Results. Guaranteed.

online

Maintaining Cybersecurity When Disaster Strikes

November 18, 2020

Objectives

- Demonstrate the cybersecurity considerations and activities relevant to incident response through the use of a case study
- Provide the main objectives and most important activities related to cybersecurity when responding to an emergency or incident
- Discuss what steps organizations should take to prepare for cybersecurity incidents

Agenda

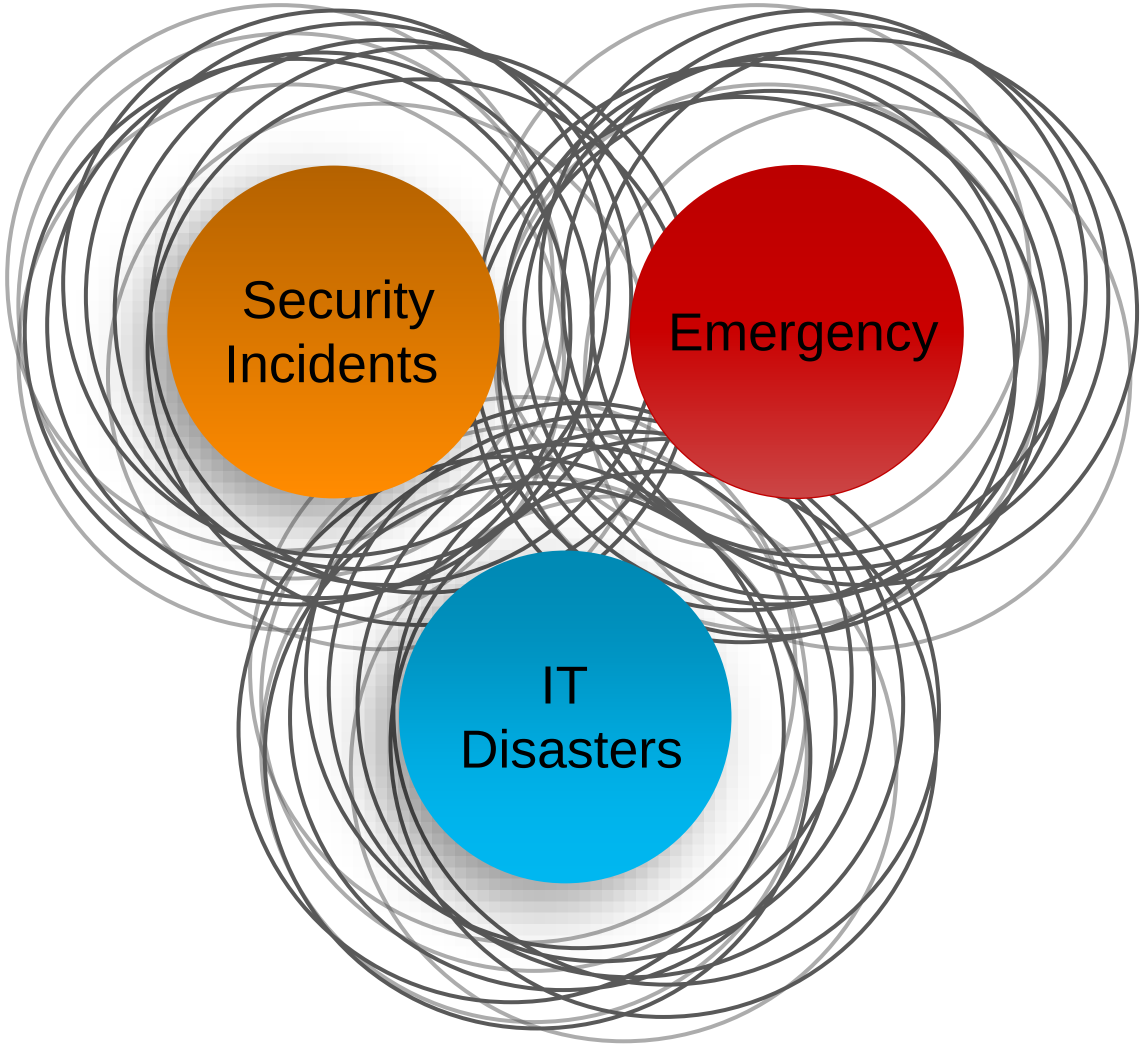
- Overview of Emergency Response
- Business Continuity and Cybersecurity
- Security Incident Response
- Case Study
- Conclusion
- Supporting Documentation

Emergency Response Overview

What Does Cybersecurity have to do with Emergency Response?

