2023 DISASTER PLANNING CONFERENCE SACRAMENTO

UCLA's Health Approach to Preparing for a Ransomware Attack

Alex Lichtenstein
Program Manager, Emergency Preparedness & Business Continuity UCLA Health

California Hospital Association

1

2023 DISASTER PLANNING CONFERENCE SACRAMENTO

UCLA Health Overview

California Hospital Association

2

2023 CHA DISASTER PLANNING CONFERENCE SACRAMENTO

Polling Question:

Has an organization you've worked for been the victim of a cyber-attack?

A. Yes
B. No
C. Don't Know
D. Prefer Not to Say

California Hospital Association

3

2023 DISASTER PLANNING CONFERENCE SACRAMENTO

Briefing Room

Ransomware Attack Prevalence & Magnitude

2018 **14 million** impacted by healthcare attacks

2020 **34 million** impacted by healthcare attacks

2021 **45 million** impacted by healthcare attacks

- *uptick in hacking incidents at **outpatient/specialty clinics***
- ***41%** increase in these types of breaches in 2021 compared to 2020*

*Data from U.S. Department of Health and Human Services (HHS) by healthcare organizations.

2021 Litigation

First litigation involving patient death alleged to be associated with ransomware attack.

THE WHITE HOUSE
WASHINGTON

TO: Corporate Executives and Business Leaders

FROM: Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

SUBJECT: What We Urge You To Do To Protect Against The Threat of Ransomware

DATE: June 2, 2021

The number and size of ransomware incidents have increased significantly, and strengthening our nation's resilience from cyberattacks – both private and public sector – is a top priority of the President's.

Under President Biden's leadership, the Federal Government is stepping up to do its part, working with like-minded partners around the world to disrupt and deter ransomware actors. These efforts include disrupting ransomware networks, working with international partners to hold countries that harbor ransomware actors accountable, developing cohesive and consistent policies towards ransom payments and enabling rapid tracing and interdiction of virtual currency proceeds.

The private sector also has a critical responsibility to protect against these threats. All organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location. But there are immediate steps you can take to protect yourself, as well as your customers and the broader economy. Much as our homes have locks and alarm systems and our office buildings have guards and security to meet the threat of theft, we urge you to take ransomware crime seriously and ensure your corporate cyber defenses match the threat.

4

Briefing Room

Ransomware Attack Prevalence & Magnitude

66% hit by ransomware in the last year

61% attacks resulted in data encryption

69% increase in volume of cyber attacks, highest across all sectors

67% increase in complexity of cyber attacks, highest across all sectors

59% increase in impact of cyber attacks, second-highest across all sectors

94% ransomware attack impacted the ability to operate

90% ransomware attack caused loss of business/revenue

US$1.85M average cost to remediate attack in healthcare, second highest across sectors

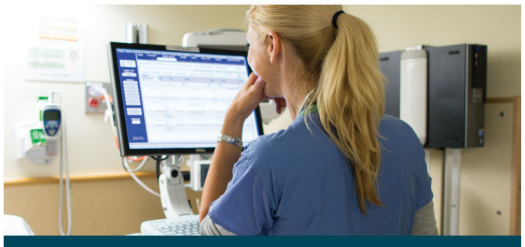
ONE WEEK average time to recover from an attack

77% put faith in approaches that don't prevent an attack

5

2023 DISASTER PLANNING CONFERENCE SACRAMENTO

Cyber Security or Insecurity?



Patient Safety Guidance for

Electronic Health Record Downtime

RECOMMENDATIONS OF THE ELECTRONIC HEALTH RECORD DOWNTIME TASK FORCE

Sentinel Event Alert

A complimentary publication of The Joint Commission — Issue 67, Aug. 15, 2023

Preserving patient safety after a cyberattack

Early one morning, staff at Princeton Community Hospital in West Virginia arrived at work to find ransomware notices on their computers. The hospital had been attacked by the Petya ransomware – a strain of ransomware that encrypts certain files on a computer then demands a ransom payment in exchange for a decryption key. Information on the hospital's electronic health record (EHR) was inaccessible to the hospital's staff, IT systems were unable to retrieve updates, and email was down.[1]

With many of the hospital's existing care systems inaccessible, this type of attack could have been disastrous for staff and for patients. Cyberattacks cause a variety of care disruptions which can lead to patient harm and have severe financial repercussions. Princeton Community Hospital knew exactly what to do.

