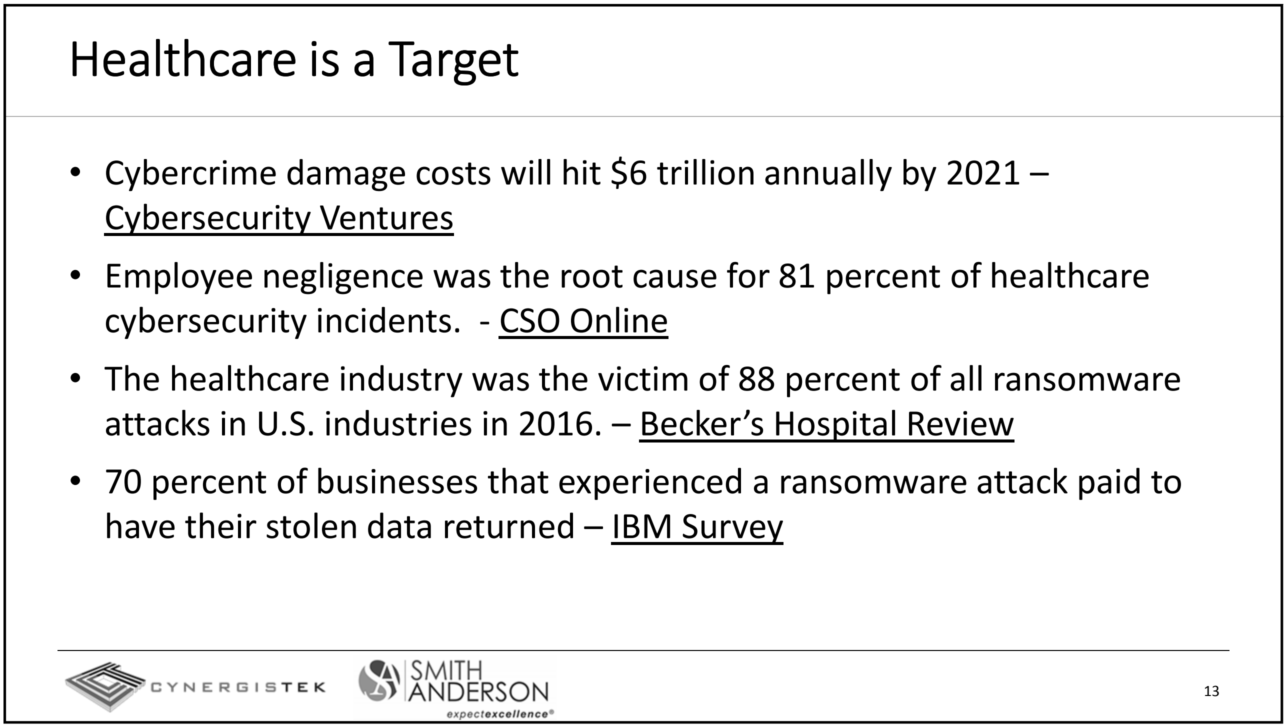
Regulations - HIPAA Security Rule

- Data emergency mode operations plan (R)
  - Establish (and implement at needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
- Testing and revision procedures (A)
  - Implement procedures for periodic testing and revision of contingency plans.
- Applications and data criticality analysis (A)
  - Assess the relative criticality of specific applications and data in support of other contingency plan components.



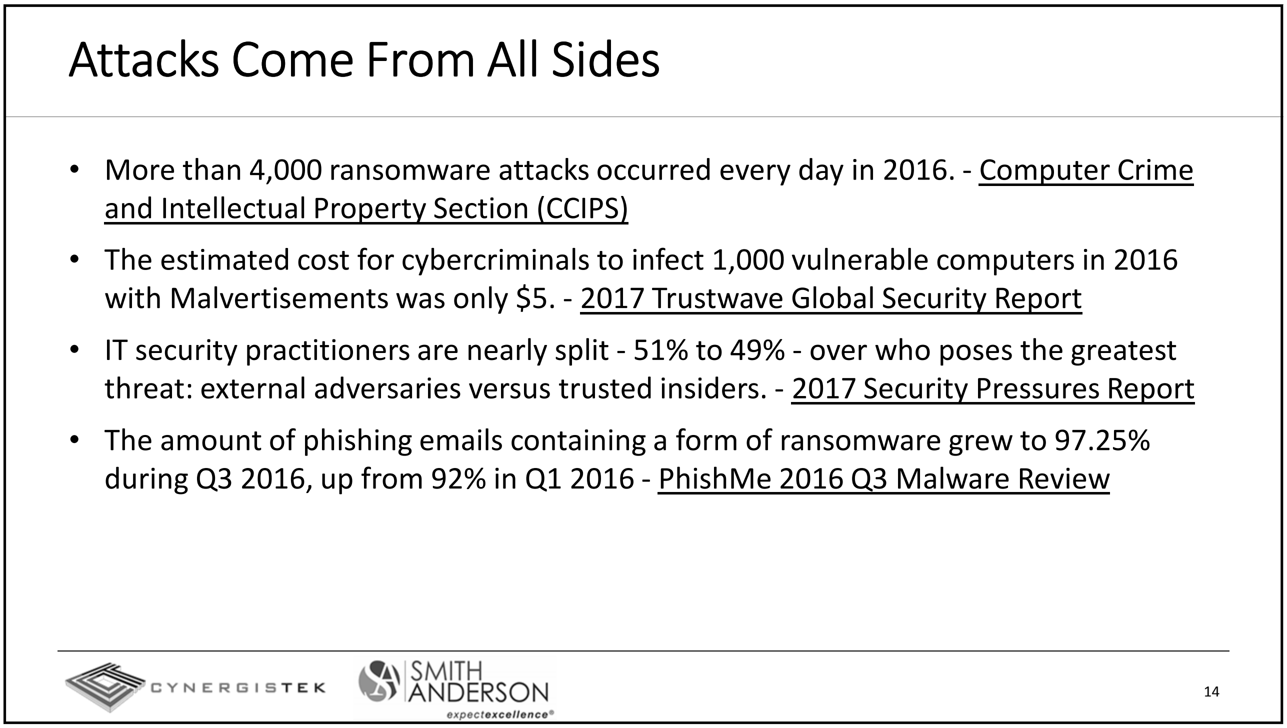
NIST 800-61 R2 Computer Security Incident Handling Guide

- The process starts with a policy
- Developing the plan
  - Get senior leadership approval (not just CIO/CISO)
  - Think beyond IT when you consider who should be on the Incident Response team
  - Think through the communications plan both internally and externally
  - Assure the players understand when to bring legal counsel into the mix.



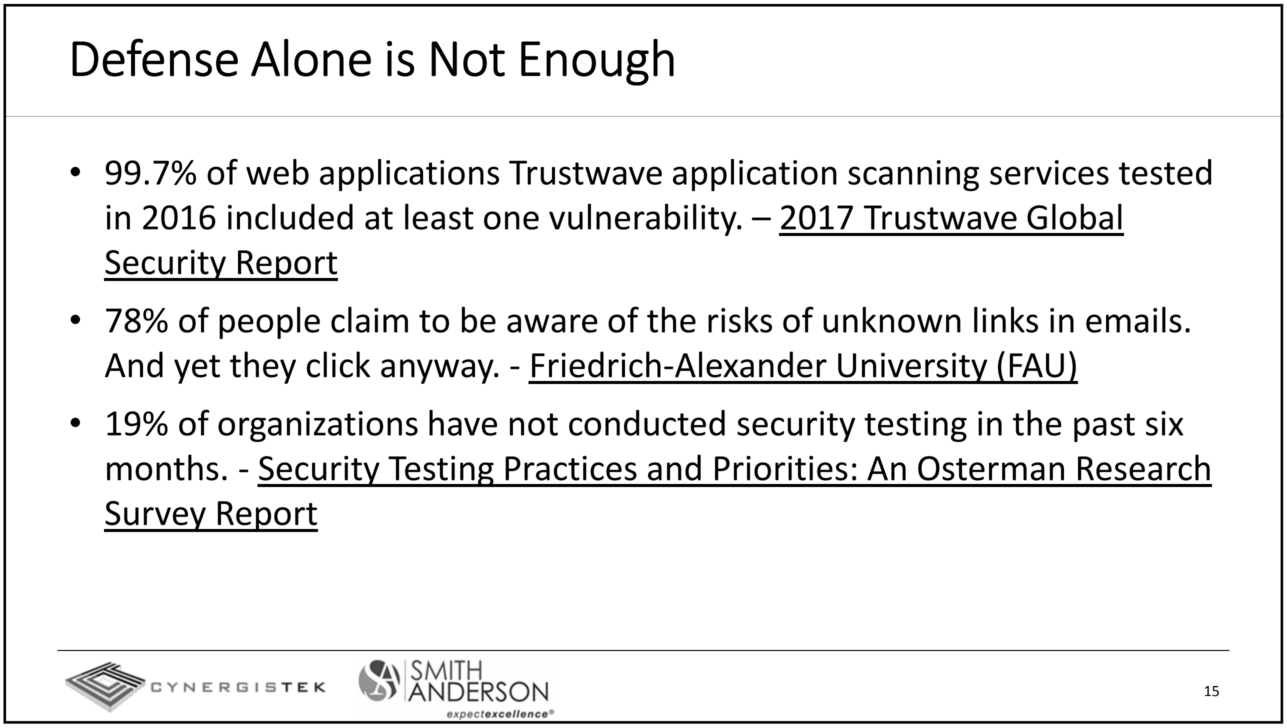
Healthcare is a Target

- Cybercrime damage costs will hit $6 trillion annually by 2021 – Cybersecurity Ventures
- Employee negligence was the root cause for 81 percent of healthcare cybersecurity incidents. - CSO Online
- The healthcare industry was the victim of 88 percent of all ransomware attacks in U.S. industries in 2016. – Becker's Hospital Review
- 70 percent of businesses that experienced a ransomware attack paid to have their stolen data returned – IBM Survey



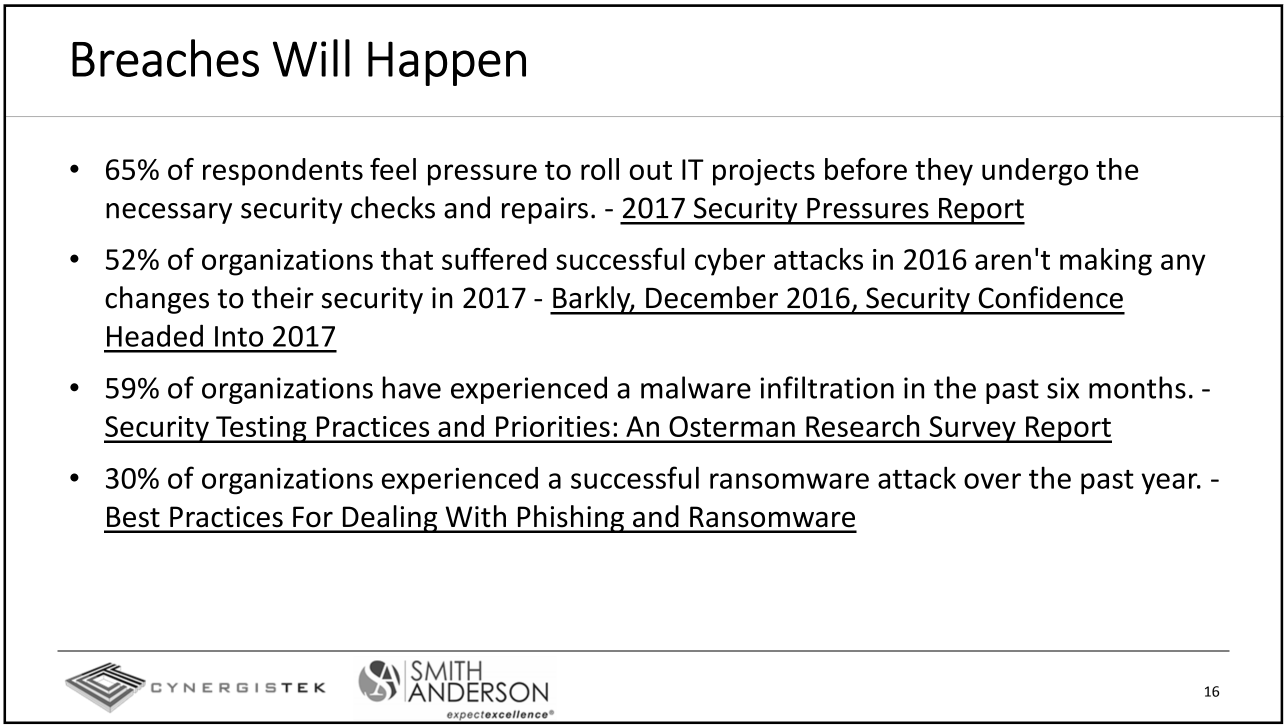
Attacks Come From All Sides

- More than 4,000 ransomware attacks occurred every day in 2016. - Computer Crime and Intellectual Property Section (CCIPS)
- The estimated cost for cybercriminals to infect 1,000 vulnerable computers in 2016 with Malvertisements was only $5. - 2017 Trustwave Global Security Report
- IT security practitioners are nearly split - 51% to 49% - over who poses the greatest threat: external adversaries versus trusted insiders. - 2017 Security Pressures Report
- The amount of phishing emails containing a form of ransomware grew to 97.25% during Q3 2016, up from 92% in Q1 2016 - PhishMe 2016 Q3 Malware Review