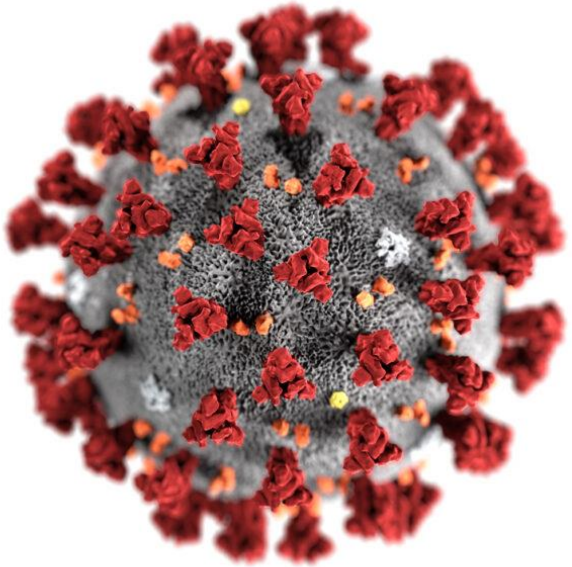
- Natural Disaster, Snowstorm
- Technical Outage, Power, Network
- Pandemic?
- Social and Political Conflict?
- Cyber Attack, Ransomware

Business Continuity and Security Incident Response



What We’ve Learned from COVID-19

1. You may need to pivot to new technologies quickly
   a) Cybersecurity considerations of work-from-home, BYOD, and Telemedicine
2. Cybercriminals don’t go away during a pandemic; if anything, they increase and focus efforts
3. Business Continuity Plans should account for loss of physical access and key staff
4. All types of emergencies have cybersecurity implication

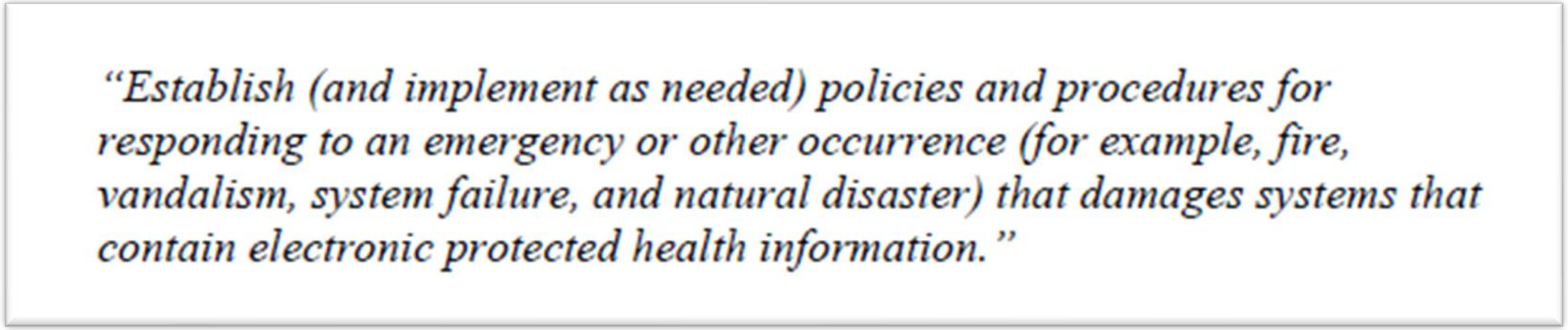


Poll Question: New Technologies

Results. Guaranteed.