Within an hour after the attack, the hospital implemented its incident response plan and began using paper and pen to order medications and lab tests. After evaluating the risks to patients, the hospital determined it could remain open, but emergency cases were diverted elsewhere. Surgeries and diagnostics were performed as usual, except for a few patients for which the hospital could not access allergy information.[1]

Using the hospital's cloud backup system and disaster recovery software, the hospital's IT team began running computers again 36 hours after the attack. Having a cyber insurance policy gave them access to experts and companies who provided assistance. While the incident was time-consuming and labor-intensive, its biggest impact was forcing the hospital to replace its hard drives and to patiently work to get all of its systems and related information back online.[1]

Published for Joint Commission accredited organizations and interested health care professionals, *Sentinel Event Alert* identifies specific types of sentinel and adverse events and high-risk conditions, describes their common underlying causes, and recommends steps to reduce risk and prevent future occurrences.

Accredited organizations should consider information in a *Sentinel Event Alert* when designing or redesigning processes and consider implementing relevant suggestions contained in the alert or reasonable alternatives.

Please route this issue to appropriate staff within your organization. *Sentinel Event Alert* may be reproduced if credited to The Joint Commission. To receive by email, or to view past issues, visit www.jointcommission.org.

6

Briefing Room

Federal Support for Ransomware in Healthcare

FOR IMMEDIATE RELEASE
Wednesday, March 8, 2023

Contact ASPR Press Office
asprmedia@hhs.gov
aspr.hhs.gov/newsroom
Twitter:@ASPRgov

HHS Partners with the Private Sector to Enhance Cybersecurity across Health Systems and Address Future Vulnerabilities

Today, the U.S. Department of Health and Human Services (HHS), through the Administration for Strategic Preparedness and Response (ASPR), released a **cybersecurity implementation** guide to help the public and private health care sectors prevent cybersecurity incidents. The *Cybersecurity Framework Implementation Guide* provides specific steps that health care organizations can take immediately to manage cyber risks to their information technology systems.

7

2023 DISASTER PLANNING CONFERENCE SACRAMENTO

UCLA Health Hazard Vulnerability Assessment

- **2021:** Ransomware – 3rd highest
- **2022:** Ransomware – 7th highest
- **2023:** Ransomware – 8th highest

California Hospital Association

8

Unique Cyber-Threat Considerations

IT ICS

IT Security implements the Incident Command System through a Department Operations Center (DOC)

Timing

There can be a significant delay between an attack and detection of the attack.

Massive Surface Area

Any employee with an internet-enabled device is a potential vector for an organization-wide attack.

Ransoms

A decision may need to be made and the logistics arranged regarding ransom payments.

Reputation

Social media, public facing webpages, and the ramifications of a ransomware payment all carry significant reputational weight.

Technical Expertise

Preparedness, detection, response, and recovery require significant technical knowledge from IT partners.

California Hospital Association

9

Polling Question:

Does your organization currently have an operational ransomware response plan?

A. Yes
B. No

California Hospital Association

10

Key Components for Response Playbooks

Response Structures

Activating the response across the organization.

Ransom Decision Making Matrix

Criteria for decisions regarding ransomware and implementation

Cyber Threat Response Playbook

Communications

Internal and External Stakeholders, Marketing and Communications

Reporting

Reporting to FBI, Local Law Enforcement, through UCOP (UC Siren).