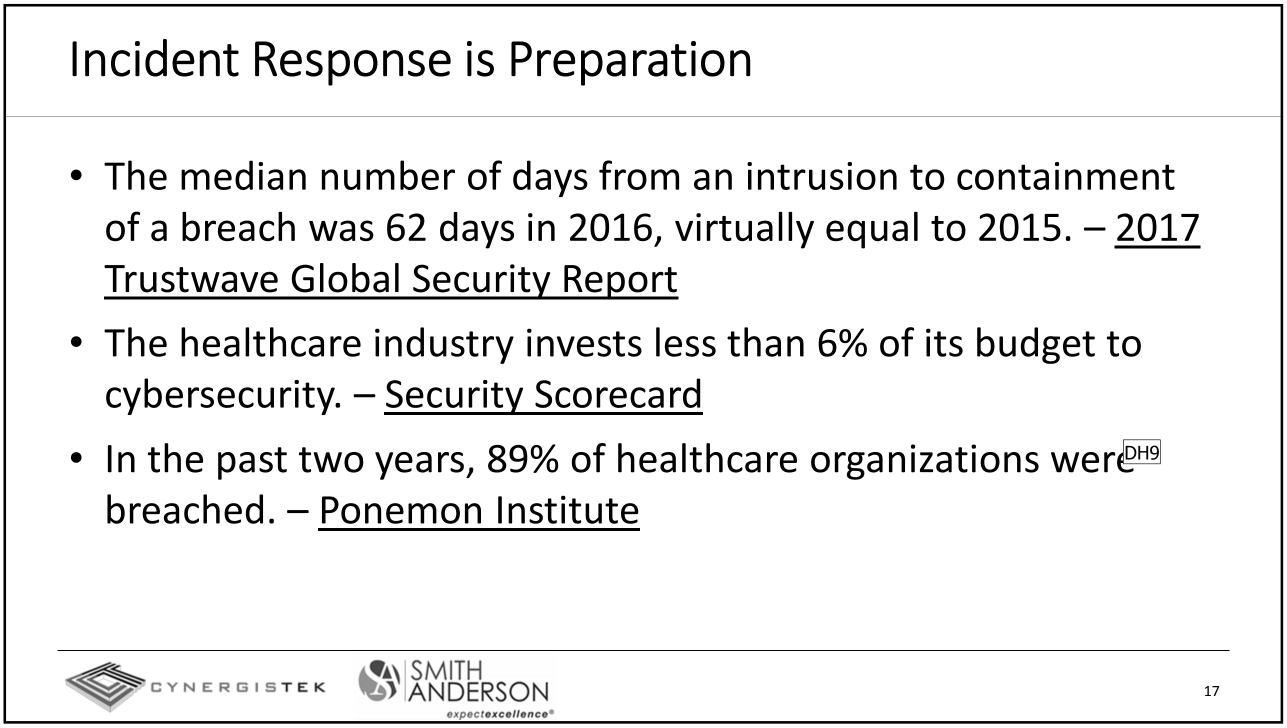
Defense Alone is Not Enough

- 99.7% of web applications Trustwave application scanning services tested in 2016 included at least one vulnerability. – 2017 Trustwave Global Security Report
- 78% of people claim to be aware of the risks of unknown links in emails. And yet they click anyway. - Friedrich-Alexander University (FAU)
- 19% of organizations have not conducted security testing in the past six months. - Security Testing Practices and Priorities: An Osterman Research Survey Report



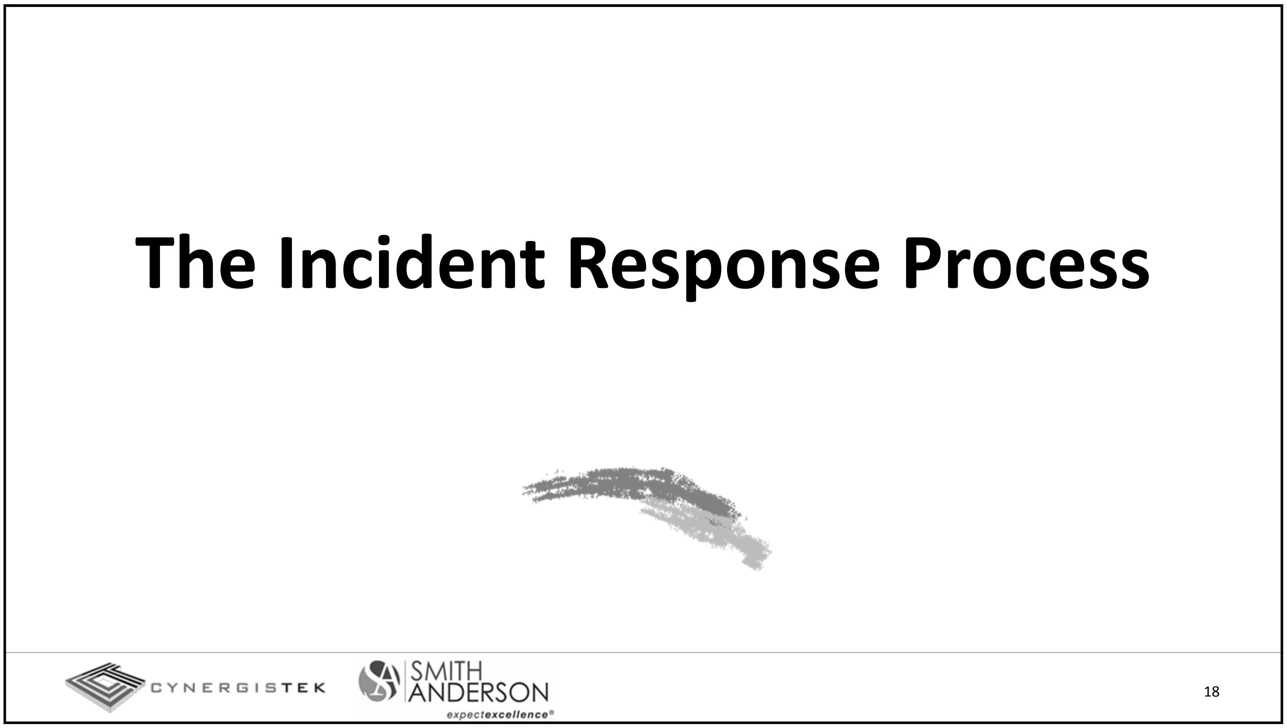
Breaches Will Happen

- 65% of respondents feel pressure to roll out IT projects before they undergo the necessary security checks and repairs. - 2017 Security Pressures Report
- 52% of organizations that suffered successful cyber attacks in 2016 aren't making any changes to their security in 2017 - Barkly, December 2016, Security Confidence Headed Into 2017
- 59% of organizations have experienced a malware infiltration in the past six months. - Security Testing Practices and Priorities: An Osterman Research Survey Report
- 30% of organizations experienced a successful ransomware attack over the past year. - Best Practices For Dealing With Phishing and Ransomware



Incident Response is Preparation

- The median number of days from an intrusion to containment of a breach was 62 days in 2016, virtually equal to 2015. – 2017 Trustwave Global Security Report
- The healthcare industry invests less than 6% of its budget to cybersecurity. – Security Scorecard
- In the past two years, 89% of healthcare organizations were DH9 breached. – Ponemon Institute



The Incident Response Process

Slide 17

DH9 This needs more thought. Ponemon measures breaches from all causes. Also, Poneomon studies are notoriously small samples that do not have statistical significance

David Holtzman, 2/15/2018

Stages of Incident Response Planning

- Plan and prepare
- Detect and report
- Assess and decide
- Respond
- Post-incident activity

Know Some of the Key Factors for Planning and Preparing

- The vocabulary of incident response
- Exercising vocabulary discipline
- Understanding communication under the incident response plan
- An incident response plan will not generally be triggered for a smaller, inconsequential event

Definitions

- **Event** - An observable occurrence of a computer or network activity causing a negative impact
  - Examples:
    - A system is down or slow
    - Server running out of disk space
    - Dead power supply on a critical system
- **Incident** - An event that violates the policy including an event that has potential to lead to data loss, reputation loss, loss of IP, loss of funds or an outage affecting the ability of the firm to do business
  - Examples
    - Misplaced laptop
    - Social engineered transfer of funds to 3rd party
    - Email outage
- **Breach** - An incident that has resulted in the confirmed data loss or exposure
  - Examples
    - Stolen or unaccounted for unencrypted removable media
    - Compromise of a system with resulting in ex-filtration of data
    - The willful improper use of data by an employee

Exercising Vocabulary Discipline

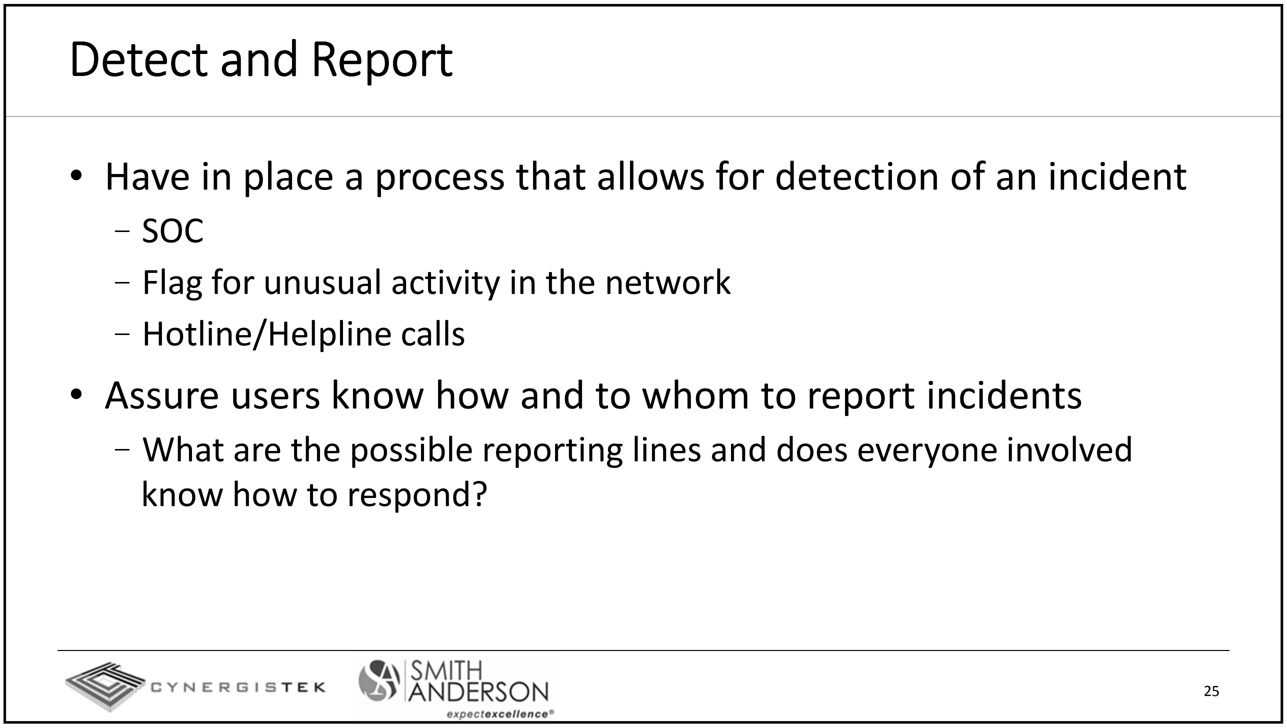
- Repeat, repeat, repeat that an incident does not become a breach and is not referred to as a breach until the party designated to determine if a breach has occurred has done so.
- Train EVERYONE
  - Don’t use the term breach and incident or breach and event interchangeably
    - Especially NOT in any written document

Planning and Preparation

- Each of the steps of an incident response plan must be thought out carefully in advance.
- Compliance and privacy professionals must be aware that this is MORE than just an Information Technology or Information Security question.
- Drafting the plan is not enough
- Testing and improving the plan will make it a meaningful when you need to actually use it

