COMMUNITY HEALTH CARE ASSOCIATION of New York State

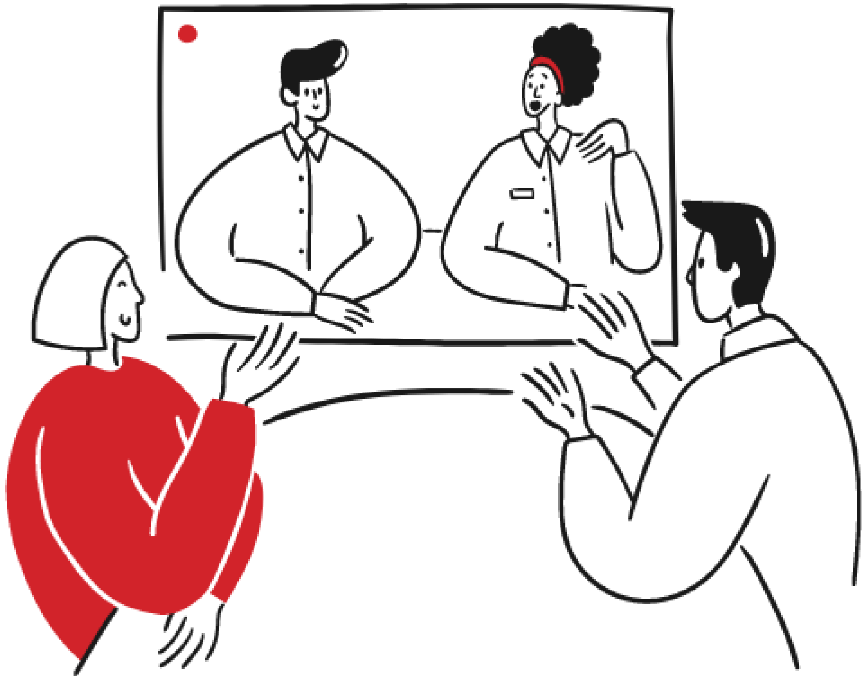
CHCANYS NYS-HCCN presents a four-part learning series with Online Business Systems

Building an Incident Response Plan

Session 4
March 1, 2023

Zoom Guidelines

- You have been muted upon entry. Please respect our presenters and stay on mute if you are not speaking.
- Please share your questions in the chat. CHCANYS staff will raise your questions to our speakers and follow up as needed if there are unanswered questions.
- The workshop is being recorded and slides will be shared after the session.



New York State HCCN Objectives

Project Period 2022-2025

1 **Clinical Quality**

2 **Patient-Centered Care**

3 **Provider and Staff Wellbeing**

2022-2025 Project Period

- ✓ **Patient Engagement**
- ✓ **Patient Privacy & Cybersecurity**
- ✓ **Social Risk Factor Intervention**
- ✓ Disaggregated Patient-level Data (UDS+)
- ✓ **Interoperable Data Exchange & Integration**
- ✓ **Data Utilization**
- ✓ Leveraging Digital Health Tools
- ✓ Health IT Usability & Adoption
- ✓ Health Equity and REaL Data Collection*
- ✓ Improving Digital Health Tools- Closed Loop Referrals*

** - Applicant Choice Objective*
Bold- Objective Carried over into 2022-2025

Building an Incident Response Plan

Shelby Kobes, CCSFP

Consultant: Risk, Security & Privacy

Online Business Systems

online

HEALTH CYBERSECURITY

Session 4: Incident Response

Best Practices, HIPAA Requirements,

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

In 2021, the average total cost of a data breach in the health industry was a whopping $9.23 million, with a 9.4% increase to $10.10 million in 2022. That's higher than the average cost of a breach in any other industry sector.

- 66% of healthcare organizations say they experienced a ransomware attack in 2021, an increase from 34% in 2020.
- There was an 84% increase in healthcare breaches from 2018 to 2021.
- 50 million Americans had their PHI exposed in healthcare data breaches in 2021 — that's a 3X increase over 2018 figures.
- In healthcare alone, there were 14 million victims of data breaches in 2018, which increased to 44.9 million victims in 2021.
- Healthcare data breaches can cost as much as $408 per record — which is the highest cost of any industry
- **Medical clinics are now the number-one target for ransomware attacks in the United States**
- **20% of hospitals that experienced a cyber attack reported an increase in patient mortality. Of that 20%, 57% reported poorer patient outcomes and 50% reported an increase in medical complications as a result of the cyber attack.**

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 ***attempted*** *or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."*

HIPAA/SHIELD Act

Stop Hacks and Improve Electronic Security (SHIELD) Act

- Works in concert with HIPAA/HITECH Breach Notification
- However, contains data elements NOT included in HIPAA (and vice versa)
- Required to notify *New York State Attorney General* in addition to HHS
- Different definitions of large breach (500 for HIPAA, 5,000 for SHIELD) and entities that must be notified.

