HIPAA Series: Ready for Ransomware?
Follow your Incident Response Plan

Presented by Susan Clarke

Health Care Information Security and Privacy Practitioner

Thursday, September 16, 2021 | 11:00 AM – 12:00 PM

HCCN Health Center Controlled Network

Mountain-Pacific Quality Health

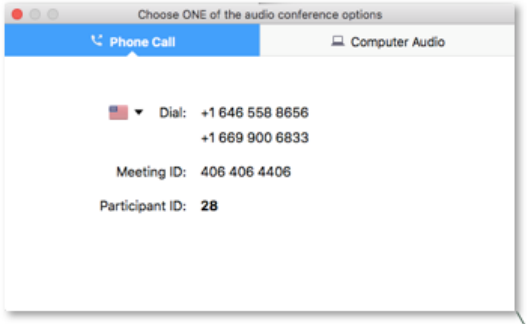
MPCA

Zoom tips and tricks!

CHAT: Please jump in if you have something to share, but we also have this nifty chat function.

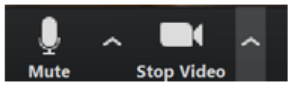
ATTENDANCE: If there are multiple attendees together on the call, please list the names and your location in the chat box

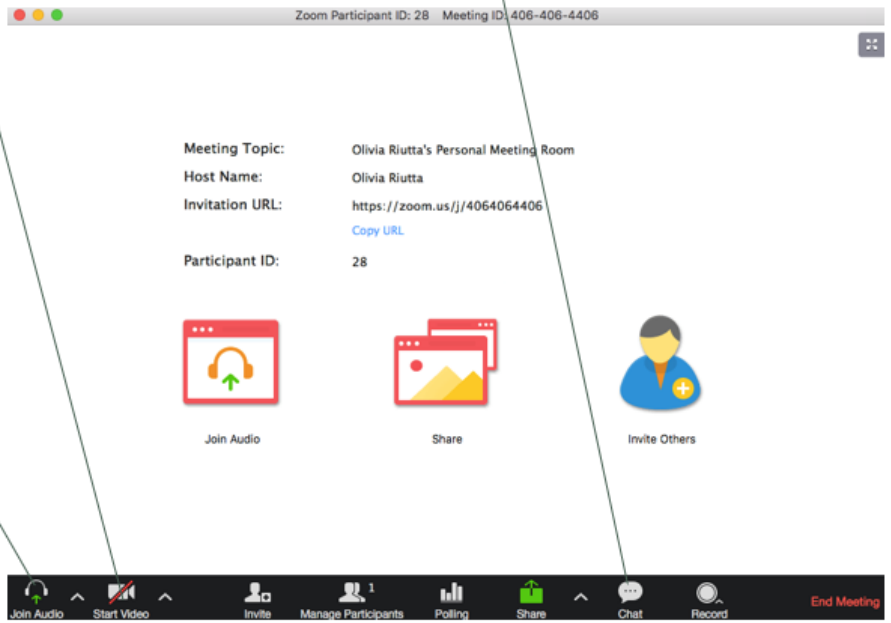
VIDEO: We want to see you!
If your camera isn't on, start your video by clicking here.



AUDIO: You can use your computer speakers or your phone for audio. The phone is generally better quality. If you click "Join Audio," this "Choose one…" box will pop up. If you dial in, just make sure you include your audio code.

MUTE/UNMUTE: *6 or click the mic on the bottom left of your screen.





Susan Clarke, HISPP

Certified Healthcare Information Security $(ISC)^2$ and Privacy Practitioner and Computer Scientist

Conducts privacy and security risk analysis in addition to HIPAA and 42 CRF, Part 2 training.

20 years' experience in health care operations.

10 years' design and coding electronic health record (EHR) software including HL7 Healthcare application development.

Served on IT security, disaster recovery and joint commission steering committee at Mayo Clinic-affiliated health care system.

Legal Disclaimer

The presenter is not an attorney and the information provided is the presenter's opinion and should not be taken as legal advice. The information is presented for informational purposes only.

Compliance with regulations can involve legal subject matter with serious consequences. The information contained in the webinar and related materials (including but not limited to recordings, handouts and presentation documents) is not intended to constitute legal advice or the rendering of legal, consulting or other professional services of any kind. Users of the webinar and webinar materials should not in any manner rely upon or construe the information as legal or other professional advice. Users should seek the services of a competent legal or other professional before acting or failing to act, based upon the information contained in the webinar to ascertain what may be best for the users' needs.

