
Don't be the Next...
Cyber War Games Simulation

Don't be the Next...Cyber War Games Simulation

Panelists

Craig Horbus
Partner
Dinsmore

Kevin Baker
CISO
Fortress Security
Risk Management

Ben Brugler
CEO
Akhia

Herb Stapleton
Retired Special Agent
FBI Cyber

Moderator

Will Hudec
Director, Security Consulting
Fortress Security
Risk Management

Dinsmore

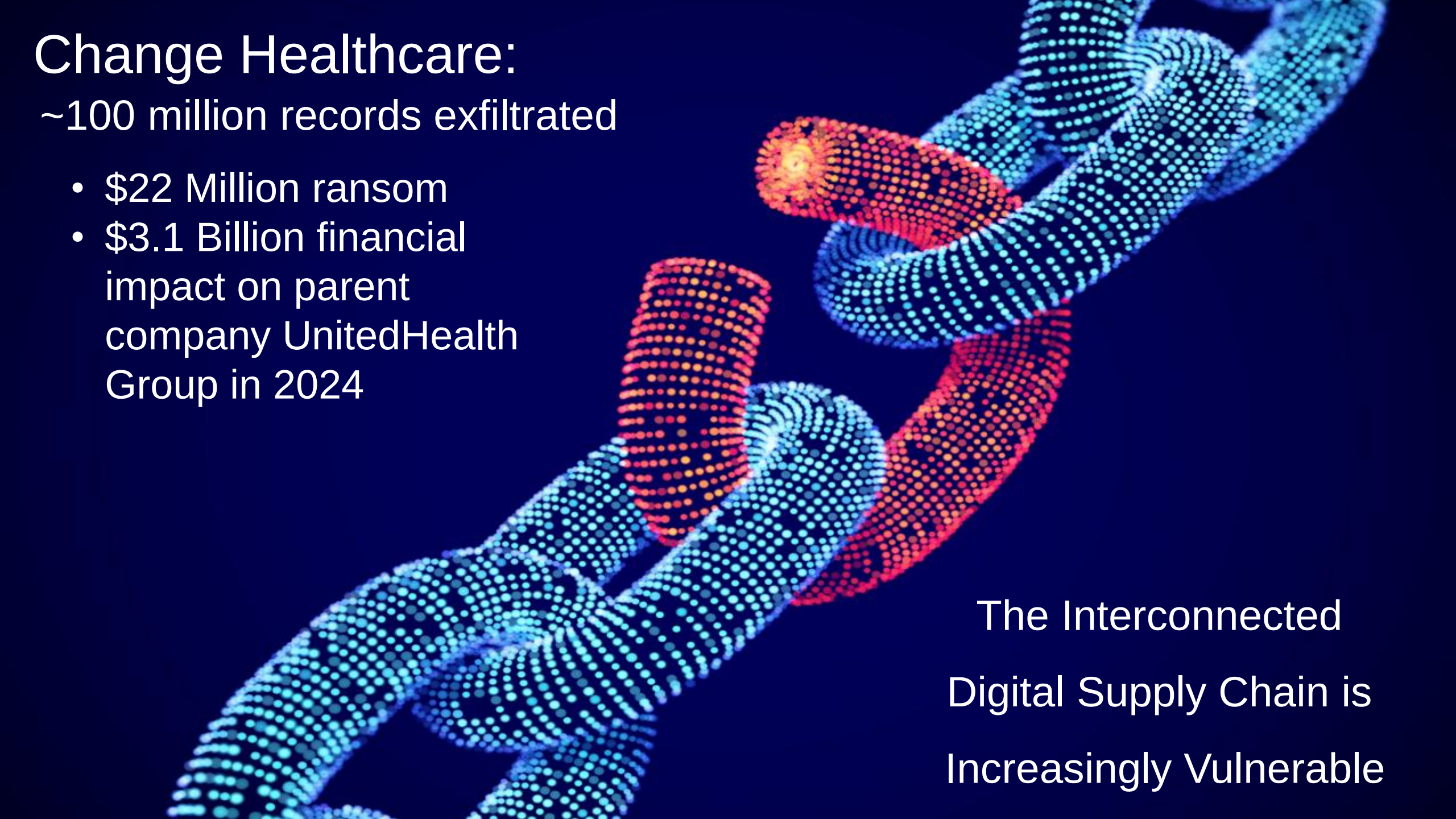
AKHIA

FORTRESS
SECURITY RISK MANAGEMENT
FULCRUM IT PARTNERS

Change Healthcare:

~100 million records exfiltrated

- $22 Million ransom
- $3.1 Billion financial impact on parent company UnitedHealth Group in 2024



The Interconnected Digital Supply Chain is Increasingly Vulnerable

Big Healthcare Hacks 2024

Kaiser Foundation Health Plan:
13.4M records

Ascension Health:
142 hospitals/ 5.6M records

Concentra Health Services:
~4M records

HealthEquity:
4.3M records

Source: 2024 HIPAA Journal

2024: >184 Million Health Records Exfiltrated = 53% of U.S. Population

Why Attack Healthcare ?