California Hospital Association

11

Cybersecurity Response Planning Journey

Today's Goal: **Sharing & Learning**

Executive Session 9/22/21 — **Hospital & Clinic** Lunch 'n Learn: 11/29/21

Tabletops, Assessments, Drills Validate Processes: 2021 -2022

- Downtime Readiness, Tabletops & Assessments: ED, Clinical Lab & Pathology, Supply Chain, OR
- Tabletop Exercises
- Inpatient Downtime Drills

Playbook Initial Draft — **Executive Exercise #2** Session: 9/19/22 — **Playbook** Final

WE ARE HERE

Evidence-based best practice from *Administration on Strategic Preparedness & Response (ASPR)*

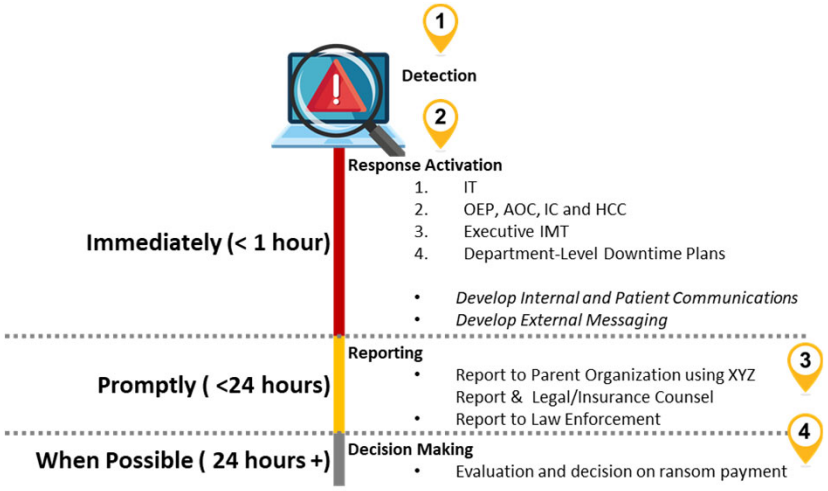
- ✓ **Preparing the People:** Employee Awareness and Cyber Hygiene
- ✓ **Preparing the Organization:** Policies and Procedures
- ✓ **Understanding Vulnerabilities:** Risk Assessments, Continuous Monitoring
- ✓ **Having a Response Strategy:** Training/Preparedness, Communication/Information Sharing
- ✓ **Hardening Cyber Infrastructures:** Access Controls, Redundancy, Patching, Encryption

California Hospital Association

12

Playbook Layout

Timeline across 4 key recommended actions



California Hospital Association

13

2023 DISASTER PLANNING CONFERENCE SACRAMENTO

Scenario to drive the conversation – 1

Saturday, December 24, 2022 at 8:55am: The organization's IT Dept. detects unusual network activity after several clinical staff have failed attempts to log on to EPIC.

- A pop-up notification demanding $20M cryptocurrency payment for decryption keys to the patient health records is reported by several staff throughout the health system.
- Attackers also threaten to release sensitive patient information to the public if payment was not made within 48 hours.
- Upon identifying the unusual network activity, IT SOC reached out to external vendor to begin assessing situation.

California Hospital Association

14

2023 CHA DISASTER PLANNING CONFERENCE SACRAMENTO

Response Structures

How do you set-up and activate the response across your organization?

Immediately (<1 hour)

California Hospital Association

15

2023 DISASTER PLANNING CONFERENCE SACRAMENTO

(Immediately)

Developing your Executive IMT

Critical Task: Consider the formation of an Executive IMT, and discuss 1) who participates 2) how are participants notified 3) how does communication occur with HCC 4) who is the IMT IC

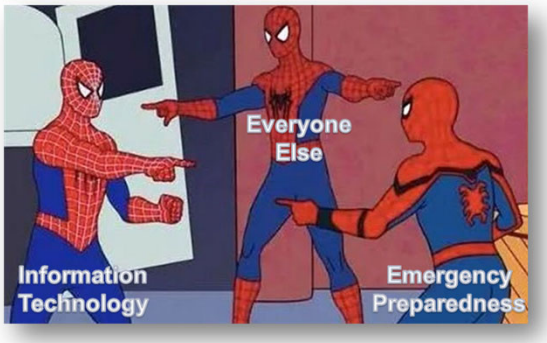
Executive Incident Management Team (IMT)
- Who should be on it, when and how should they be notified?
- Who will serve as IMT commander(s)?
- How should communication occur with hospital command center?
- How will communication flow with hospital command center?

California Hospital Association

16

Who is on your Ransomware IMT?