Abbreviations and Acronyms

- BA: Business Associate
- BAA: Business Associate Agreement
- CE: Covered Entity
- CEHRT: Certified Electronic Health Record Technology
- CMS: Centers for Medicare & Medicaid Services
- EHR: Electronic Health Record
- EDR: Endpoint Detection and Response
- ePHI: Electronic Protected Health Information
- HIPAA: Health Insurance Portability and Accountability Act
- HIT: Health Information Technology
- MDR: Managed Detection & Response
- MSP: Managed Service Provider
- NIST: National Institute of Standards and Technology
- OCR: Office for Civil Rights
- PHI: Protected Health Information
- SLA: Service Level Agreement
- SRA: Security Risk Analysis

Learning Objectives

Planning to respond

Practice, practice, practice

Ransomware today

Training your staff

Incident response tabletop

Post ransomware

Important to Make the Right Decision

Pressure when decision needs to be swift

May have nothing to do with technical!

IT and C-suite speak different languages

Often many ways to address

.

How to best communicate with executives

Executives are making decision despite IT best effort to influence

Communication Disconnect

- IT needs to put incident response into business terms using clear language
- IT tends to jump to the technical response
- If incident turn into crisis – large impact
- C-suite is focused on health care operations
- C-suite has increased interest with increased responsibility and need to be informed
- Incidents may lack communication process

Communication Leads to Decisions

1

- Effective incident response plan communications
- Plan is in place. Needs to be strategic

2

- Consider messaging and stakeholders
- Consider purpose, audience, roles and responsibilities

3

- Mechanism will vary based on scenario
- Complicated by “hair on fire” factor

Using managed service provider?

- Outsource with no internal IT
- Need point of contact, name including a backup
- Understand SLAs
- Understand communications strategy
- Health center may want to be involved in the decision making—impact to health center
- May not have communication plan

Cyber Kill Chain

MDR sensors and the security stack to detect and contain threats earlier in the kill chain