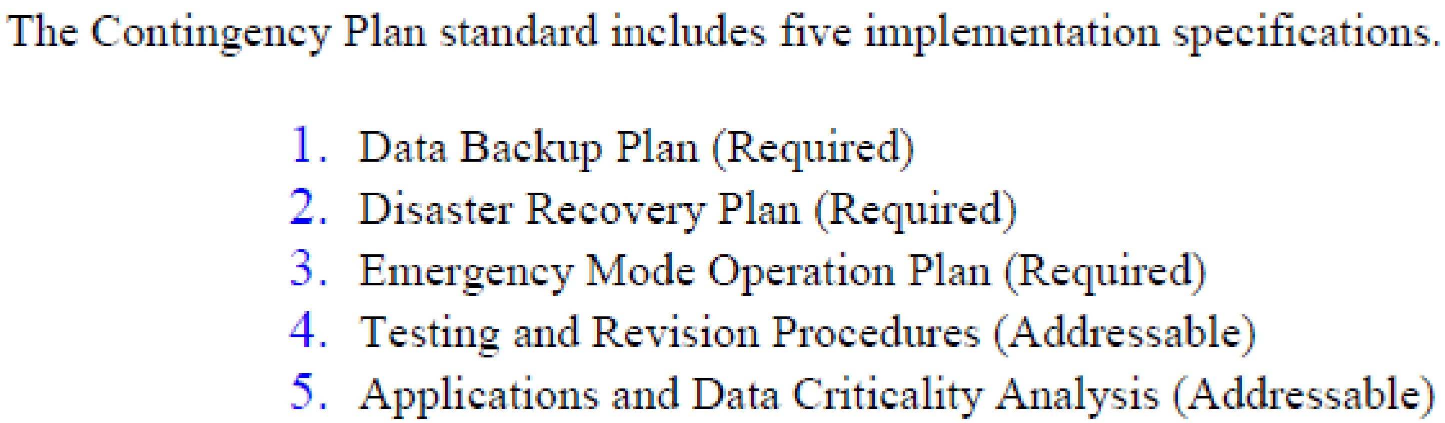
Business Continuity and Cybersecurity

Contingency Plan - § 164.308(a)(7)



"Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information."

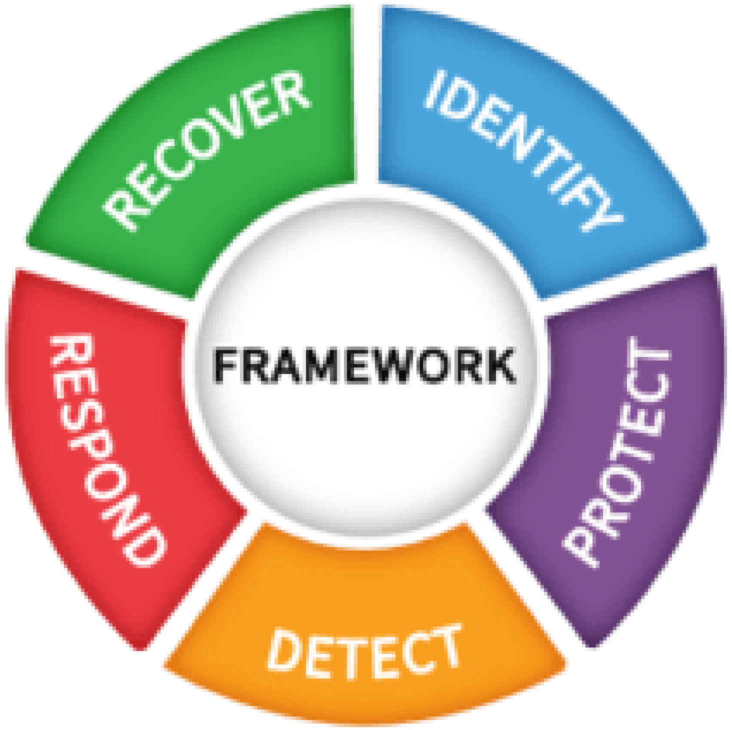
HIPAA and Emergency Response



The Contingency Plan standard includes five implementation specifications.

1. Data Backup Plan (Required)
2. Disaster Recovery Plan (Required)
3. Emergency Mode Operation Plan (Required)
4. Testing and Revision Procedures (Addressable)
5. Applications and Data Criticality Analysis (Addressable)

NIST Cybersecurity Framework



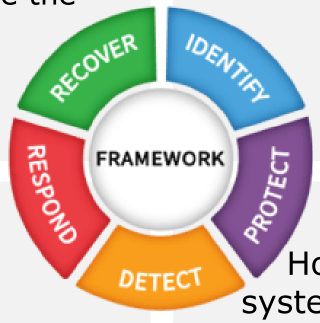
Business Continuity Plan

Respond

Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected events.
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Identify

- Perform a Business Impact Analysis
- What workflows are critical during an emergency?
- What systems and information are critical to supporting those workflows?