UCLA Health's Executive Incident Management Team



UCLA Health
- Chief Technology Officer
- Chief Information Security Officer
- Chief Information Officer
- Chief Privacy and Compliance Officer
- Chief Counsel
- Chief Risk Officer
- Vice Chancellor, Health Sciences
- President, UCLA Health
- Chief Nursing Officer
- Chief Financial Officer
- Chief Communications Officer
- Chief Operations Officer
- Chief Medical and Quality Officer
- Dean, School of Medicine
- Director, OEP

Campus
- Legal Affairs
- Chief Information Security Officer
- Dir. Insurance and Risk Management
- Associate VC for Audit and Compliance
- Chief Information Officer
- Strategic Communications
- Associate Vice Chancellor

UCOP
- Emergency Management
- Vice President UC Health
- Chief Legal Counsel
- Chief Risk Officer
- Chief Information Officer

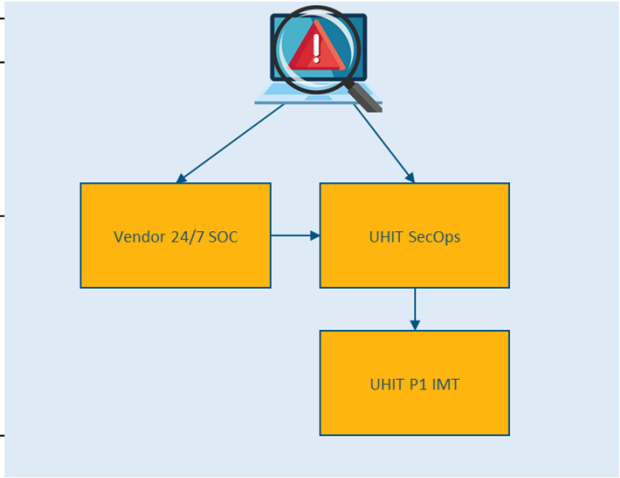
California Hospital Association

17

(Immediately)

Confirmation of Attack

Group	Responsibility
Vendor 24/7 SOC	• Fire Eye/Mandiant
UHIT SecOps	• UHIT SecOps Detection • Continuous Monitoring, Countermeasures, Incident Response, and Digital Forensics • Validation (Scope and Impact) • Initial Action (Isolate and Contain) • Guidance/Management of Release of Information (TLP:RED)
IT P1 IMT	• **Organizational Detection** • Engage 3rd Party Incident Response Retainer • Engage IT Support Groups/3rd Parties as Required • Guidance on Containment and Usage • Validation (Scope and Impact) • Initial Action (Isolate and Contain) • Remediation/Mitigation/Containment • Engagement with Law Enforcement as Requested • Guidance/Management of Release of Information (TLP:RED)



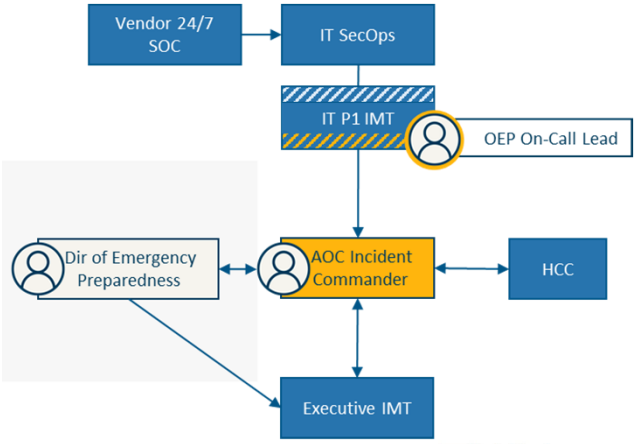
18

(Immediately)

Once confirmed, how are the response groups notified?