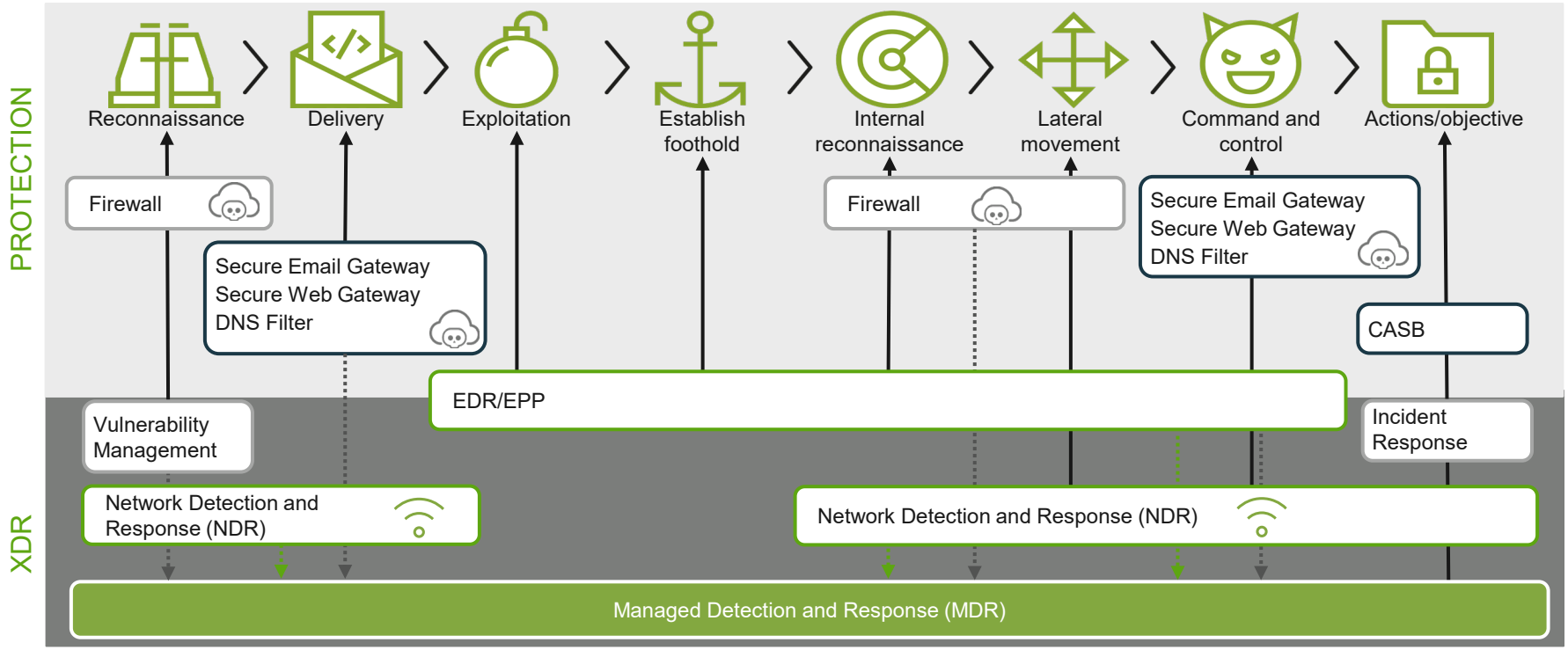


Image used with approval from Robert Kauffman, Senior Sales Engineer, Open Systems

Communications Categories

FUNCTION	CATEGORY UNIQUE IDENTIFIER	CATEGORY
IDENTIFY	ID.AM	Asset Management
	ID.BE	Business Environment
	ID.GV	Governance
	ID.RA	Risk Assessment
	ID.RM	Risk Management Strategy
	ID.SC	Supply Chain Risk Management
PROTECT	PR.AC	Identity Management and Access Control
	PR.AT	Awareness and Training
	PR.DS	Data Security
	PR.IP	Information Protection and Process Procedures
	PR.MA	Maintenance
	PR.PT	Protective Technology
DETECT	DE.AE	Anomalies and Events
	DE.CM	Security Continuous Monitoring
	DE.DP	Detection Processes
RESPOND	RS.RP	Response Planning
	RS.CO	**Communications**
	RS.AN	Analysis
	RS.MI	Mitigation
	RS.IM	Improvements
RECOVER	RC.RP	Recovery Planning
	RC.IM	Improvements
	RC.CO	**Communications**

Communications Categories Within the Respond and Recover Functions of the NIST CSF

CATEGORY	SUBCATEGORY
Communications (RS.CO) Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1** Personnel know their roles and order of operations when a response is needed
	RS.CO-2 Incidents are reported consistent with established criteria
	RS.CO-3 Information is shared consistent with response plans
	RS.CO-4 Coordination with stakeholders occurs consistent with response plans
	RS.CO-5 Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

CATEGORY	SUBCATEGORY
Communications (RC.CO) Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTS, and vendors).	**RC.CO-1** Personnel know their roles and order of operations when a response is needed
	RC.CO-2 Reputation is repaired after an incident
	RC.CO-3 Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

Adapted from nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf *pages 23, 41–44*

Source: A Guide to Effective Incident Management Communications: https://resources.sei.cmu.edu/asset_files/Handbook/2021_002_001_651819.pdf

NIST Recommendations:

Develop and implement incident recovery plan

With defined roles and strategies for decision-making.

Plan, implement, test data backup and restoration strategy

Not only to secure backups of important data but to ensure backups are isolated and immutable.

Maintain up-to-date list of all contacts

For ransomware attacks likely start with cyber insurance contact.