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
- 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

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?

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

Tabletop Exercises

Tabletop Exercises (Why)

- Improve response time to reduce finical costs and improve patient outcomes
- HIPAA alignment – Grants, etc.
- State and local requirements
- Find weaknesses in the organization
- Build a security culture

Tabletop Exercises

Tabletop Exercises (Who)

- Depends on the goals of the organization!
- Anyone with decision-making responsibilities
- IT, Admin, HR, Buildings, Legal, Compliance, and third-party providers
- Who is Impacted

Tabletop Exercises

Tabletop Exercises (What do you need, Tips)

- Good conversation
- Stepping out of roles
- Someone to keep records and notes
- Everyone to participate because in a real event, it affects everyone
- Do not make assumptions that your IT people will be available
- Do not make assumptions that everyone knows how to use paper

Tabletop Exercises

After Action Report (AAR)

- Record what occurred
- Who was involved?
- What scenarios were tested?
- What decisions were made along the way?
- Lessons learned
- What went right? What went wrong?
- Improvements to be made
- Action Items

Building Your SIRT Team

SECURITY INCIDENT RESPONSE TEAM (SIRT)

The Security Incident Response Team (SIRT) consists of the following primary and alternate members:

	SIRT Team
1	
2	
3	
4	
5	
6	
7	

Enterprise Security Office (CISO)

Internal Support Services (ISS)

Hosting Service Desk (HSD)

Server and Desktop Support Services

Network Support Services

EMR Services Lead

Urgent Process Response Team

CEO

ROLES AND RESPONSIBILITIES

The SIRT's role is to provide a quick, organized and effective response to computer-related and physical breach incidents.

The SIRT's mission is to prevent a serious loss of information, information assets, property, and customer confidence by providing an immediate, effective and informed response to any event involving information systems, networks or workplace.

Team members must be able reprioritize their daily responsibilities to respond to a security incident,

Enterprise Security Office (CISO)	• Determines the nature and scope of the security incident • Contact Insurances and Security Consultants • Contacts the SIRT members • Determines resources necessary to aid in security incident response • Coordinates security incident response efforts • Escalates to management as appropriate • Contacts other departments as appropriate • Monitors and reports on the progress of the investigation to The New York State Department of Health (NYSDOH) • Ensures evidence gathering, chain of custody and preservation is performed as appropriate • Prepares a written summary of the security incident and corrective actions taken • Organizes and participates in Post-Mortem / Lessons Learned meetings

DETECTION AND ANALYSIS
SECURITY INCIDENT HANDLING PROCEDURES

GENERAL SECURITY INCIDENT HANDLING PROCEDURES:
The following is an overview of the general security incident handling procedures. Specific procedures for each phase are located in the corresponding sections of this plan.