High Value:

- PHI
- Whole Databases
- Research Data
- Prescription & Pharmacy Records
- Insurance & Billing Information

Uses:

- Identify Theft & Fraud
- Financial Gain
- Blackmail & Extortion (Ransomware)
- Phishing & Scams
- Espionage

Source: GuidePoint Security Research and Intelligence Team (GRIT]
https://www.hipaaguide.net/healthcare-ransomware-attacks-increased-in-q1-2025/

What's the Risk?

- Unavailable Data
- Disrupted Patient Care & Scheduling
- Surgeries on Hold
- ER Arrivals Diverted
- Rx & Rx Systems Impacted
- Employees, Doctor Groups & Vendors affected


Ransomware Attacks are a Healthcare Emergency.
What would you do?
AMBULANCE
MEDIC
43

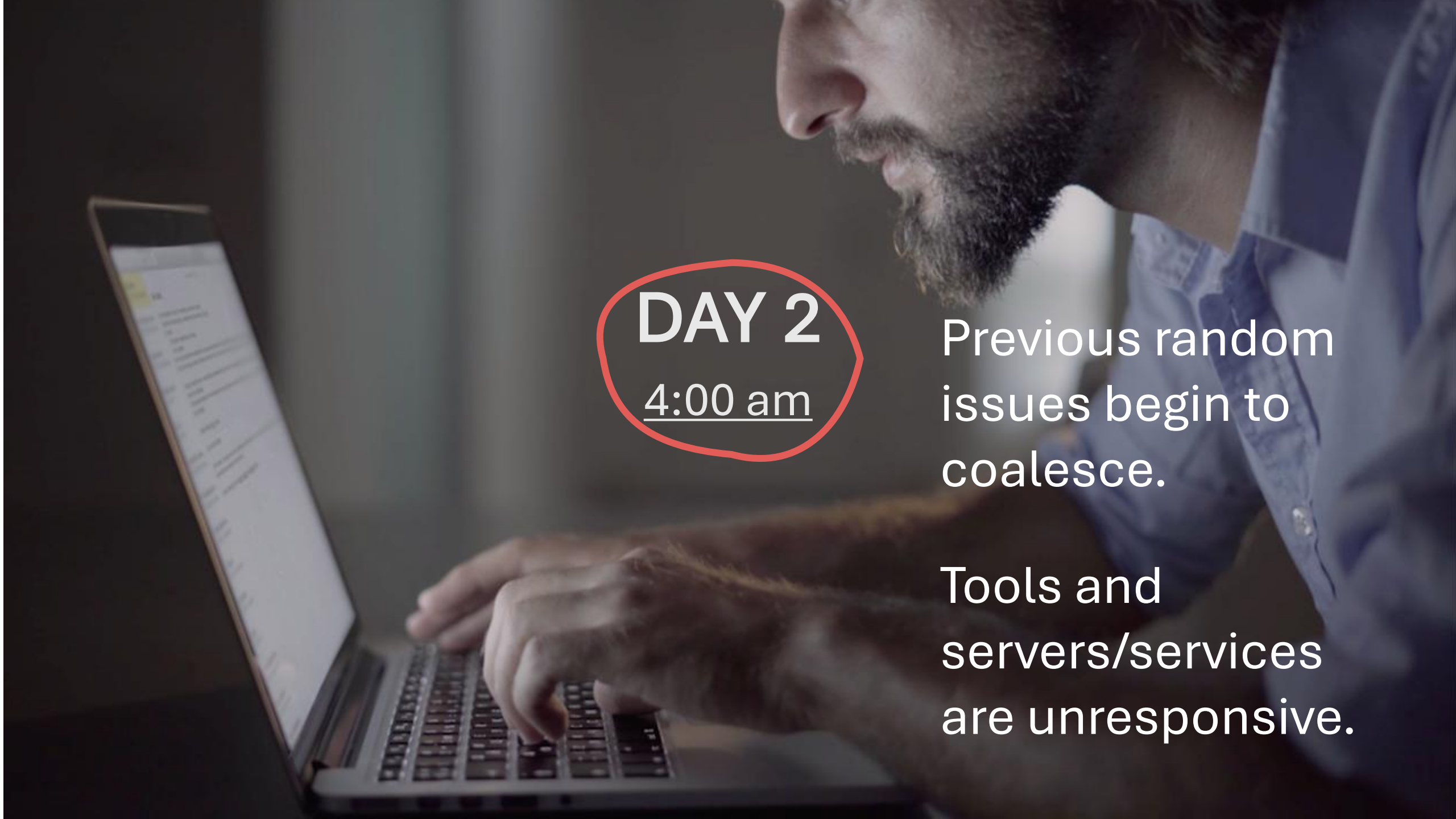

Simulation Scenario:
Aggressive Phishing
Allows Unauthorized
Access into Your Network.