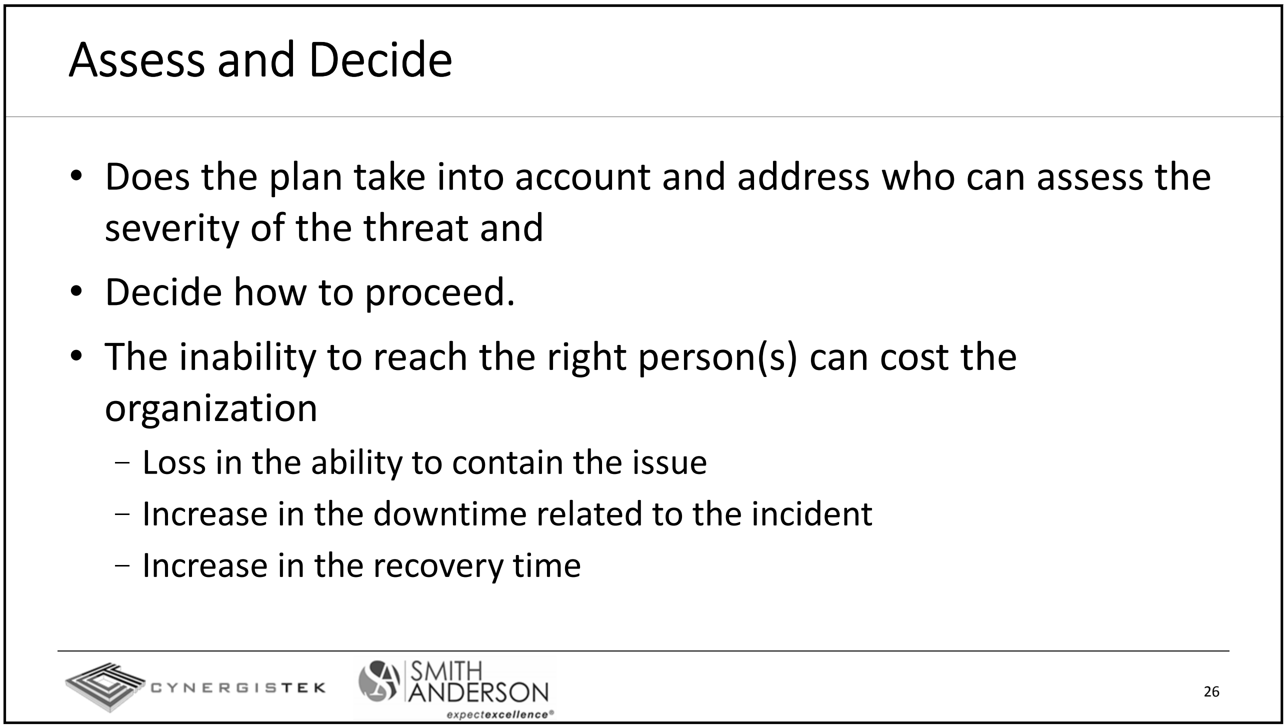
The Incident Response Plan

- Like any plan, an incident response plan is an outline of what needs to be done and by whom and in some instances, when
- What makes a successful IRP?
  - It is well thought out
  - Can be applied to multiple scenarios
  - It so MORE than Information Technology issue



Detect and Report

- Have in place a process that allows for detection of an incident
  - SOC
  - Flag for unusual activity in the network
  - Hotline/Helpline calls
- Assure users know how and to whom to report incidents
  - What are the possible reporting lines and does everyone involved know how to respond?



Assess and Decide

- Does the plan take into account and address who can assess the severity of the threat and
- Decide how to proceed.
- The inability to reach the right person(s) can cost the organization
  - Loss in the ability to contain the issue
  - Increase in the downtime related to the incident
  - Increase in the recovery time

Respond

- Assuring everyone knows how to
  - Respond based on the severity
    - Is a forensic expert needed?
    - Do we contact law enforcement?
  - Recognize when an issue might need to be escalated because the severity has changed
  - Reach all the right players in the appropriate timeframe
    - Do you need the CEO now, in the next hour, sometime today or tomorrow?

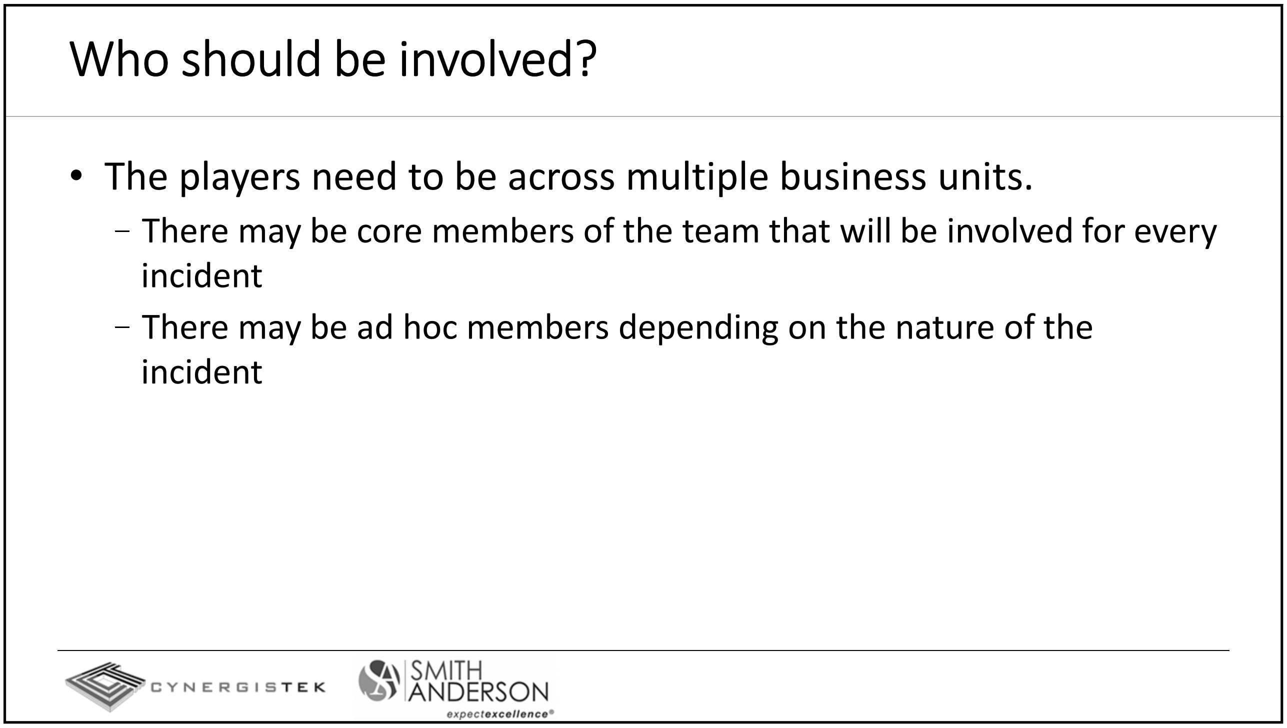
Respond

- Does the organization have the right resources/tools to respond?
  - Hardware/devices
  - Software
  - External support
    - Vendors for forensics
    - Vendors for breach notification assistance
    - Legal expertise
    - General staffing support to maintain reasonable level of operations

Post Incident Recovery

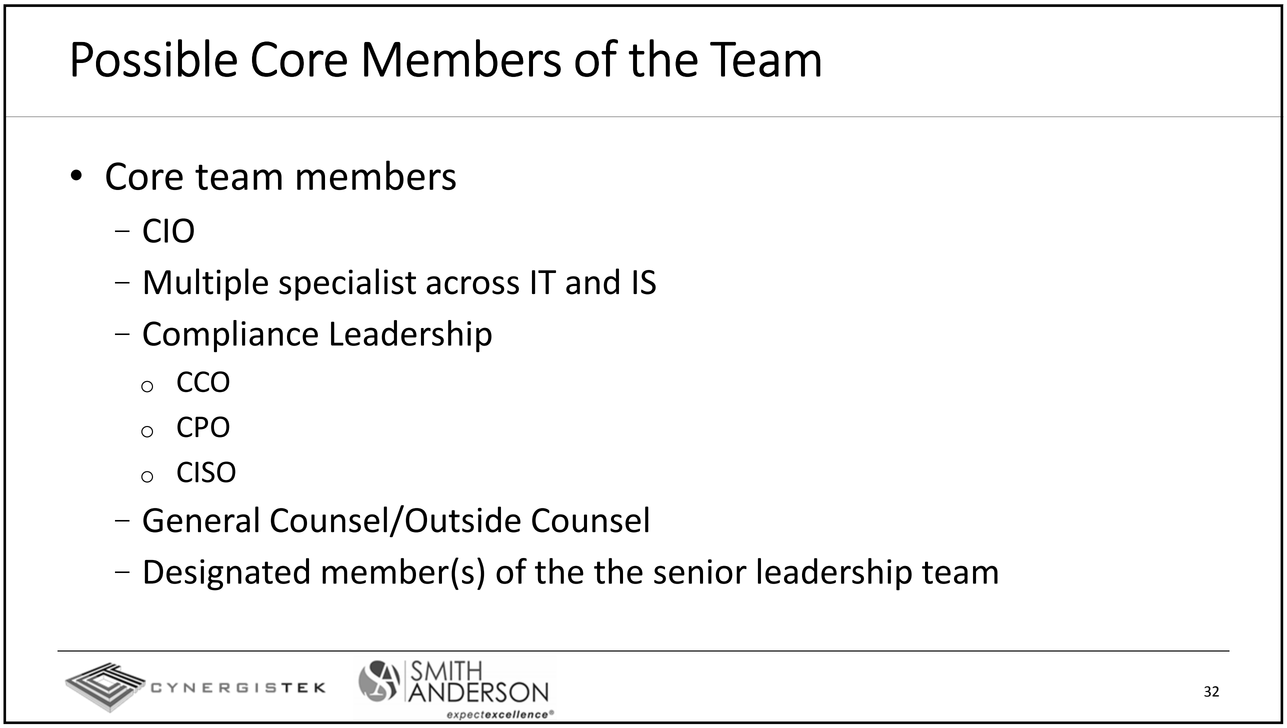
- Getting systems back online in a safe manner
- Conducting an assessment for breach notification
  - Who might we need to notify
    - Patient
    - Regulatory bodies
    - State officials
    - Entities with whom we contract
    - Affiliated business partners

Incident Response People



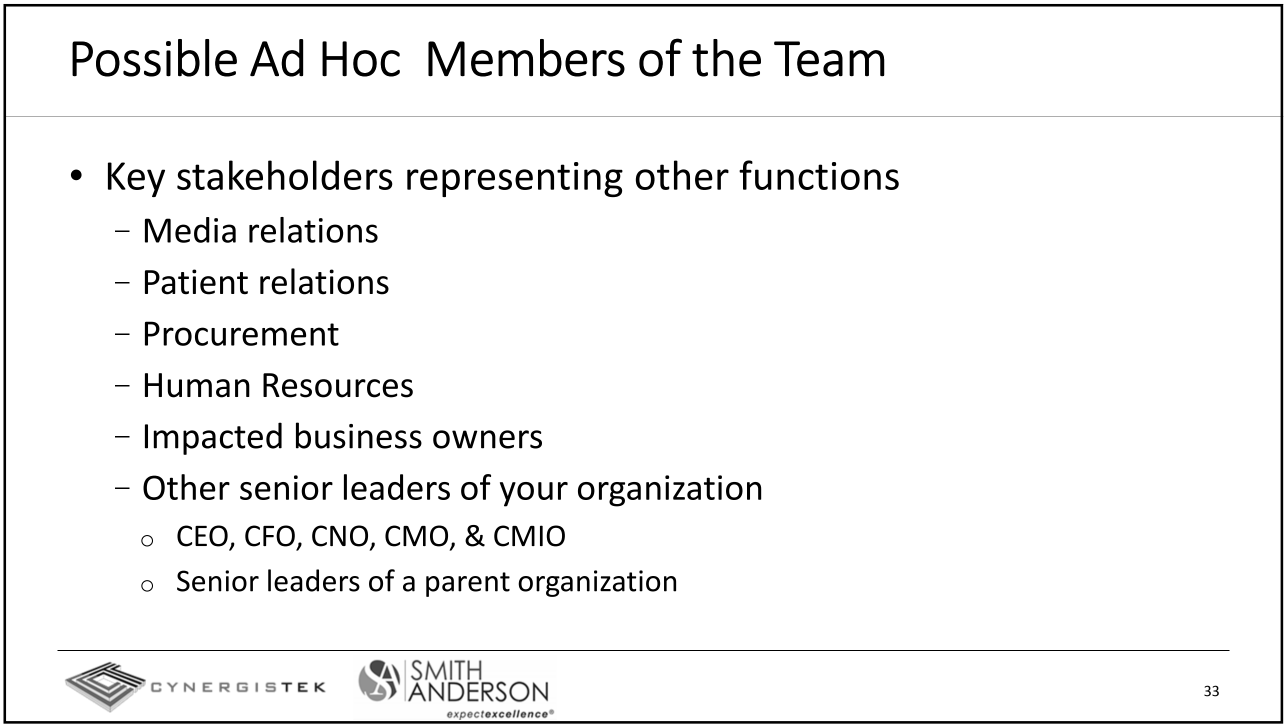
Who should be involved?