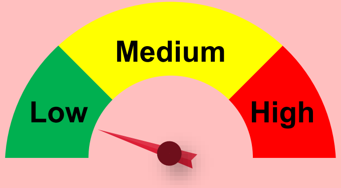
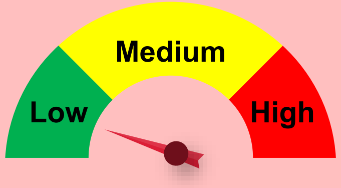
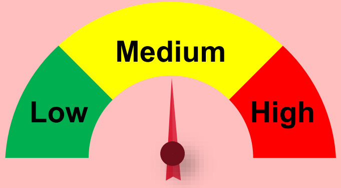
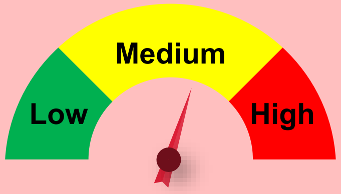
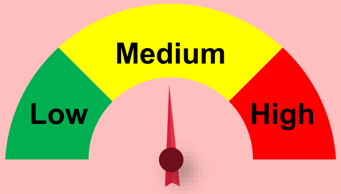
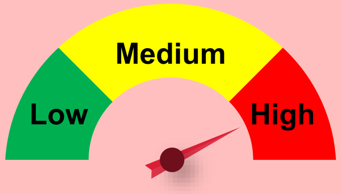
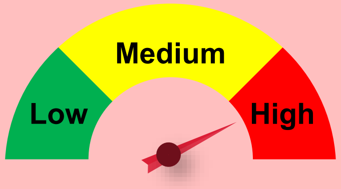
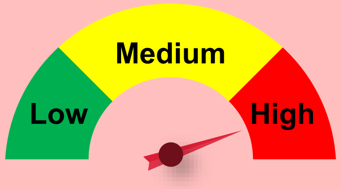
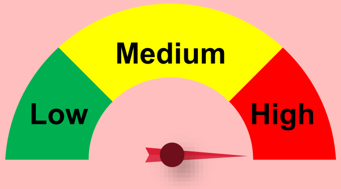
DETECTION AND ANALYSIS

Step	Action	Owner	Completed by
Detection and Reporting			
1	Monitor security tools for incident indicators to detect security incidents.	CISO	
2	Report internally detected incidents		
3	Report detected customer-related incidents		
4	Complete the Security Incident Intake Form.		
5	Verify that an incident actually occurred and determine the incident type (e.g., denial of service, malware, inappropriate use).		
6	Assign initial priority rating (e.g., Urgent, High, Medium, Low).		
Notification			
1	If the CISO is not yet aware of the incident, notify the CISO by sending an e-mail to (Email Address)		
2	Acknowledge the receipt of incident notification.		
3	If the CISO does not acknowledge the incident within the appropriate time period, escalate the incident to the CISO via mobile phone and e-mail.		
4	If the CISO does not acknowledge the incident within the appropriate time period, directly contact the SIRT via e-mail distribution list and contact numbers.		
5	Notification of authorities if needed (Breach Response)		

online

INCIDENT PRIORITIZATION MATRIX

Results. Guaranteed.

Impact: People & Service Severity: Time			Severity		
			3-Low **User cannot perform a portion of their duties**	**2-Medium User cannot perform critical time sensitive functions**	**1-High** **Major portion of a critical service is unavailable**
Impact	**3-Low**	▪ One or two personnel ▪ Degraded Service Levels but still processing within SLA constraints ▪ EMR is still Working with limited available			
	2-Medium	▪ Multiple personnel in one physical location ▪ Degraded Service Levels at or below SLA constraints ▪ Cause of incident falls across multiple functional areas ▪ EMR is down but not infected			
	1-High	▪ All users of a specific services ▪ Personnel from multiple agencies are affected ▪ Public facing service is unavailable ▪ Any item listed in the Crisis Response tables ▪ ePHI is Breached/ EMR is Encrypted			