Detection → Response

- ✓ OEP On-Call is participating in the IT P1 activation when the attack is confirmed.
- ✓ OEP on-call notifies the AOC and OEP Director of confirmed attack.
- ✓ AOC determines to activate Disaster Response Protocol in order to transition management of the attack to the HCC
- ✓ OEP Director activates the Executive IMT



California Hospital Association

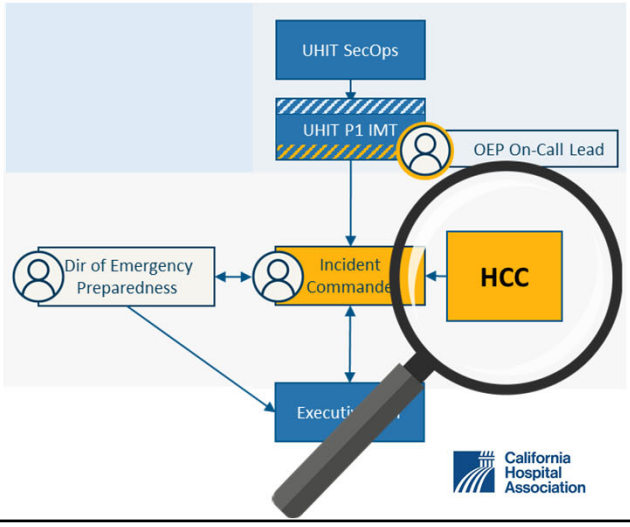
19

(Immediately)

Hospital Command Center (HCC)

Objectives of the Hospital Command Center

- ✓ Maintain safe patient care capabilities
- ✓ Isolate and repair affected information technology systems
- ✓ Notify affected end user supervisory personnel and provide directed guidance on information technology systems use
- ✓ Restore automated systems and services
- ✓ Assess, collect, and escalate organizational impacts to the Executive IMT

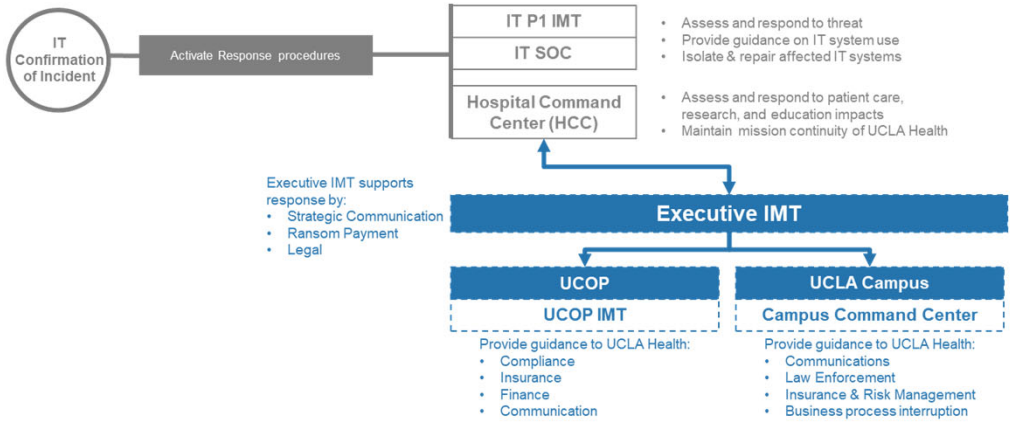


California Hospital Association

20

(Immediately)

Combined Workflows for Response Areas



Critical Task: Consider the formation of an Executive IMT and discuss: 1) who participates, 2) **how are participants notified, 3) how does communication occur with HCC, and 4) who is the IMT commander.**

California Hospital Association

21

Risk Communication

Guiding Principles, Objectives, and Roles

Immediately (<1 hour)

California Hospital Association

22

(Immediately)

Developing Your Risk Communication Guidance

Critical Task: Discuss external messaging and engage public information officers and strategic communications to manage message dissemination and regulation.

Information Sharing Considerations

- What information do we share with:
  - Patients
  - Media
  - Staff/Trainees
  - Partners/Affiliates
- Guidance for PIO?
- Potential impacts to brand and reputation?