Recover

- When you return to “normal”, how will you reconcile production and backup systems?
- Who will make determinations of when to switch systems?
- Lessons Learned.

Protect

How can you perform those workflows if those systems aren’t available? How will information be available when and where needed?

- How will you maintain integrity of information as you go to paper-based or offline systems?
- How will you maintain security controls during an emergency?
- Consider: Access Control, Encryption, Monitoring, Backup/Recovery. Are there areas where you will bypass controls? For example: Emergency Authorization for access to systems? What compensating controls are in place?

Business Continuity Plan

- Components of the Business Continuity Plan
  - Business Units/Locations with primary and backup contact names and numbers
  - BCP Team Members and Responsibilities
  - List of critical assets (input from BIA)
  - Reference Documents such as facility recovery plans, system backup/recovery plans, State/local plans
  - Departmental BCPs
  - Communications and Coordination Plans
  - Critical Vendor, Service Provider, and Law Enforcement contact information
  - Procedure to return to normal operations

Poll Question: Ransomware

Case Study: Ransomware

Topic	Questions
Identify	• Are critical assets identified and their susceptibility to Ransomware assessed?
Protect	• Are critical assets backed up? Are backups logically and physically separated from production systems? • Are critical assets on separate network segments?
Detect	• Are systems in place to detect ransomware Indicators of Compromise (IOCs) so that it can be contained before it launches or spreads?
Respond	• If critical assets are locked up, how will the organization respond? • How will the message be communicated externally?
Recover	• Have you tested recovery plans for affected systems?

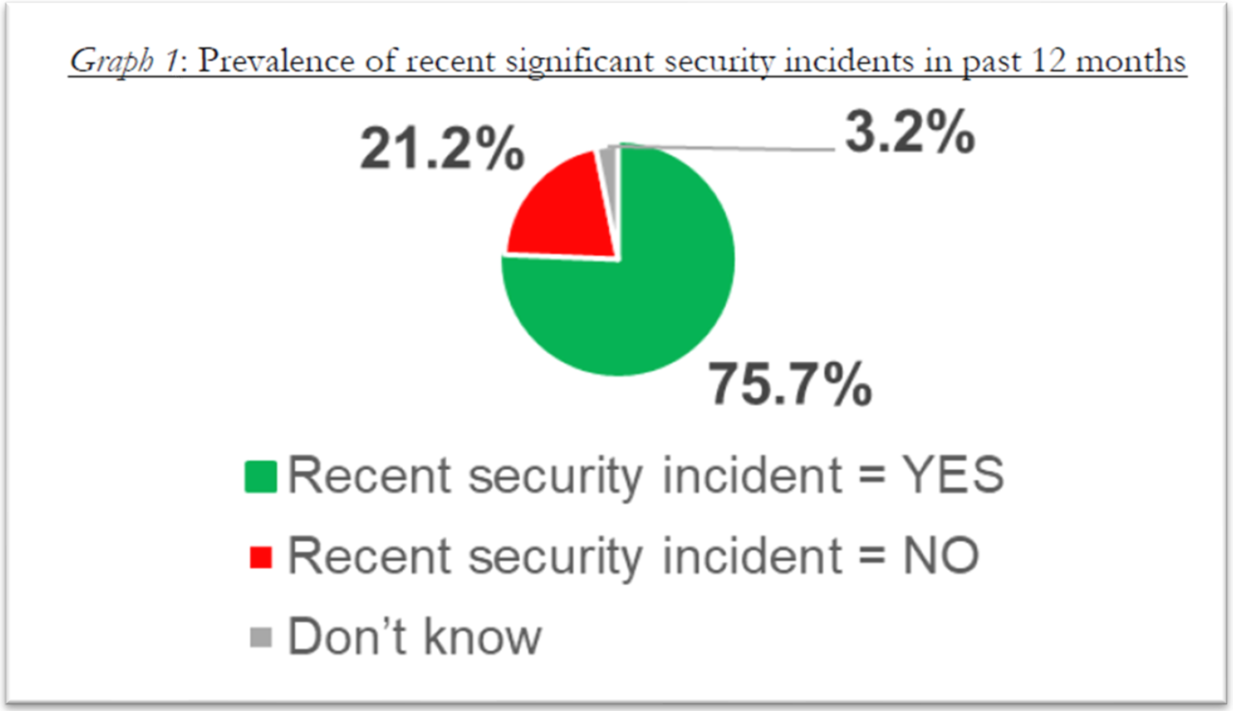
Results. Guaranteed.