- The players need to be across multiple business units.
  - There may be core members of the team that will be involved for every incident
  - There may be ad hoc members depending on the nature of the incident



Possible Core Members of the Team

- Core team members
  - CIO
  - Multiple specialist across IT and IS
  - Compliance Leadership
    - CCO
    - CPO
    - CISO
  - General Counsel/Outside Counsel
  - Designated member(s) of the the senior leadership team



Possible Ad Hoc Members of the Team

- Key stakeholders representing other functions
  - Media relations
  - Patient relations
  - Procurement
  - Human Resources
  - Impacted business owners
  - Other senior leaders of your organization
    - CEO, CFO, CNO, CMO, & CMIO
    - Senior leaders of a parent organization

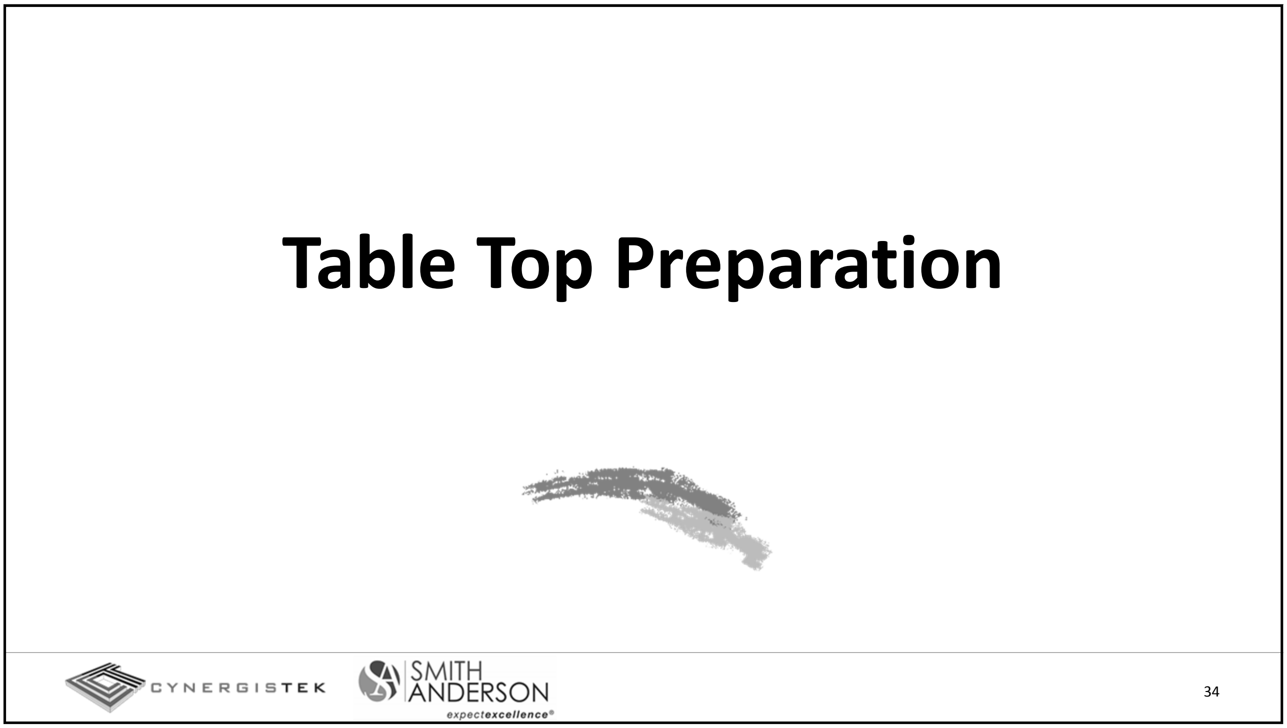
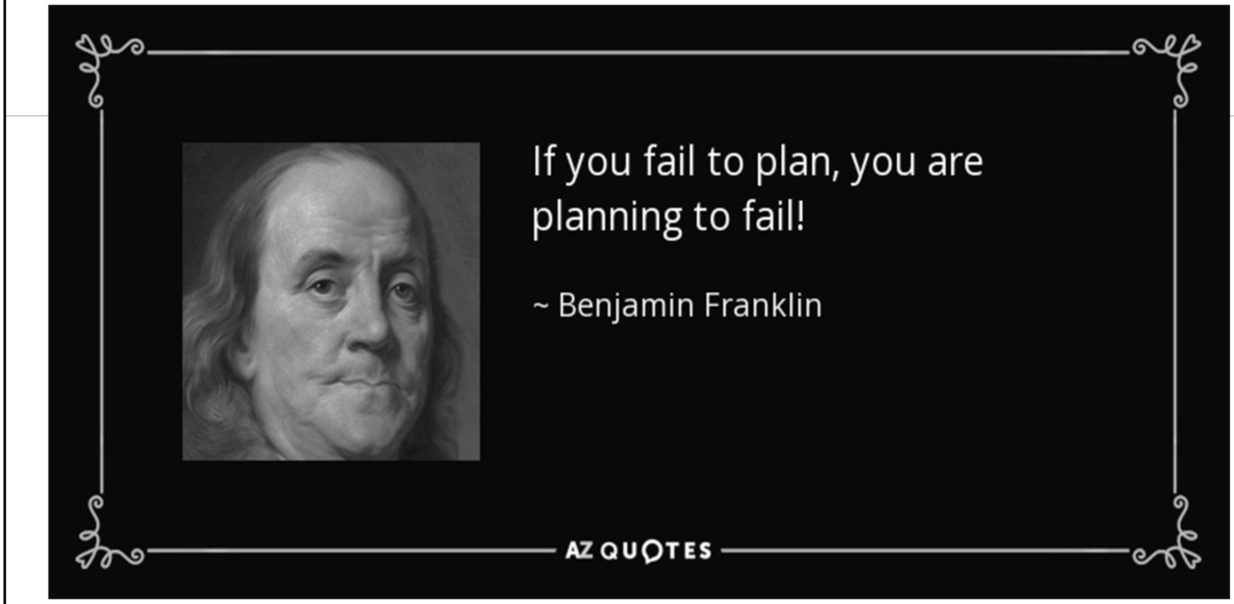


Table Top Preparation



If you fail to plan, you are planning to fail!

~ Benjamin Franklin

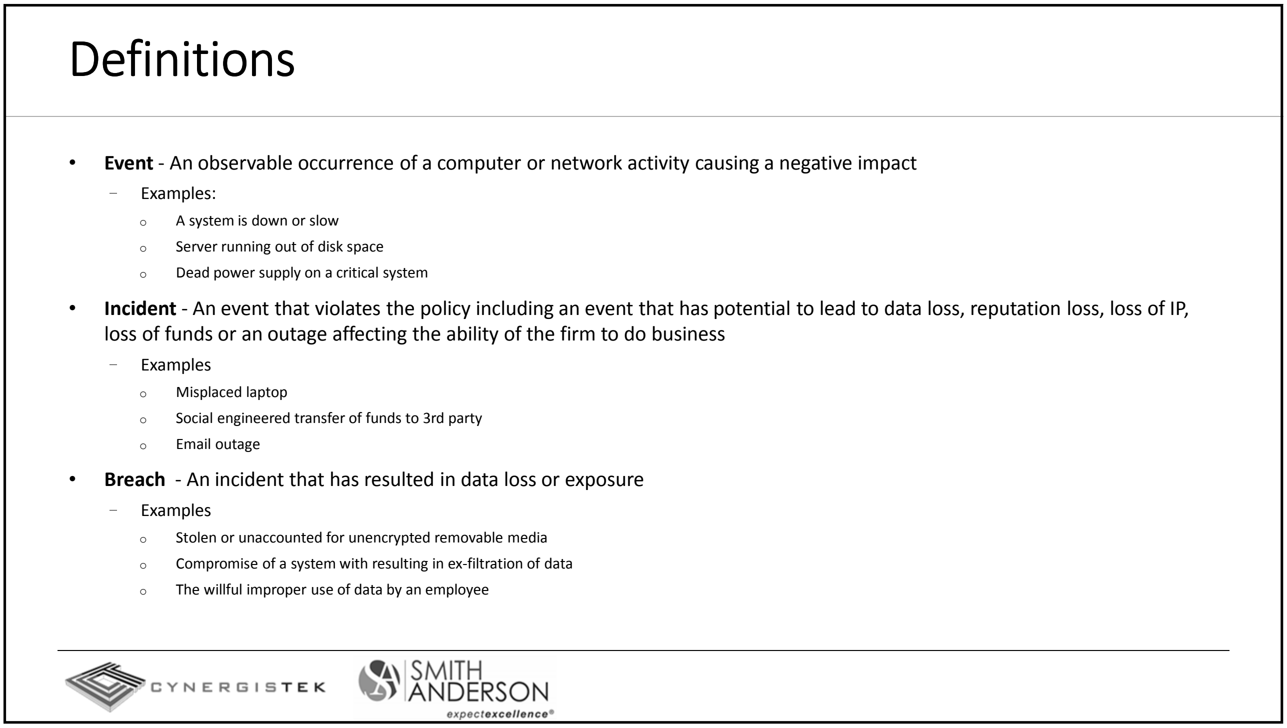
What to Do in Preparation for an IR Exercise

- Have an incident exercise check list
  - Review P & Ps
  - Understand the communication process
    - Who to tell
    - What and when to tell them
  - Review the escalation process
  - Communication about the incident

Incident Response Exercise

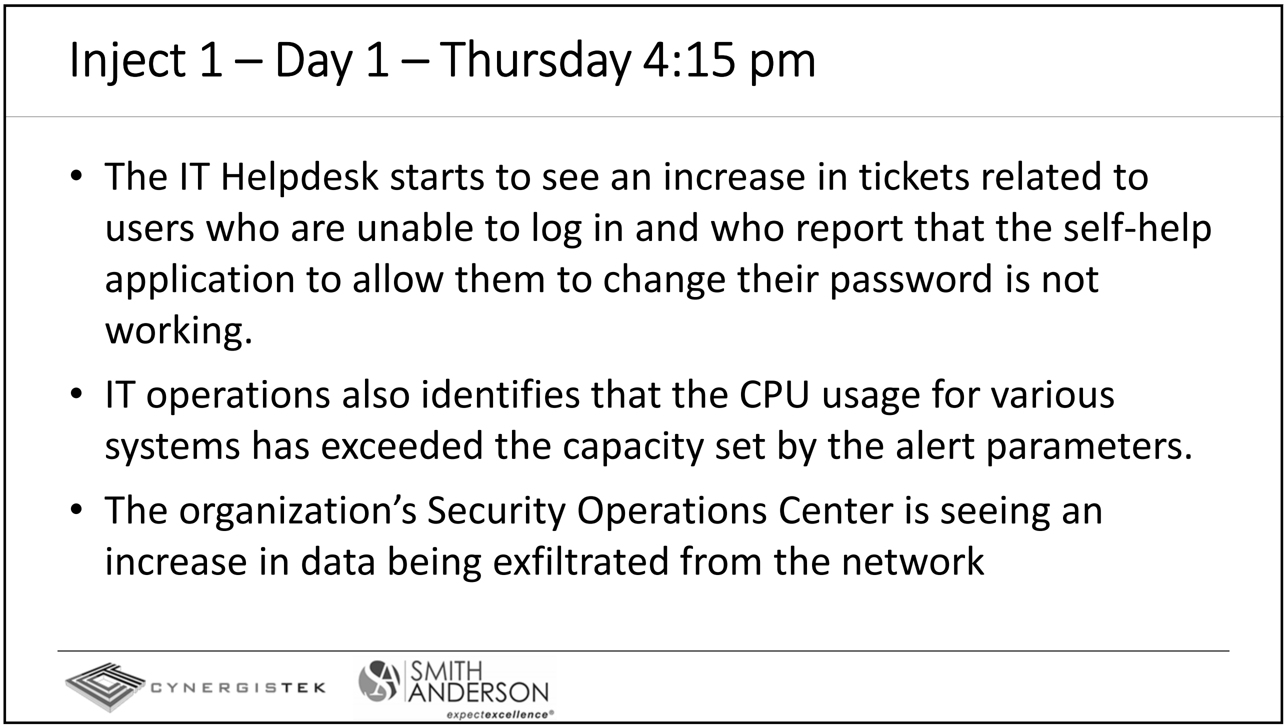
Introduction and Overview

- What is a Table Top Exercise?
- What is your level understanding/experience?
- Definitions
- Actual Exercises
- Debrief