** Develop messaging specific to ransomware for your response playbook.*

California Hospital Association

23

2023 DISASTER PLANNING CONFERENCE SACRAMENTO

(Immediately)

Information Sharing & Risk Communication

Objectives of Information Sharing

1. Protect the organization's brand and reputation through adherence to your mission
2. Instill confidence that the organization is managing the emergency responsibly

Communication Approval Workflow & Alternate Methods

✓ Developed by the PIO* and approved by the HCC Incident Commander

✓ Alternative communication methods identified

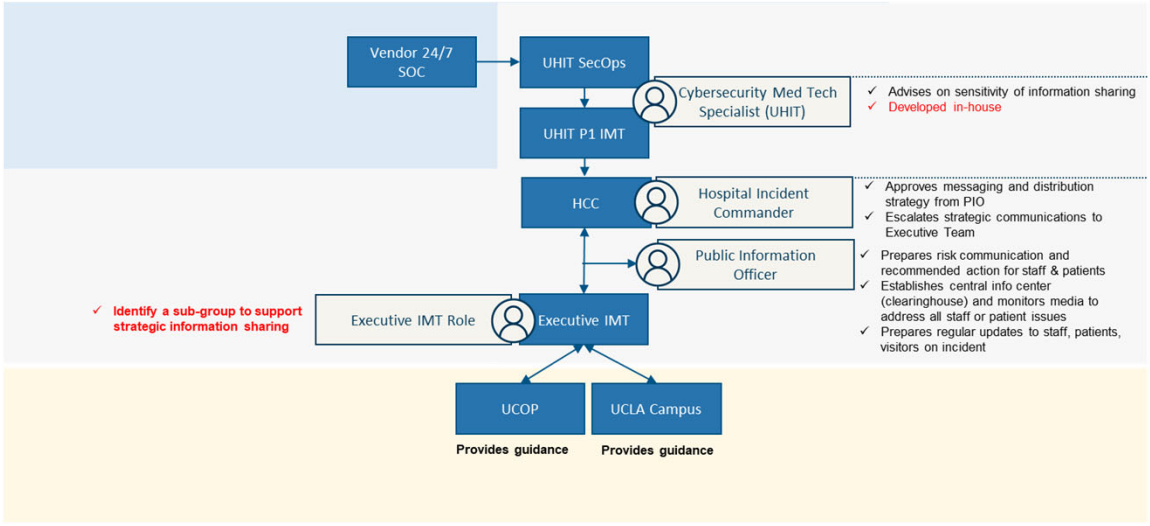
California Hospital Association

** Pre-developed messaging specific to ransomware included in plan (media, internal, public posting).*

24

(Immediately)

Combined Workflows for Information Sharing



25

Scenario Updates

California Hospital Association

26

Scenario update to drive playbook development – 2

After activating response procedures, clinical areas expressed that there is concern about disruption to patient care.

- Additionally, users are reporting that CareConnect, patient portals (e.g., MyChart, Mednet, production databases) are inaccessible in addition to Outlook Email, BOX, Elentra (DGSOM LMS) and our Warehouse Management System.
- Call traffic into the UCLA Health Call Center has increased as patients are unable to login to their patient portals.
- Patient complaints and local news outlets begin to saturate social media with speculation about the incident.

California Hospital Association

27

2023 DISASTER PLANNING CONFERENCE SACRAMENTO

Scenario update to drive playbook development – 3

Hospital Command Centers are active in both hospitals

- Internal and external communication has gone out to address concerns and provide information and guidance for staff
- There are twice daily briefings from the Incident Commander
- Impact information is being collected from the organization and partners
- Resolving issues and developing strategies/workarounds to ensure continuity of mission critical functions

California Hospital Association

28

Polling Question

If the EHR, email, and VoIP communications went down right now, select the time interval that your facility could maintain full operations:

A. We could not maintain full operations without these systems
B. 1 day of downtime
C. 3 days of downtime
D. 1 week of downtime
E. We can maintain full operations without these systems for as long as necessary

California Hospital Association

29

Reporting a Crime

Law Enforcement & Required Notification

California Hospital Association

30

Polling Question

How confident are you in knowing how to report a ransomware attack to law enforcement?

A. Very confident
B. Somewhat confident
C. Not very confident

California Hospital Association

31

(Promptly)

How to Develop Reporting Guidance

Critical Task: Identify and notify appropriate authorities of the attack and continuously serve as liaison between your organization and investigative agencies. Also consider the timing of notification.

Law Enforcement Considerations
- Have we identified all agencies?
- Do we know what resources they bring to the table?
- Are we able to share information as quickly as possible to FBI/local law enforcement?