Case Study: Ransomware

Mikkel Finsen, Open Door Family Medical Center

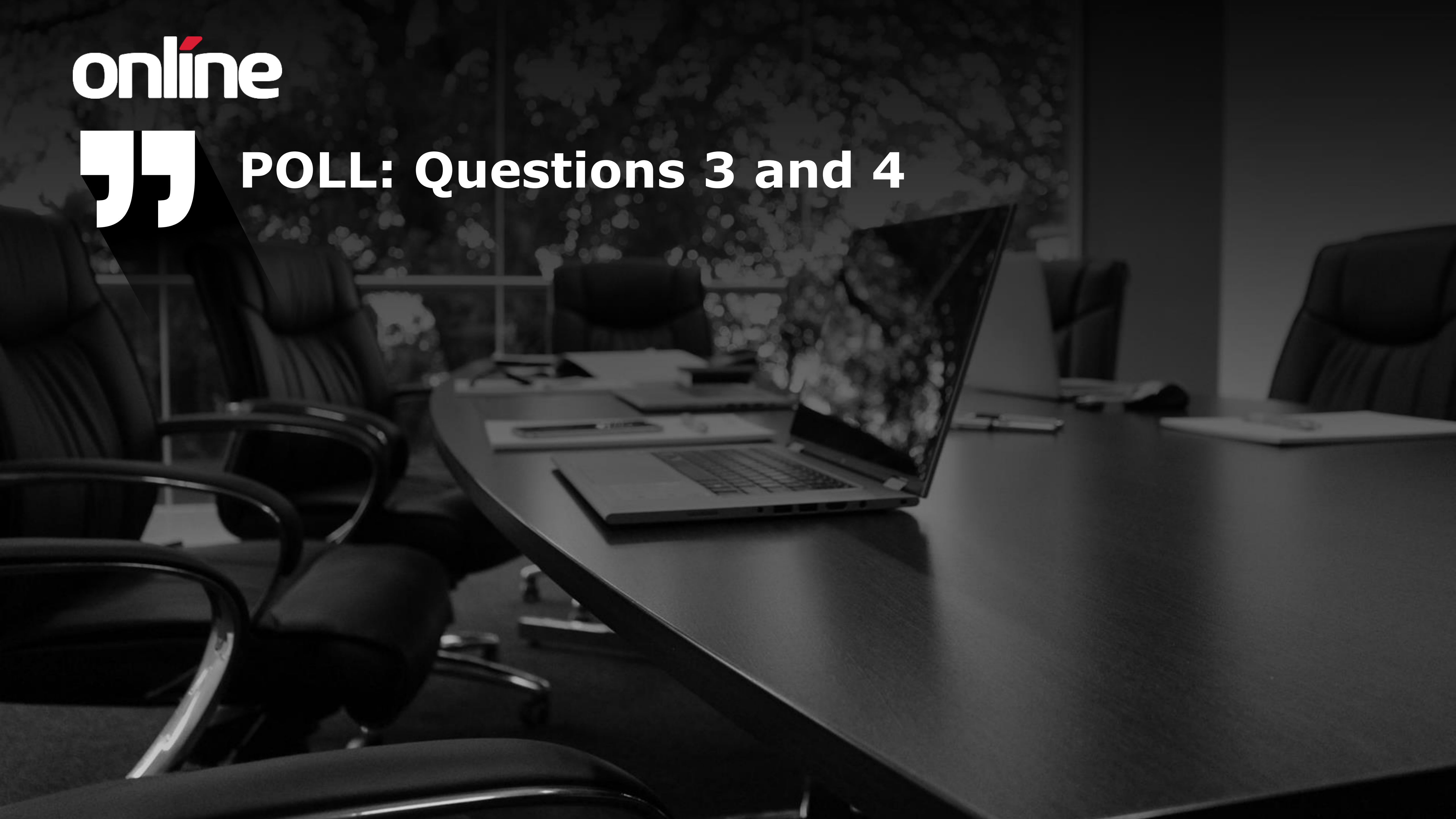
Security Incident Response

What's Happening: Healthcare organizations continue to experience significant security incidents.