Maturity Level 2 / Incident Plans

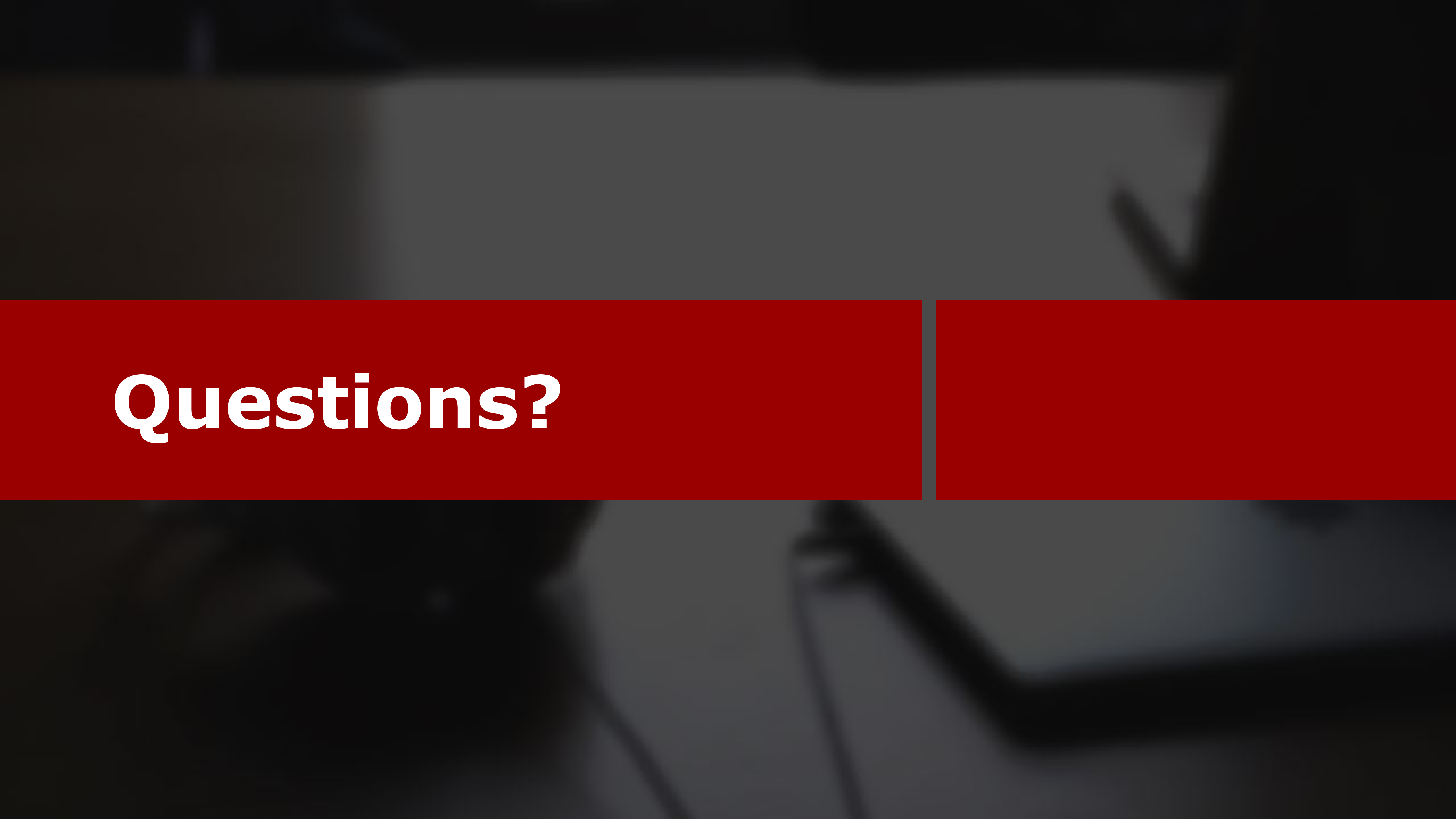
online
HEALTH CYBERSECURITY

Information technology assessments at your Clinic indicate that about 80% of the systems are updated weekly with the latest patches and firewalls, but some systems are months out of date and, for a few, years out of date. Late last evening, all printers throughout your Clinic began to print reams of gibberish. This morning, there are widespread computer-associated problems: computers are slow to boot up; are not loading. The Chief Information Officer received an email from someone claiming to have invaded the system using a Ransomware program and threatened to broadcast the patient information database unless he's paid at least $4 million. Email is not available. Servers are shut down and unable to reboot. Router traffic is unreliable. The Chief Information Technology Officer's assessment is that with consultant support, he can sterilize and return to use about 75% of computers used for documentation in two weeks. Email servers and router traffic will also remain unavailable for at least 4 days. Backups have been contaminated over the previous two months. As the news of these events spreads, there is great interest from local authorities, media, and social media.

Thank You

Shelby Kobes
Skobes@obsglobal.com
Adam Kehler
akehler@obsglobal.com
www.obsglobal.com

Compliance and Assessment (HIPAA) – Online Business Systems (obsglobal.com)



Questions?

Incident Response Workshop:

Tarrytown, NY In-Person Event

Tuesday, March 21, 10AM-4PM

Register Here

Limited availability!

Workshop Evaluation Survey

Please share your feedback on this session. This should take less than 3 minutes to complete.

Survey Link:

https://forms.office.com/Pages/ResponsePage.aspx?id=YSZl7iDhjEqs_lCzVbYzoqmlH89zfFNPhDWTC9uAhXZUOUg0STRCUEdUVjFGTU9BWE1CVE85QUlURS4u