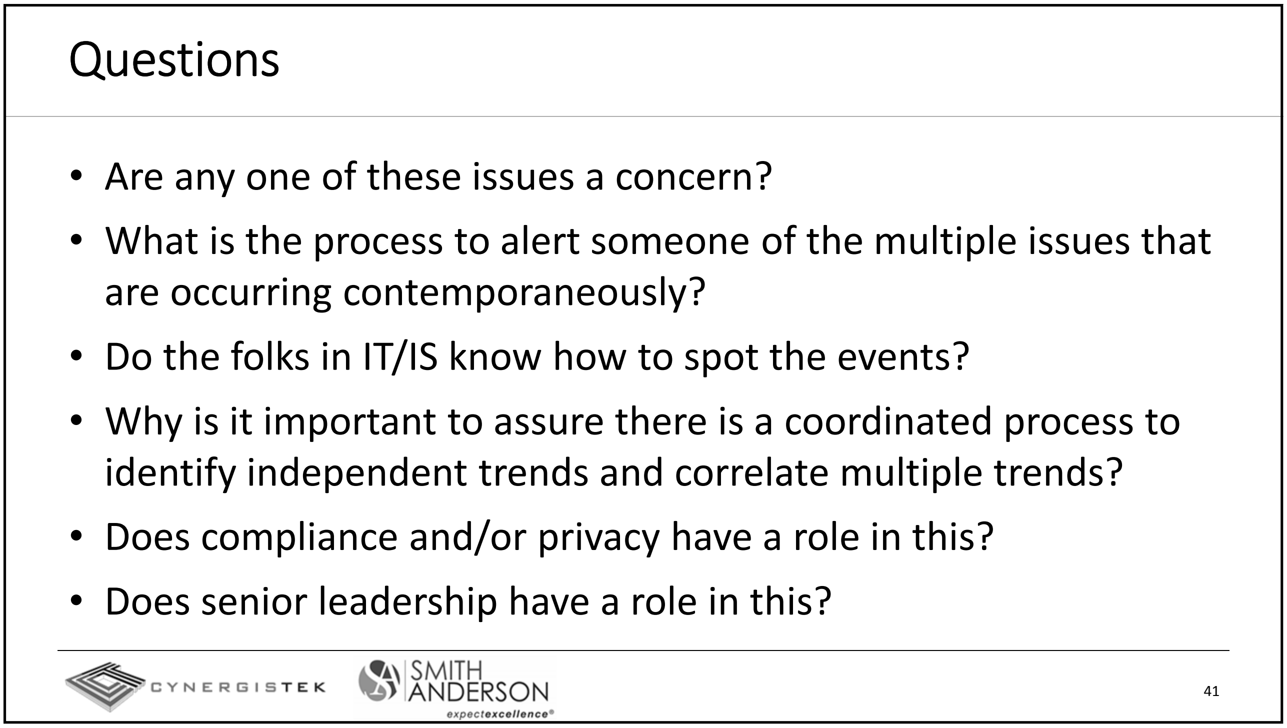
Definitions

- **Event** - An observable occurrence of a computer or network activity causing a negative impact
  - Examples:
    - A system is down or slow
    - Server running out of disk space
    - Dead power supply on a critical system
- **Incident** - An event that violates the policy including an event that has potential to lead to data loss, reputation loss, loss of IP, loss of funds or an outage affecting the ability of the firm to do business
  - Examples
    - Misplaced laptop
    - Social engineered transfer of funds to 3rd party
    - Email outage
- **Breach** - An incident that has resulted in data loss or exposure
  - Examples
    - Stolen or unaccounted for unencrypted removable media
    - Compromise of a system with resulting in ex-filtration of data
    - The willful improper use of data by an employee



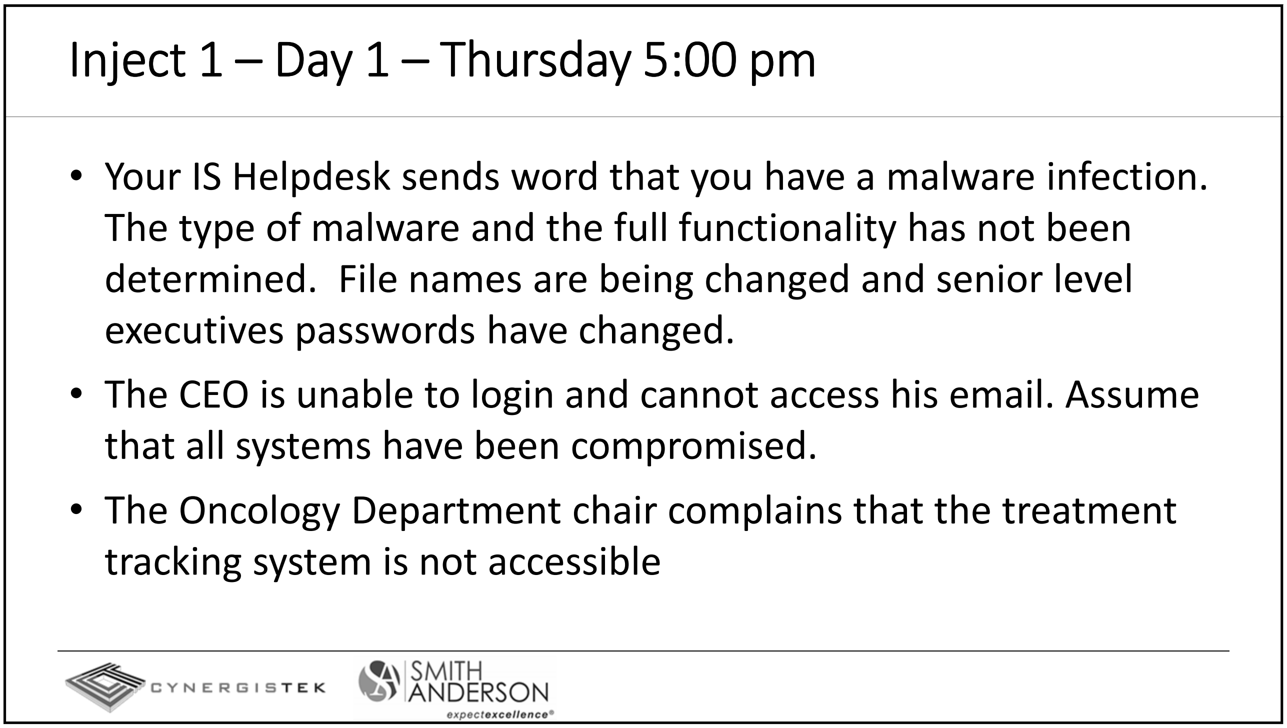
Inject 1 – Day 1 – Thursday 4:15 pm

- The IT Helpdesk starts to see an increase in tickets related to users who are unable to log in and who report that the self-help application to allow them to change their password is not working.
- IT operations also identifies that the CPU usage for various systems has exceeded the capacity set by the alert parameters.
- The organization's Security Operations Center is seeing an increase in data being exfiltrated from the network



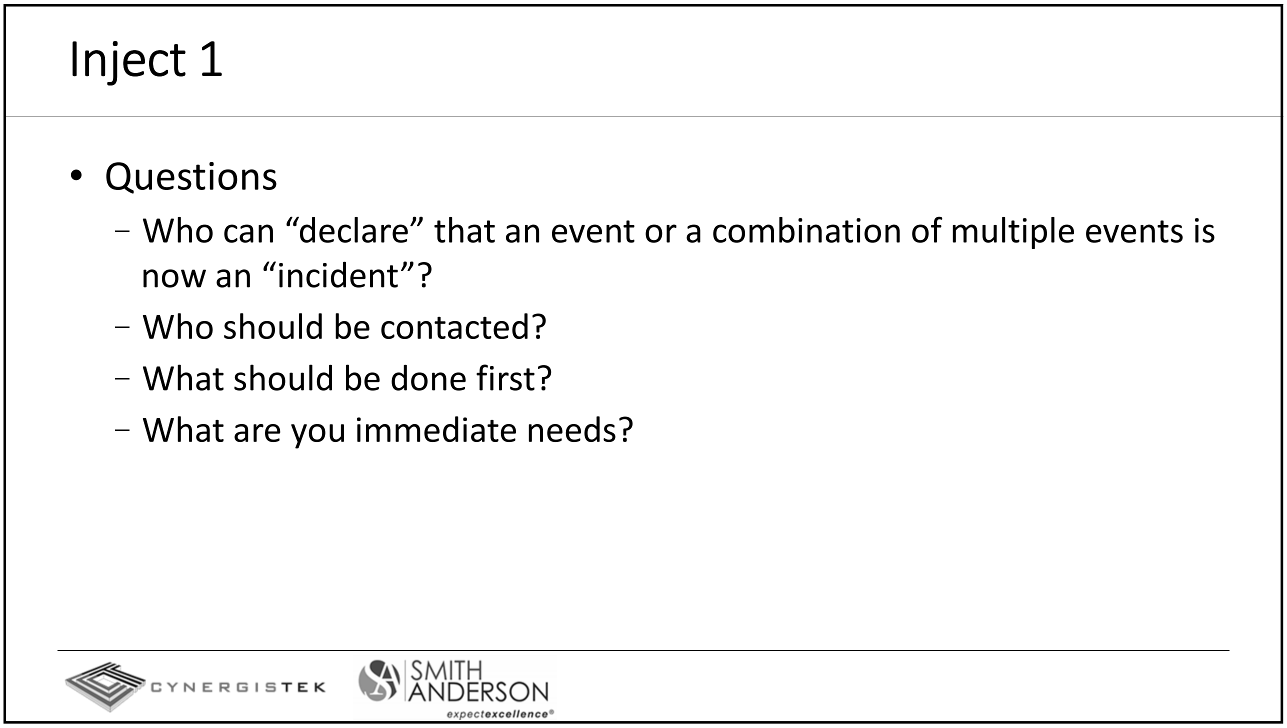
Questions

- Are any one of these issues a concern?
- What is the process to alert someone of the multiple issues that are occurring contemporaneously?
- Do the folks in IT/IS know how to spot the events?
- Why is it important to assure there is a coordinated process to identify independent trends and correlate multiple trends?
- Does compliance and/or privacy have a role in this?
- Does senior leadership have a role in this?



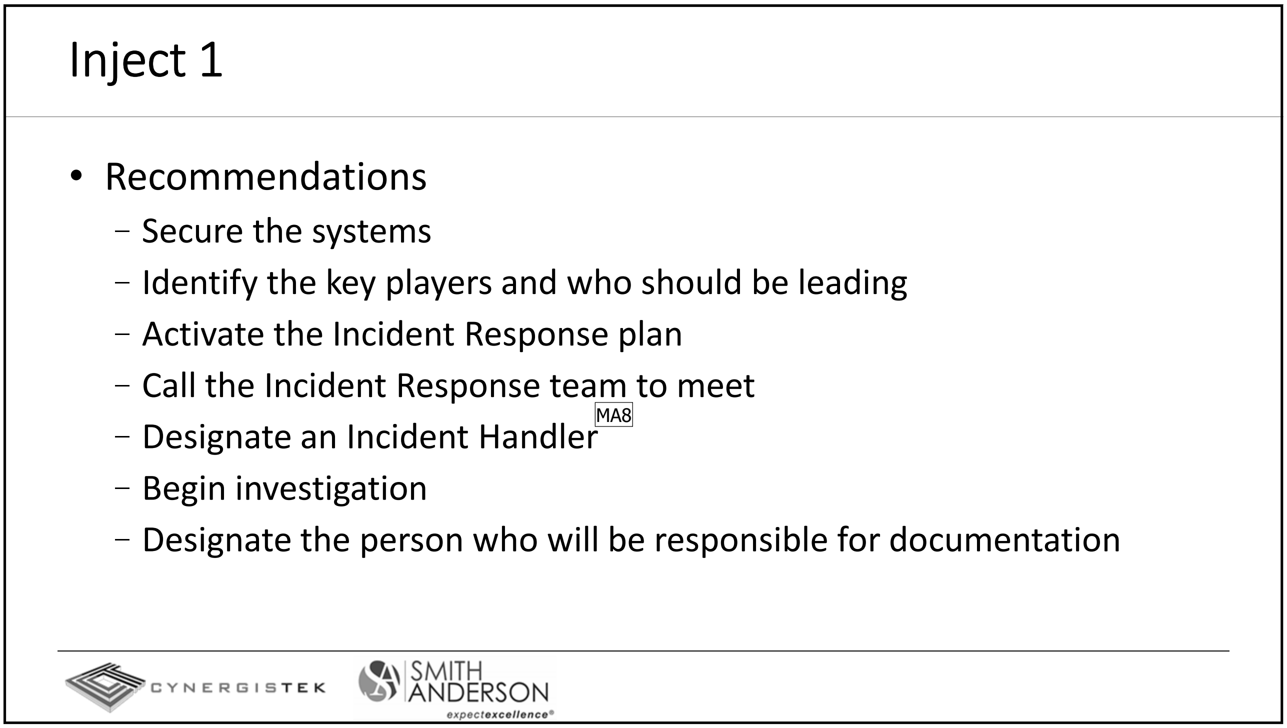
Inject 1 – Day 1 – Thursday 5:00 pm

- Your IS Helpdesk sends word that you have a malware infection. The type of malware and the full functionality has not been determined. File names are being changed and senior level executives passwords have changed.
- The CEO is unable to login and cannot access his email. Assume that all systems have been compromised.
- The Oncology Department chair complains that the treatment tracking system is not accessible



Inject 1

- Questions
  - Who can “declare” that an event or a combination of multiple events is now an “incident”?
  - Who should be contacted?
  - What should be done first?
  - What are you immediate needs?