Graph 1: Prevalence of recent significant security incidents in past 12 months

Source: 2018 HIMSS Cybersecurity Survey



POLL: Questions 3 and 4

HIPAA and Security Incident Response

Security Incident Procedures - §164.308(a)(6)

"Implement policies and procedures to address security incidents."

RESPONSE AND REPORTING (R) - § 164.308(a)(6)(ii)

"Identify and respond to <u>suspected or known security incidents</u>; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."

Definition of Security Incident:

"the <u>attempted or successful</u> unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

Security Incident Response

Maintenance

- Test Incident Response Plan through Tabletop Exercises
- Test likely scenarios (e.g. Ransomware, Phishing, Theft
- Improve based on lessons learned
- Review documentation of security incidents to identify improvements
- Update/Review annually

Security Incident Response

Questions to ask yourself?

- How are we documenting security incidents?
- What is our communications plan? Internal/External?
- Who are the decision makers? For example, who has ultimate authority to shut down critical systems such as EMR in order to prevent further infection of malware?
- Do all employees know how to recognize a security incident, know their obligation to report, and know how to report?

online

Security Incident Response Plan

NIST SP 800-53 (IR-8) Incident Response Plan:

- Provides the organization with a roadmap for implementing its incident response capability;
- Describes the structure and organization of the incident response capability;
- Provides a high-level approach for how the incident response capability fits into the overall organization;
- Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
- Defines reportable incidents;
- Provides metrics for measuring the incident response capability within the organization;
- Defines the resources and management support needed to effectively maintain and mature an incident response capability

Security Incident Response

Components of a Security Incident Response Plan

- Business Units/Locations with primary and backup contact names and numbers
- CIRT Team Members and Responsibilities (RACI Chart)
- Communications and Coordination Plans
- Security Incident Handling Procedures
- Security Incident Notification Plans
- Escalation Procedures
- Chain of Custody Procedures
- Critical Vendor, Service Provider, and Law Enforcement contact information
- Post Incident Activities

RACI Chart

The Responsibility Assignment Matrix (RACI) describes the level of participation by various roles in handling different stages of the incident response lifecycle. The RACI matrix is comprised of the following actions:

R – Responsible – owns the action; is responsible for completion
A – Accountable – ultimately accountable for completion
S – Supporting – provides resources or plays supporting role
C – Consulted – provides information or has capabilities to necessary to complete work
I – Informed – must be notified of results, but does not need to be consulted

	Users	CIO	ISS / HSD	ESO	Legal / IPO	RMO	Server / Desktop Support	Network Support	Urgent Response Team	HR	Workplace Services
Detection	R	A	S	R	I	I	I	I	I	I	I
Notification	I	A	R	R	I	I	I	I	I	I	I
Analysis	C	A	S	R	C	I	S	S	S	C	C
Containment	I	A	I	R	I	I	R	R	R	I	I
Eradication	I	A	I	R	I	I	R	R	R	I	I
Recovery	I	A	I	R	C	C	S	S	S	I	I

Interaction: Scenario 1

You just received a call from the FBI indicating your systems have been compromised.

What do you do?
Who do you call?
Do you have a Security Incident Response Plan ready to use?

Interaction: Scenario 2

Your Internet connection is down, and you determine it is due to a Distributed Denial-of-Service Attack.

What do you do?
Who do you call?
What do you tell you employees, patients, and the public?
How do you maintain operations and availability of information?

Consider: Confidentiality, Integrity, and Availability

Interaction: Scenario 3

A doctor reports that they were tricked by a phishing email into entering their credentials into a fake website.