Top Three Recommended

Security Awareness Training for Staff

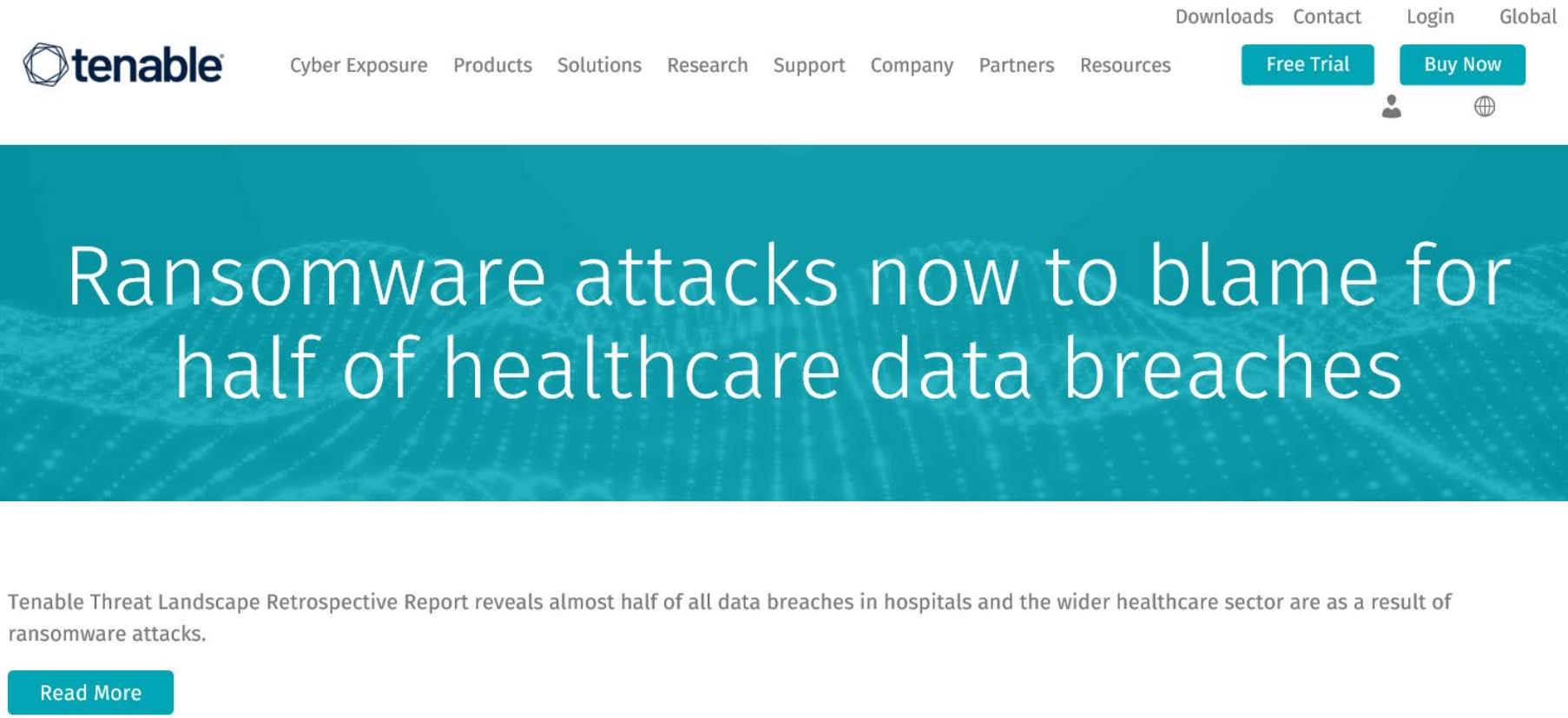
Make this foundational, responsible for lots of ransomware

Advanced Endpoint Detection and Response (EDR)

EDR installed on the endpoint in the event that a malicious link has been clicked (it will happen!)

Overall security strategy including segmentation

For ransomware attacks likely start with cyber insurance contact.



Source: https://www.tenable.com/in-the-news/ransomware-attacks-now-to-blame-for-half-of-healthcare-data-breaches

Why is ransomware so painful?

Encrypts files and holds for ransom

More and more cases of file exfiltration

Impact → panic, helplessness, embarrassment

Forces tough deliberations

Goes beyond technical

Ransomware Examples

Colonial Pipeline

- Darkside ransomware
- Both encryption and data exfiltrated
- Paid $4.4M ransom
- Decipher inefficient; backups required
- Millions estimated for incident response

Universal Health Services

- 400 hospitals, cost $67M
- Wiped out IT, three-week recovery
- Back to pen and paper
- Patients reported delays


PREPARE
& PRACTICE
YOUR PLAN
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

Develop incident response for ransomware

No clear answer on whether to pay ransom

Typically starts with Cyber Security Insurance contact

Identify when to disable and segment networks

Evaluate your backups

Develop your incident response in advance

Time for our tabletop discussion!

Tests communication and decision making – not a replacement for technical testing

Record and check all expectations (do not assume)

Only “failure” is to not learn from the test to make improvements for next time

What does it look like?

For today's tabletop:

1. Facilitator sets scene and describes series of hypotheticals.
2. You are part of incident response team at WeCureU CHC.
3. Audience participates through chat – No wrong answers!