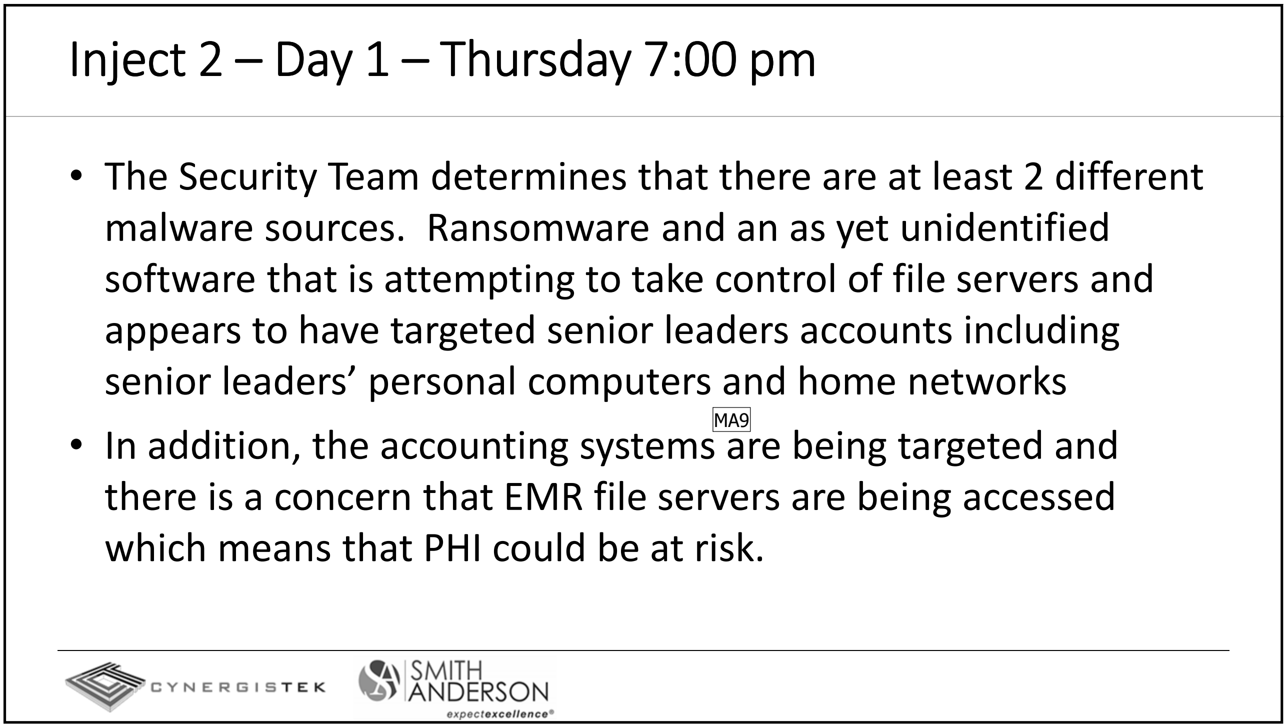
Inject 1

- Recommendations
  - Secure the systems
  - Identify the key players and who should be leading
  - Activate the Incident Response plan
  - Call the Incident Response team to meet
  - Designate an Incident Handler MA8
  - Begin investigation
  - Designate the person who will be responsible for documentation

Slide 44

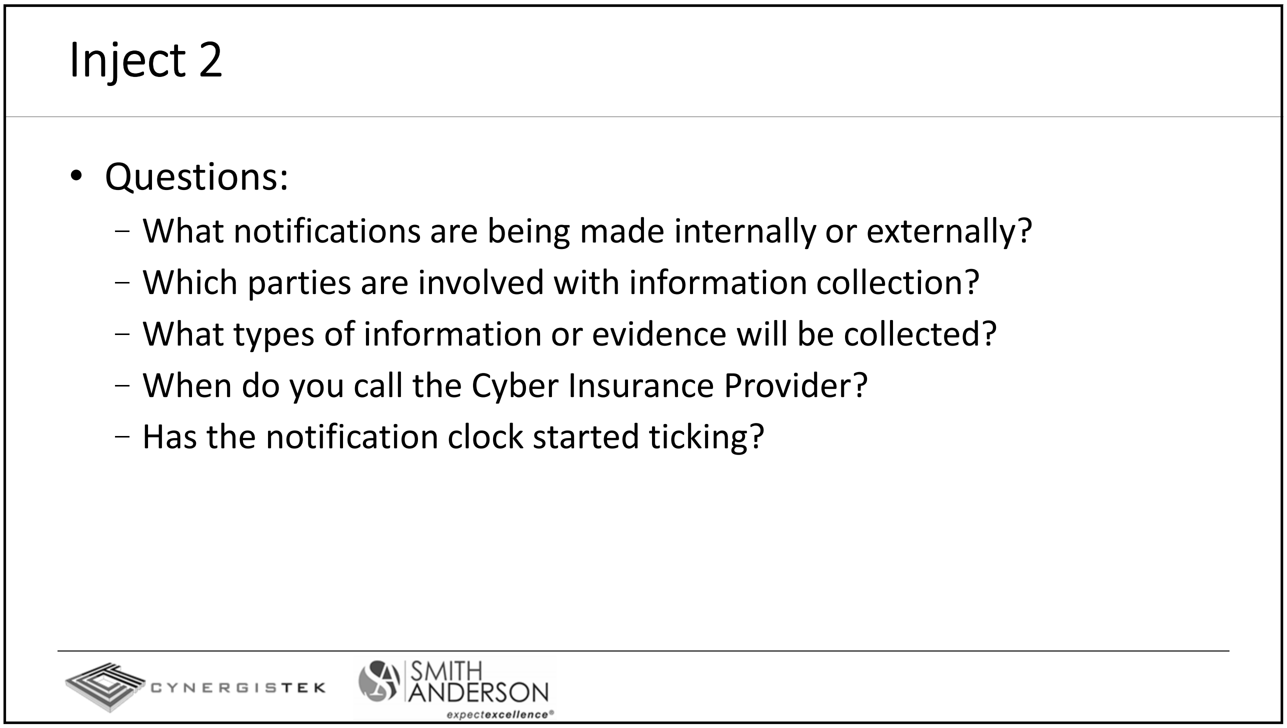
MA8 should this be Leader?

Marti Arvin, 3/2/2018



Inject 2 – Day 1 – Thursday 7:00 pm

- The Security Team determines that there are at least 2 different malware sources. Ransomware and an as yet unidentified software that is attempting to take control of file servers and appears to have targeted senior leaders accounts including senior leaders' personal computers and home networks
- In addition, the accounting systems are being targeted and there is a concern that EMR file servers are being accessed which means that PHI could be at risk.



Inject 2

- Questions:
  - What notifications are being made internally or externally?
  - Which parties are involved with information collection?
  - What types of information or evidence will be collected?
  - When do you call the Cyber Insurance Provider?
  - Has the notification clock started ticking?

Slide 45

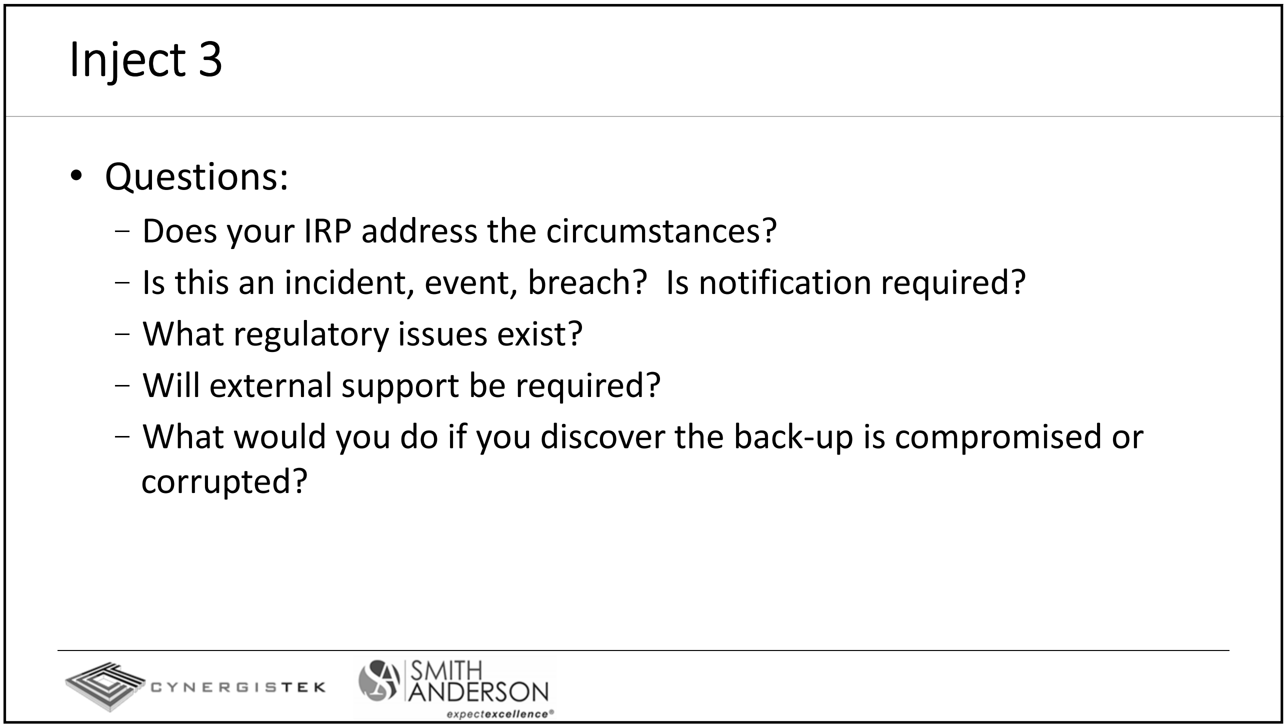
MA9 wouldn't PHI be at risk in the financial systems as well?
Marti Arvin, 3/2/2018

Inject 2

- Recommendation:
  - Forensics? Need to know extent of infection.
  - What technical responses need to be considered?
  - Status update for team.

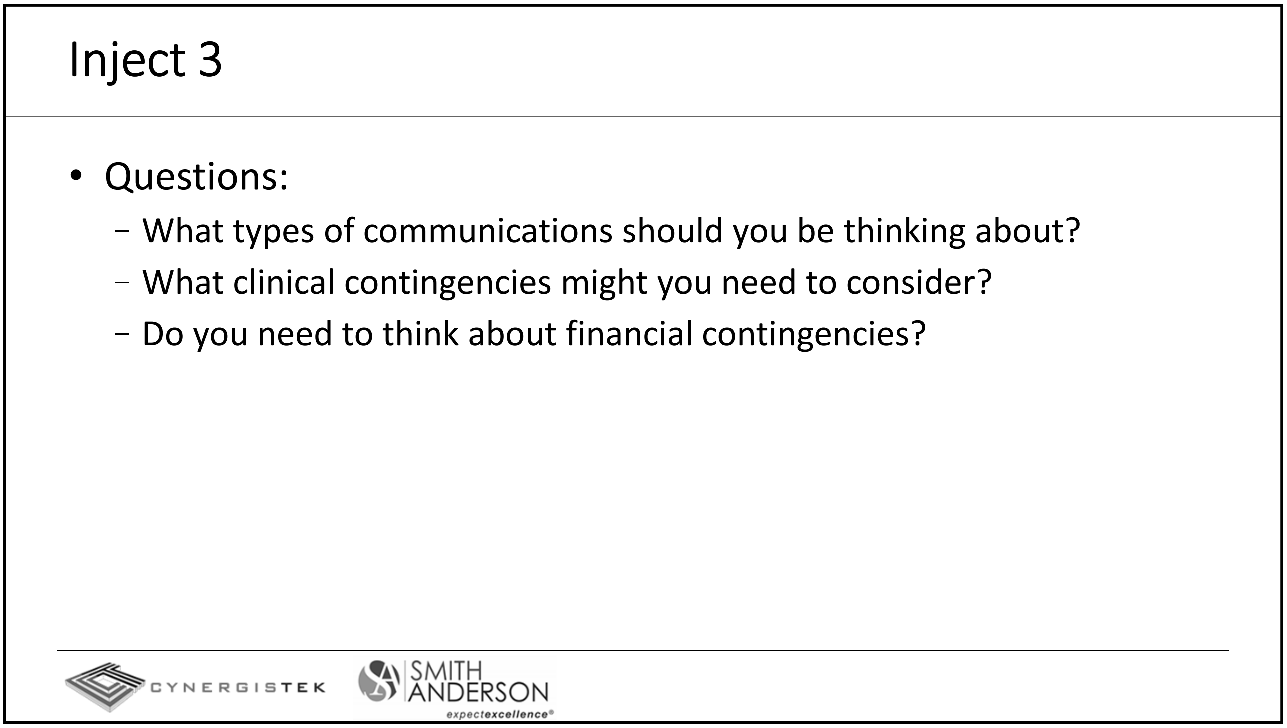
Inject 3 – Day 2 - Friday 11:30 am

- Reviewing the information gathered to date, you learn that health plan data, ERISA data, trade secret information and senior leadership credentials have been compromised. You don’t yet know the extent of the data encrypted by ransomware and data copied from your systems. Senior Leaders home networks are encrypted.
- Firewall and security logs from various sources show that data was exfiltrated via secure file transfer protocol (SFTP) to 46.30.45.39 and 185.43.205.98 in Eastern Europe and the current backups are being accessed to attempt a recovery.



Inject 3

- Questions:
  - Does your IRP address the circumstances?
  - Is this an incident, event, breach? Is notification required?
  - What regulatory issues exist?
  - Will external support be required?
  - What would you do if you discover the back-up is compromised or corrupted?



Inject 3

- Questions:
  - What types of communications should you be thinking about?
  - What clinical contingencies might you need to consider?
  - Do you need to think about financial contingencies?