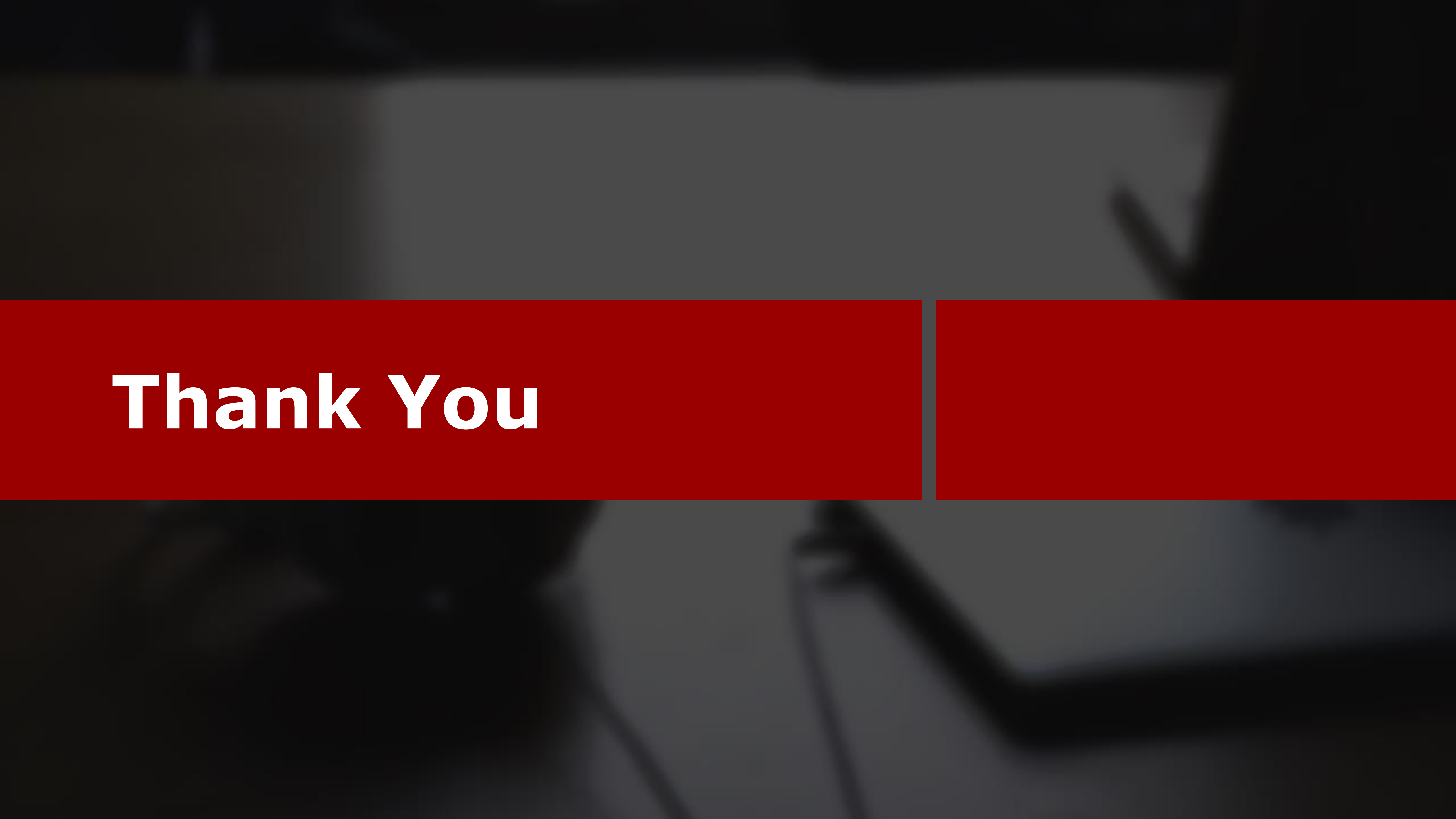
What actions should you take?
Who do you inform?
What documentation and evidence do you maintain and where?

Conclusion

- Consider what types of emergencies or incidents are likely to occur in your organization and the cybersecurity ramifications
- Have your response plans ready and tested
- Know roles and responsibilities for your organization (Hint: this isn’t just an IT problem)
- Know when and how to reach out to experts

References

- NIST 800-61 – Computer Security Incident Handling Guide - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- NIST 800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities - https://csrc.nist.gov/publications/detail/sp/800-84/final
- https://www.fema.gov/media-library/assets/documents/26845
- https://security.berkeley.edu/faq/ransomware/



Thank You