Other Required Reporting
- Who else needs to know?
- Regulatory, Insurance, Corporate Partners, Affiliates?

California Hospital Association

32

(Promptly)

Reporting Requirements

Report to Parent Organization

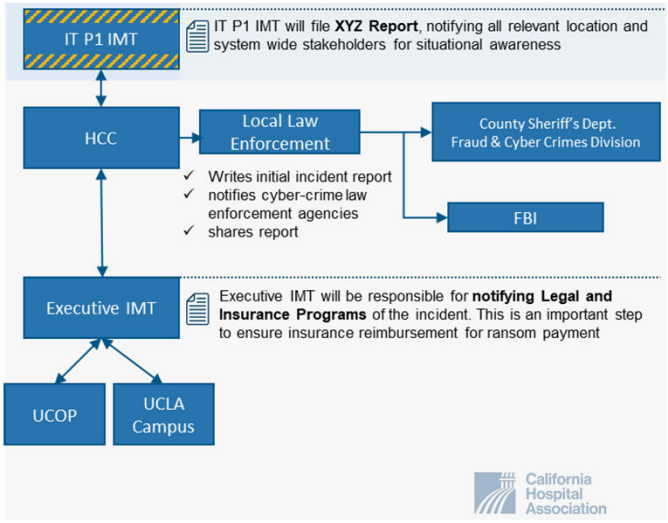
- ✓ File XYZ Official Report
- ✓ Notify sister institutions using ABC Cyber Incident Escalation Protocol Process Map
- ✓ Notify Insurance Programs (requirement for reimbursement)

Report to Law Enforcement

- ✓ Notify local law enforcement of crime
- ✓ Local law enforcement notifies County Sherriff's Fraud & Cyber Crimes Division
- ✓ File complaint with FBI – IC3.gov

Report to CISA

- ✓ Within 72 hours



33

Ransom Decision Making Matrix

How will your leaders make a recommendation to pay or not pay?

When possible (>24 hours)

California Hospital Association

34

2023 CHA DISASTER PLANNING CONFERENCE SACRAMENTO

Polling Question

Who in your organization would make the decision of whether to pay a ransom?

A. CFO
B. Incident Commander
C. CEO
D. Emergency Manager
E. Not sure

California Hospital Association

35

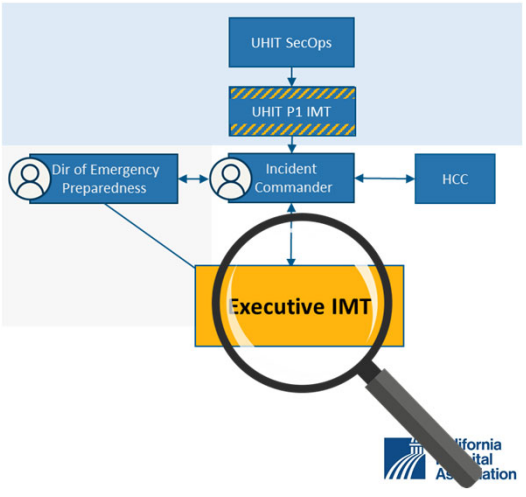
2023 DISASTER PLANNING CONFERENCE SACRAMENTO

(When Possible)

Developing Your Decision-Making Guidance

CRITICAL TASKS

- ✓ Review legal and insurance policy requirements to guide ransom payment decision
- ✓ Use impact assessment information to inform risks and reward surrounding ransom payment decision
- ✓ Identify who has authority on your Executive IMT to make a **decision** or **recommendation** to pay ransom



36

(When possible)

Impact assessment roll-up to Executive IMT

Situation Status Report focus areas:

- Patient Care
- Research
- Medical Education
- Community Service Initiatives
- Continuity of Administration
- Financial Viability of the Organization
- Brand and Reputation
- Relationships with partners and stakeholders
- Impacts to safety and security of the broader community
- Maintain strong and visible leadership