Inject 3

- Recommendation:
  - Investigate to see what machines are compromised.
  - What technical responses need to be considered?
  - Status update for team.
  - Discuss the legal, compliance ramifications.
  - Discuss forensic needs.

CYNERGISTEK SMITH ANDERSON expectexcellence®

JN6

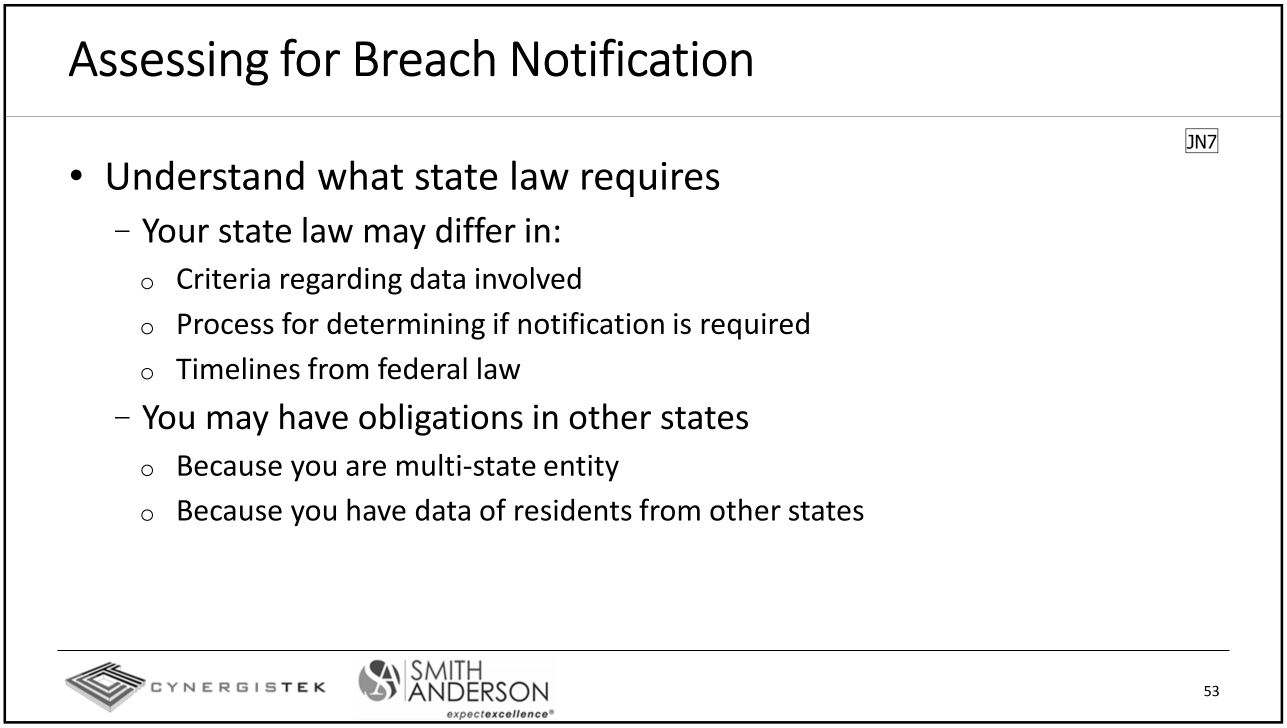
Assessing for Breach Notification

- Understanding what HIPAA Requires
  - The clock starts when the event is discovered
  - Notification must must occur without undue delay
    - The maximum for undue delay is 60-day
- If you are a business associate you must notify the covered entity of a breach without undue delay but not more than 60 days from discovery
  - Your BAA agreement may have a shorter timeframe

CYNERGISTEK SMITH ANDERSON expectexcellence®

Slide 52

JN6 Needs an image or more copy
John Nye, 2/13/2018

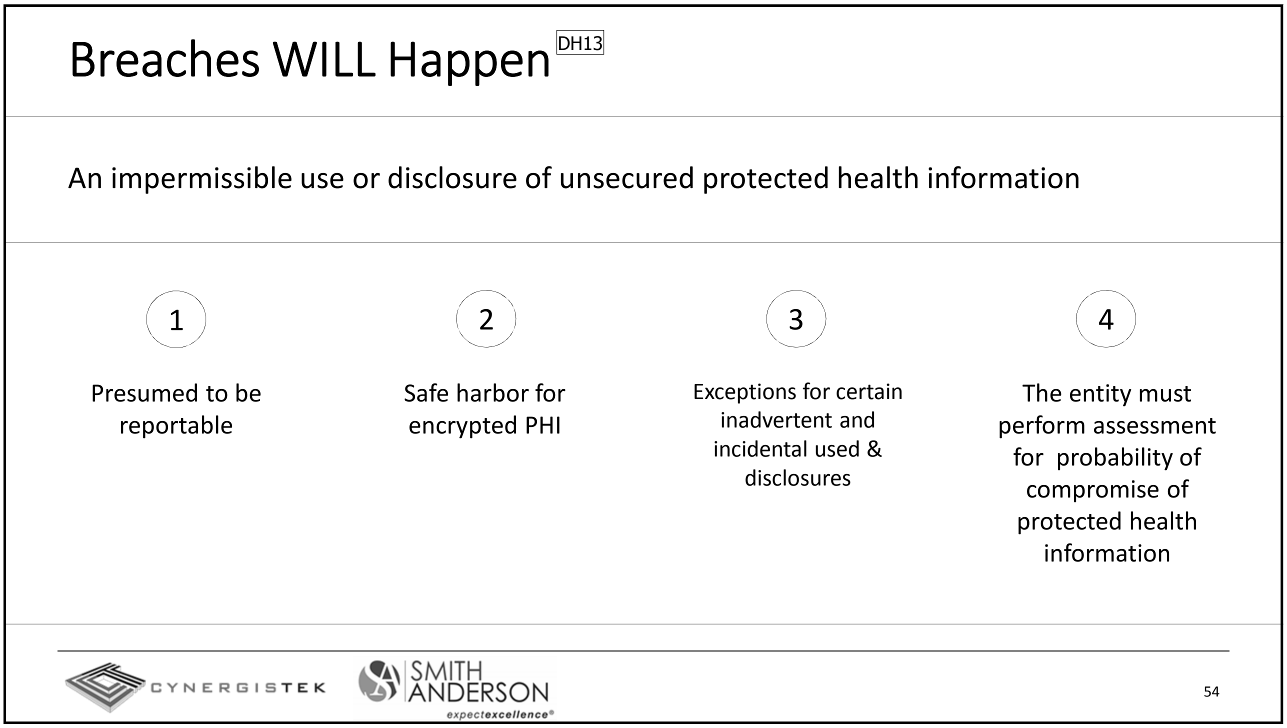


Assessing for Breach Notification

JN7

- Understand what state law requires
  - Your state law may differ in:
    - Criteria regarding data involved
    - Process for determining if notification is required
    - Timelines from federal law
  - You may have obligations in other states
    - Because you are multi-state entity
    - Because you have data of residents from other states

CYNERGISTEK SMITH ANDERSON expectexcellence®



Breaches WILL Happen

DH13

An impermissible use or disclosure of unsecured protected health information

1. Presumed to be reportable
2. Safe harbor for encrypted PHI
3. Exceptions for certain inadvertent and incidental used & disclosures
4. The entity must perform assessment for probability of compromise of protected health information

CYNERGISTEK SMITH ANDERSON expectexcellence®

Slide 53

JN7 Probably needs an image or more copy. Maybe this sections needs to be created entirely by Marti :thinking face
John Nye, 2/13/2018

Slide 54

DH13 Reordered and edited
David Holtzman, 2/15/2018

Breach: Assessing Probability of Compromise

Assessment to determine probability of compromise

1 The nature and extent of PHI involved

2 The unauthorized person who used the PHI or to whom the disclosure was made

3 Whether the PHI was actually acquired or viewed

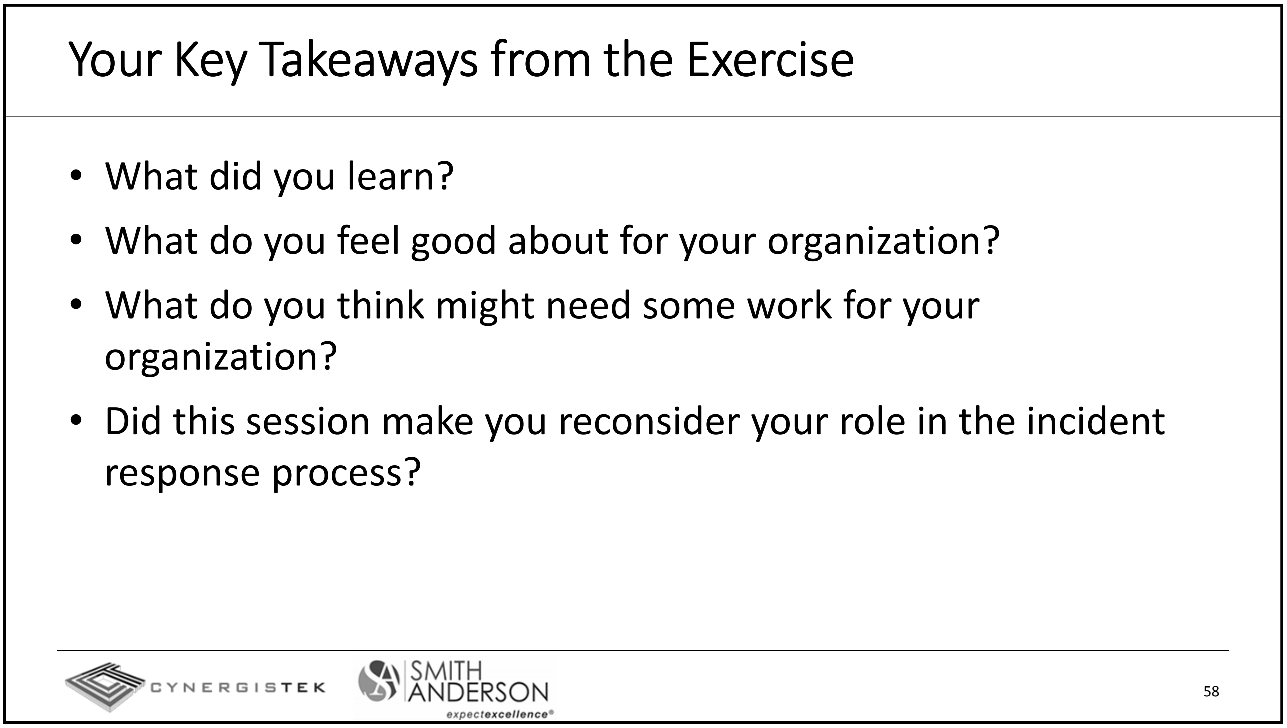
4 The extent of mitigation present

Additional factors to be considered in ransomware incidents:
- Whether there is high risk of unavailability of PHI?
- Whether there is high risk to the integrity of PHI?

Notification of others

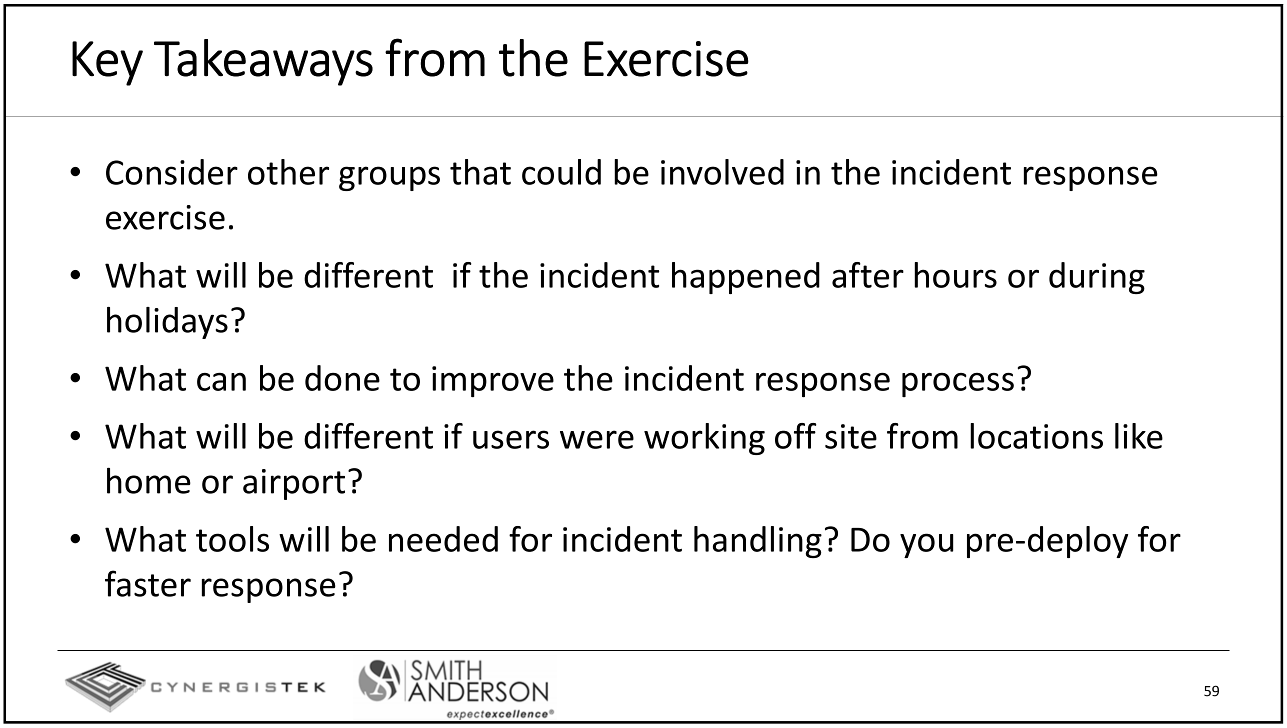
- In addition to regulatory obligations to notify there may also be other obligations
  - Contractual obligations
    - Are you a BA to another covered entity?
    - Does the organization have contracts that require notification regarding a data incident or breach