Follow-up at your facility:

1. Follow-up plan – What controls should we implement?
2. Print paper copy of manual/checklist.
3. Report to participants and other stakeholders.
4. Plan your next test.

Scenario #1

September 17, 2021, 3:00 PM
WeCureU Community Health

Your EDR solution has blocked a Word document with malware on the CEO's laptop.

What are the next steps?

Scenario #1
Feedback and Opinions

1. CEO clicked on
2. If possible, send IT to location ASAP
3. Elevate to supervisor

Scenario #2

September 17, 2021, 4:00 PM

WeCureU Community Health

IT staff evaluate CEO's laptop, discover email subject was COVID update with two Word documents. One is blank and was not detected; other contains malware blocked by the EDR.

Is there a cause for concern?

Scenario #2
Feedback and Opinions

- On device means got through – inside
- Are we concerned about the Word document that was NOT blocked?
- Time is critical, assess what may come next
- Should we…
  1) Clean with EDR
  2) Image and wipe
  3) Just wipe
- Is more information needed to make decision?

Scenario #3

September 17, 2021, 6:00 PM

WeCureU Community Health

IT staff does forensics on Word document. Document shows suspicious elements. At the same time logs and alerts show vulnerability has been exploited to allow attacker on our network. New account just created with elevated privileges.

How should we respond?

Scenario #3
Feedback and Opinions

- We now understand what is likely to come next
- CEO double clicked on document; code executed
- If we had wiped, we would also wipe evidence
- Logs provide details like the time the document opened and if opened by others
- Do we now…