UCLA Health

Situation Status Report | MM/DD/YYYY | Updated 00:00

Impact Area / Responsible for Identifying	Identified Impacts
Patient Care HCC Staff	• All service lines are open • Full paper downtime (charting, orders, documenting) o Unit based documentation are maintained for 24 hr. par level o Replenishment of forms becoming a concern o Depts. are struggling to keep up with paper management and are requesting filing cabinets and secured location to maintain patient records • Inefficiencies related to paper ordering, charting, & resulting processes are resulting in delays and increased frustration among staff & patients o Two medication administration errors reported related to the downtime (pediatric wrong dose, adult wrong patient) • Incomplete paper requisitions submitted to (Lab, Pharmacy, Radiology) are resulting in significant patient care delays • Patient Placement & Admissions are struggling to keep up with new admissions, transfers, & discharges utilizing a paper system
Research Vice Dean of Research, DGSOM	• Researchers reporting a myriad of issues related to lack of access to data maintained in BOX and Outlook Email
Medical Education Vice Dean of Research, DGSOM	• Remote students are unable to access course material on Elentra and requesting alternate accommodations to keep up with course work • Medical trainees reporting to their Union that they are ill-prepared for downtime
Community Service Initiatives HCC Staff	• Pending
Continuity of Administration Executive IMT Staff	• Continuity of Administration over the core mission areas
Financial Viability of the Organization CFO, Finance Section Chief	• Automated billing processes in CareConnect have been down for 24 hours o Charges have not been captured and no ETA for manual process to reconcile
Brand and Reputation Executive IMT Staff	• Significant brand and reputation impacts have been reported o Public scrutiny in media and social media posts are describing poor patient experience. o Significant reports of patient's threatening to find care elsewhere are being escalate to the command center.
Relationships with partners and stakeholders HCC Staff / Executive IMT Staff	• Affiliate health care partners have isolated their IT network from UCLA Health's out of an abundance of caution • Corporate sponsorship partners have reached out to determine the risk and vulnerability related to their client's privacy and data security
Impacts to safety and security of the broader community HCC Staff	• Ability to meet the needs of the community is being evaluated o Higher level of care transfers o Transplant volume o Blood donations
Maintain strong and visible leadership HCC Staff	• Messaging is largely effective demonstrating strong leadership presence • Staff and faculty leadership who are on holiday travel are struggling to provide remote leadership support due to loss of IT systems

37

(When possible)

Cyber Insurance Policy

- **How much are you insured for?**
  - What is your deductible?
- **Is your insurance dependent on you adhering to specific standards, policies, or guidelines?**
- **What is covered under your insurance program?**
  - *EXAMPLES: Lawsuit liability, business interruption, 3rd party legal counsel, incident response, and crisis communication support related to breach*

University of California – Policy BUS-80

Insurance Programs for Institutional Information Technology Resources

Responsible Officer:	Chief Risk Officer
Responsible Office:	RK - Risk / EH&S
Issuance Date:	12/17/2018
Effective Date:	12/17/2018
Last Review Date:	11/29/2018
Scope:	This policy applies to all of the following: • All UC campuses and medical centers, the UC Office of the President, UC Agriculture and Natural Resources, and all other UC locations (Locations). • All Workforce Members, Suppliers, Service Providers and other authorized users of Institutional Information and IT Resources. Note: This policy does **not** generally apply to students who are not Workforce Members. • All use of Institutional Information, independent of the location (physical or cloud), ownership of any device or account that is used to store, access, process, transmit or control Institutional Information. • All devices, independent of their location or ownership, when connected to a UC network or cloud service used to store or process Institutional Information. • Research projects performed at any Location and UC-sponsored work performed by any Location.

Contact:
Title:
Email:
Phone:

TABLE OF CONTENTS

1 of 7

California Hospital Association

38

(When possible)

Making the Ransom Payment

- Authority
  - Executive IMT Leadership Group
    - Identify a subset of this group with final decision making/recommendation authority
- Risk Management and Legal Counsel
  - Many insurance programs that cover ransomware response assist with identification of third party vendor to convert funds to cryptocurrency and complete transfer of payment or otherwise meet ransom demands

California Hospital Association

39

Polling Question

Does your organization need a ransomware response plan?

A. Yes
B. No
C. Not sure

California Hospital Association

40

Questions

California Hospital Association

41

Thank You

Email: ALichtenstein@mednet.ucla.edu

Phone: (310)923-5140

California Hospital Association

42