Post Exercise Debrief



Your Key Takeaways from the Exercise

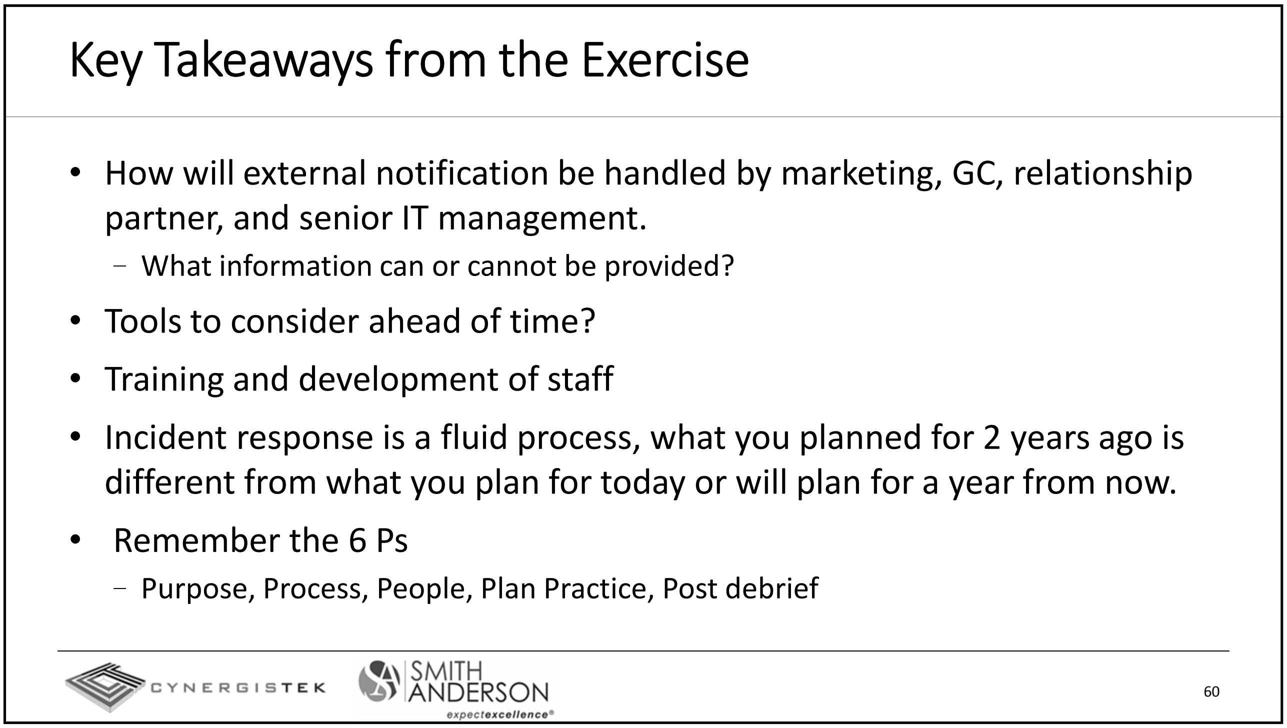
- What did you learn?
- What do you feel good about for your organization?
- What do you think might need some work for your organization?
- Did this session make you reconsider your role in the incident response process?



Key Takeaways from the Exercise

- Consider other groups that could be involved in the incident response exercise.
- What will be different if the incident happened after hours or during holidays?
- What can be done to improve the incident response process?
- What will be different if users were working off site from locations like home or airport?
- What tools will be needed for incident handling? Do you pre-deploy for faster response?

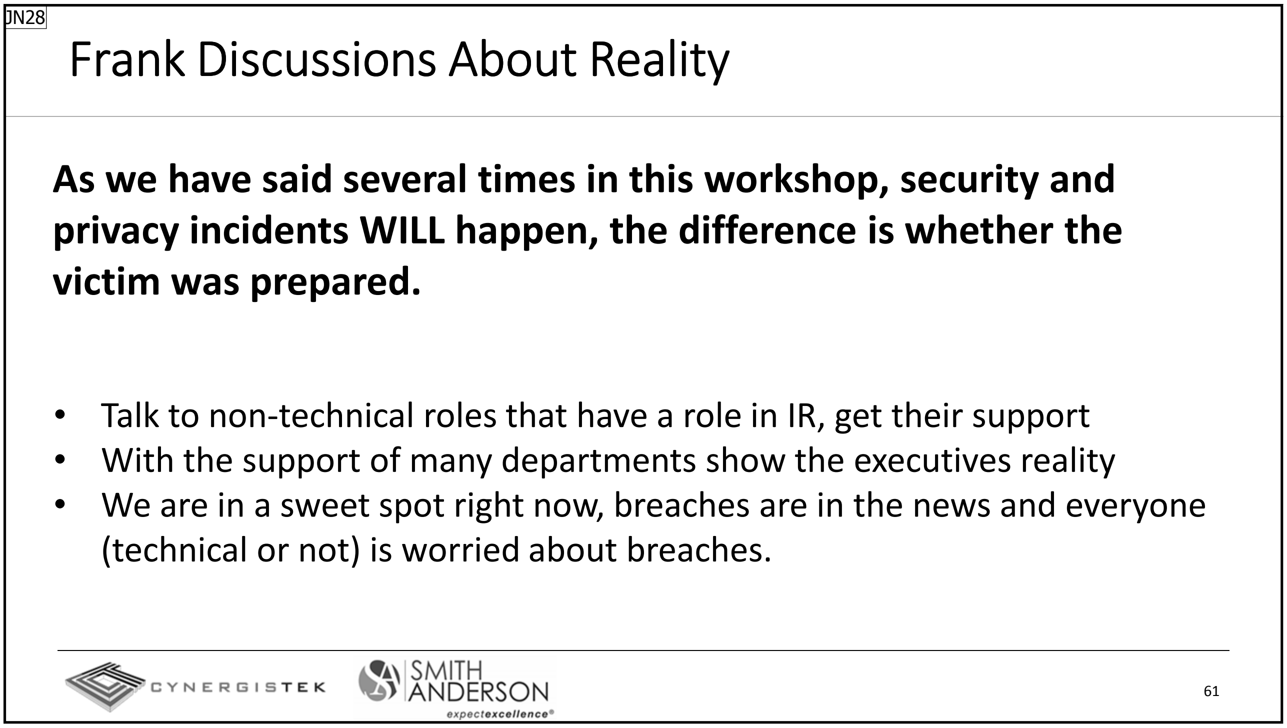
CYNERGISTEK SMITH ANDERSON expectexcellence®



Key Takeaways from the Exercise

- How will external notification be handled by marketing, GC, relationship partner, and senior IT management.
  - What information can or cannot be provided?
- Tools to consider ahead of time?
- Training and development of staff
- Incident response is a fluid process, what you planned for 2 years ago is different from what you plan for today or will plan for a year from now.
- Remember the 6 Ps
  - Purpose, Process, People, Plan Practice, Post debrief

CYNERGISTEK SMITH ANDERSON expectexcellence®

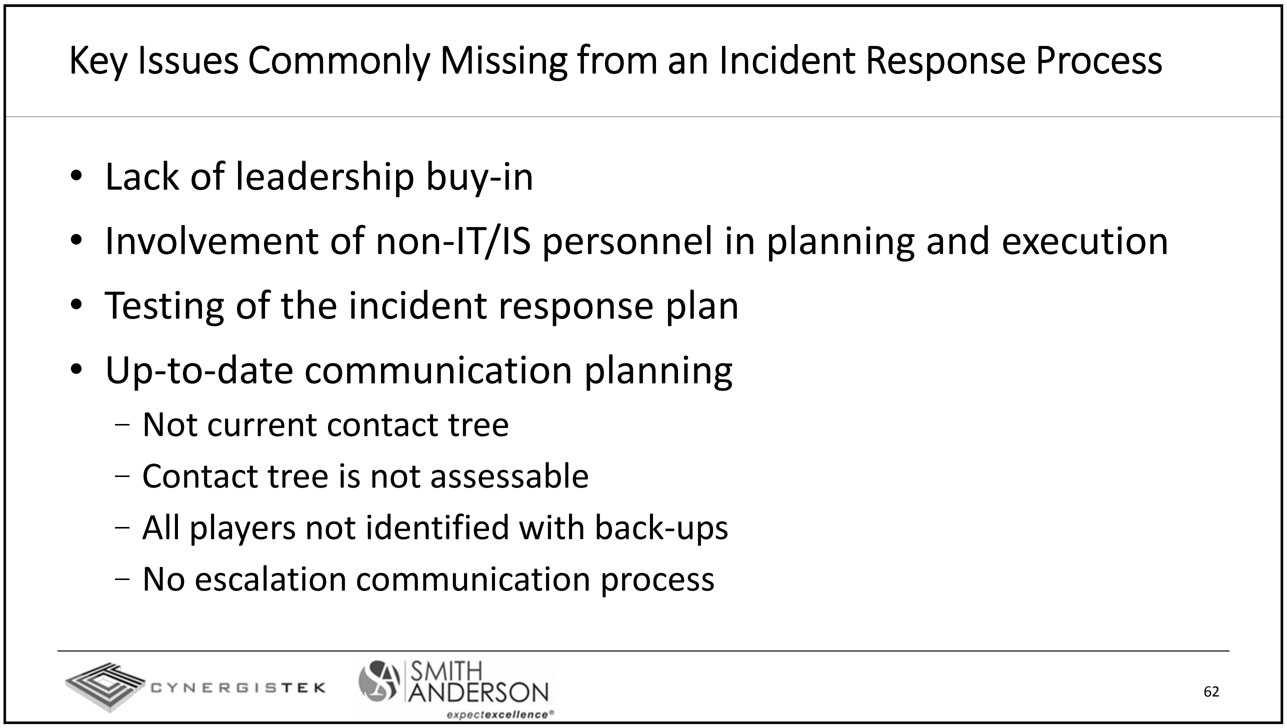


JN28

Frank Discussions About Reality

As we have said several times in this workshop, security and privacy incidents WILL happen, the difference is whether the victim was prepared.

- Talk to non-technical roles that have a role in IR, get their support
- With the support of many departments show the executives reality
- We are in a sweet spot right now, breaches are in the news and everyone (technical or not) is worried about breaches.



Key Issues Commonly Missing from an Incident Response Process

- Lack of leadership buy-in
- Involvement of non-IT/IS personnel in planning and execution
- Testing of the incident response plan
- Up-to-date communication planning
  - Not current contact tree
  - Contact tree is not assessable
  - All players not identified with back-ups
  - No escalation communication process

Slide 61

JN28 Needs more content
John Nye, 2/14/2018

Incident Response:
Making a Business Case

JN27 MA2

Convincing Senior Leaders

- Cost of a data compromise
  - Time, it takes on average*
    - 50 days to resolve a malicious insider attack
    - 23 days to return to normal operations after a ransomware attack, months or years to recover the financial impact
  - Resolving issues will take key personnel way from their usual work which may
    - Cause projects to lag
    - Resolution to standard IT issues to fall behind

*Ponemon 2017 Cost of Cyber Crime Study

Slide 64

JN27 Find some stats that weren't already used earlier to help sell the importance of IRP to executives.
John Nye, 2/14/2018

MA2 I deleted the 7 Ps slide before this one because I agree with David's comment regarding it.
Marti Arvin, 2/20/2018

JN27

Convincing Senior Leaders

- Cost of a data compromise
  - Money – downtime*
    - The average cost of downtime across all industries is $8,851/min according to a 2016 survey
    - This is up from $5,617/min in 2010
    - The average duration of a partial unplanned outage is 64 minutes or $566,464
    - The average duration of a total unplanned outage is 130 minutes or $1,150,630
  - Money – lost revenue, decreased cash flow
    - Cancelled services (elective procedures, reduced clinic hours)
    - Delay in billing secondary to downtime procedures or loss of the system

*Ponemon 2016 Cost of Data Center Outages

Thank You!

Questions?

Joe Dickinson
Partner, Smith Anderson
jdickinson@smithlaw.com
919-821-6782

Marti Arvin
VP Audit Strategy
Marti.arvin@cynergistek.com
512-402-8550 x7051

Slide 65

JN27 Find some stats that weren't already used earlier to help sell the importance of IRP to executives.
John Nye, 2/14/2018