1) Delete new suspicious account
2) Shut down network
3) Reset passwords

Scenario #4

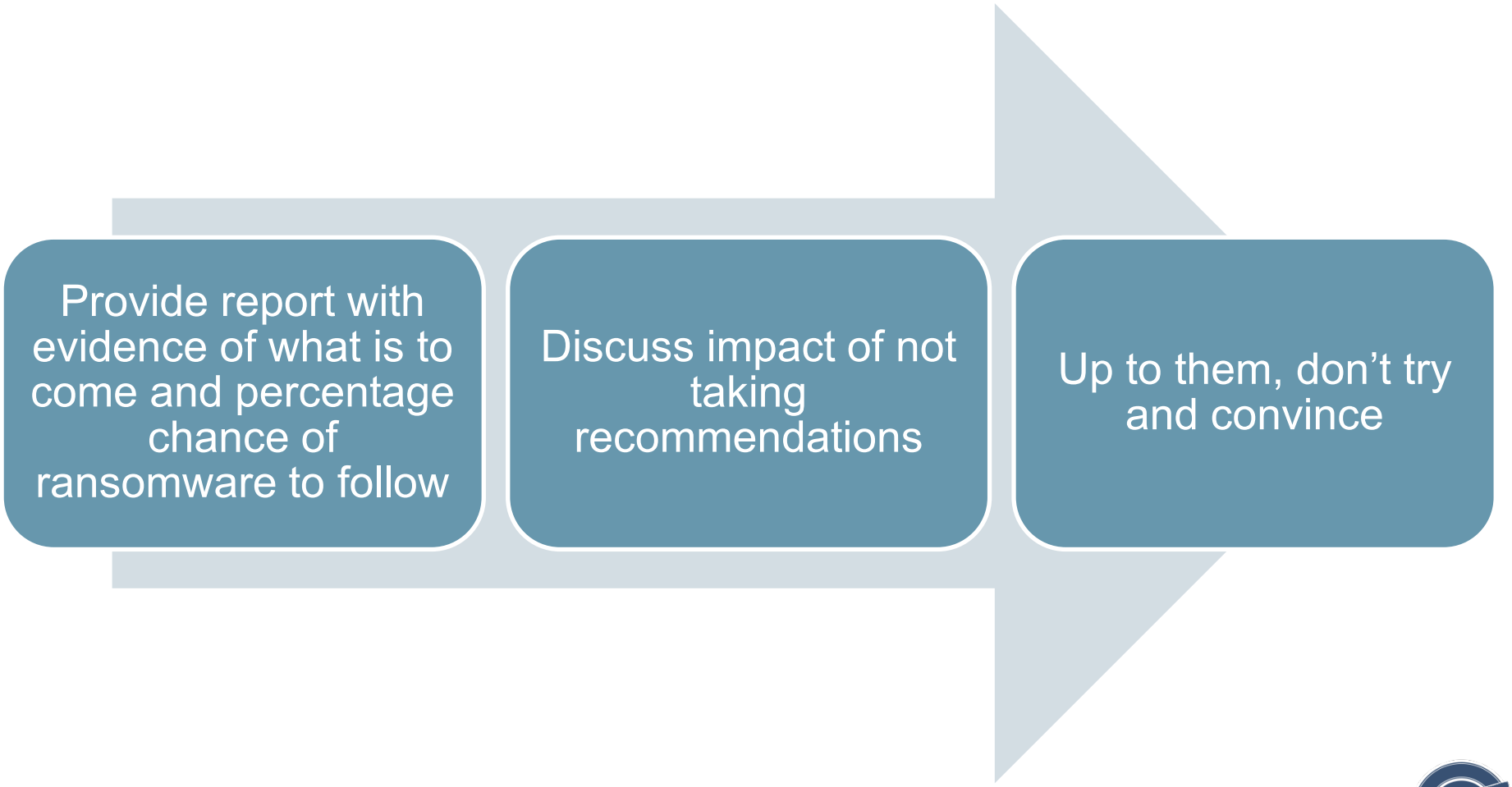
September 17, 2021, 8:00 PM

WeCureU Community Health

C-suite is not convinced that drastic action is necessary. Main concern is patient care and patient safety; health center extremely busy with COVID patients.

What is your response, do you try and persuade?

Scenario #4
Feedback and Opinions



Ransomware Strikes

September 17, 2021, 9:15 PM

WeCureU Community Health

No surprise, files across the network are not accessible and ransomware notes are popping up across user screens. CEO has contacted cyber insurance company to work with the incident response team to handle the next steps.

Post Ransomware

IT staff are working the weekend. The initial plan was to restore from backups, but it is taking too long. The health center is completely on paper. There is a concern they may be forced to close and move patients, including those with COVID, to another facility.

Post Ransomware

C-suite and Board of Directors want your opinion:

1. Yes, pay the ransom
2. No, continue to restore

Post Ransomware

Breach notification

Under state law, HIPAA, Payment Card Industry Data Security Standard (PCI DSS) contracts/ agreements, etc.

Master patient index size matters

Likely over 500 HIPAA threshold

Plan for some staff finding it difficult to go back to paper

Scripting

- Get in front of patient communication
- Have single contact and message, no confliction
- Do not speculate in case you are wrong

HIPAA Safe Harbor Bill

Signed January 5, 2021

Amends HITECH Act ("recognized cybersecurity practices")

Lenient fines if basic safeguard requirements met

- HIPAA Security Rule
- Security risk analysis

Awareness Training: Signs of Malicious Email


To/from/received/reply unconnected


URLs branding slightly off


Disconnected/bogus URLs

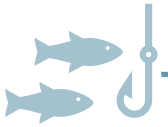

Unexpected file attachments


Internet mail extension type mismatches


Unexpected requests for actions


Stressor claims, sense of urgency

Training and Education



Be aware of phishing and malware.

Be aware of video conferencing security and privacy issues.

Only use approved devices for work.

Keep laptop and software up-to-date.

Check WiFi and VPN connection.

Ransomware Resources

- CISA Ransomware Guidance and Resources
- CISA Ransomware Guide
- DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks
- FBI Ransomware Webpage
- FBI IC3 Webpage for Ransomware
- NIST Tips and Tactics for Dealing with Ransomware
- HHS HC3 Homepage
- 405(d) Ransomware Threat Flyer
- 405(d) Spotlight Webinar- Ransomware
- 405(d) Ransomware Cyber Awareness Flyer
- Ransomware Task Force: Combatting Ransomware Report
- Software Engineering Institute Resources for Preparing and Responding to Ransomware

Ransomware Resource Material

Joint Cybersecurity Advisory, Technical Approaches to Uncovering and Remediating Malicious Activity:

https://us-cert.cisa.gov/sites/default/files/publications/AA20-245A-Joint_CSA-Technical_Approaches_to_Uncovering_Malicious_Activity_508.pdf

FREE KnowBe4 manual used for some of today's content:

https://info.knowbe4.com/ransomware-hostage-rescue-manual-0

HIPAA Ransomware Fact Sheet:

https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

Please let me know how I can help.

For assistance, please contact:

Susan Clarke
sclarke@mpqhf.org | (307) 248-8179

THANKS FOR YOUR VALUABLE TIME TODAY!

Questions