DAY 1

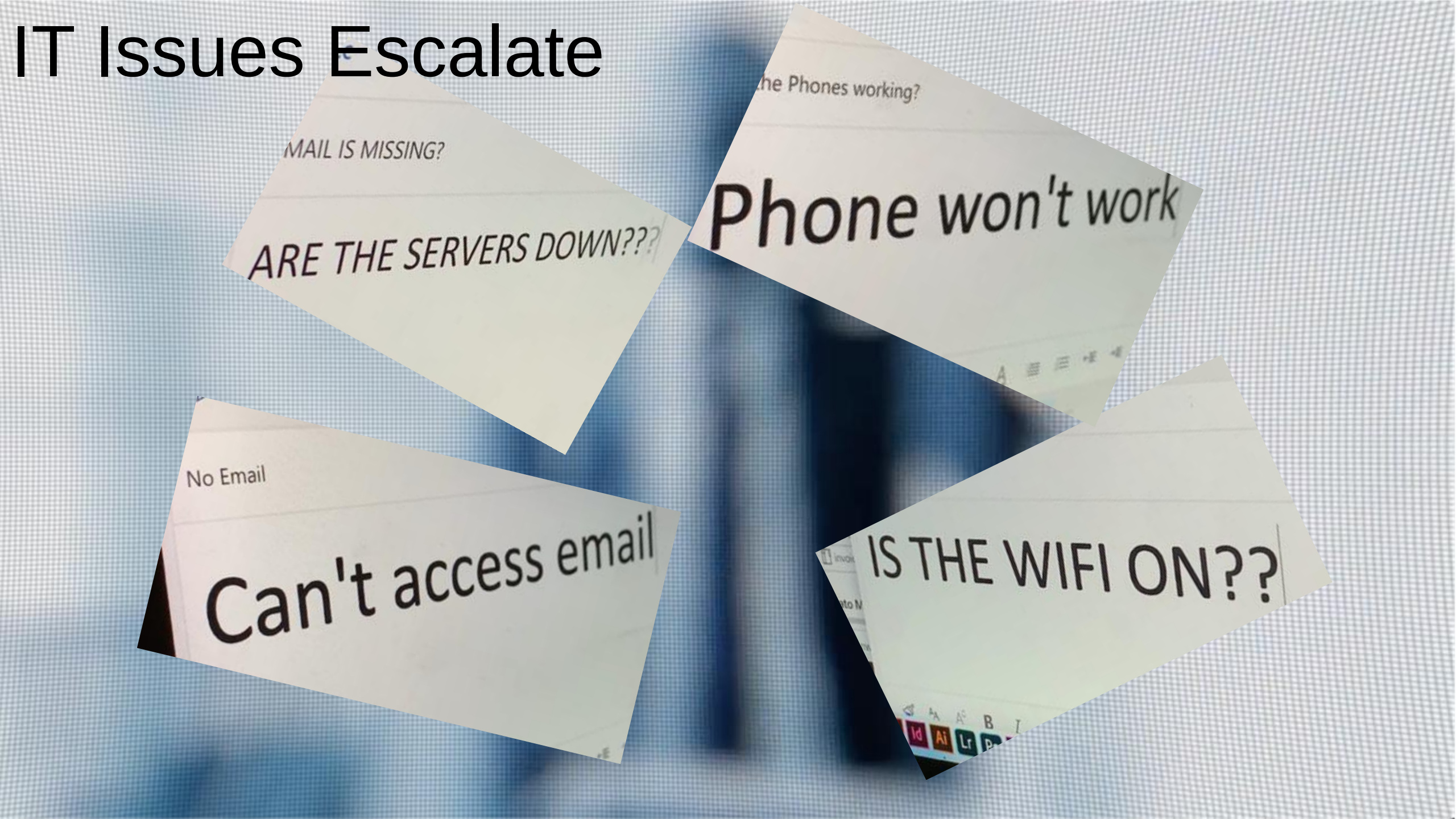
- Staff cannot access data on some file shares
- Growing number of help desk tickets
- Early Evening - IT is not responding

SUN	MON	TUES	WED	THUR	FRI	SAT
		Day 0	Day 1 6pm			

Troubling developments are unfolding…


DAY 2
4:00 am
Previous random issues begin to coalesce.
Tools and servers/services are unresponsive.

IT Issues Escalate



IT and security teams are on alert…

- Exactly what systems are affected?
- Have we stopped the issue?
- What's the impact?

Logging into one of the servers locally, **an IT admin finds a ransom note**…

Ransomware Attack:

After stealing key data, cyber criminals encrypt your network and extort your hospital for payment.

What do you do now?

All hospital systems are encrypted…

No patient care data is available…

All data driven services are frozen…

Do you declare an incident?

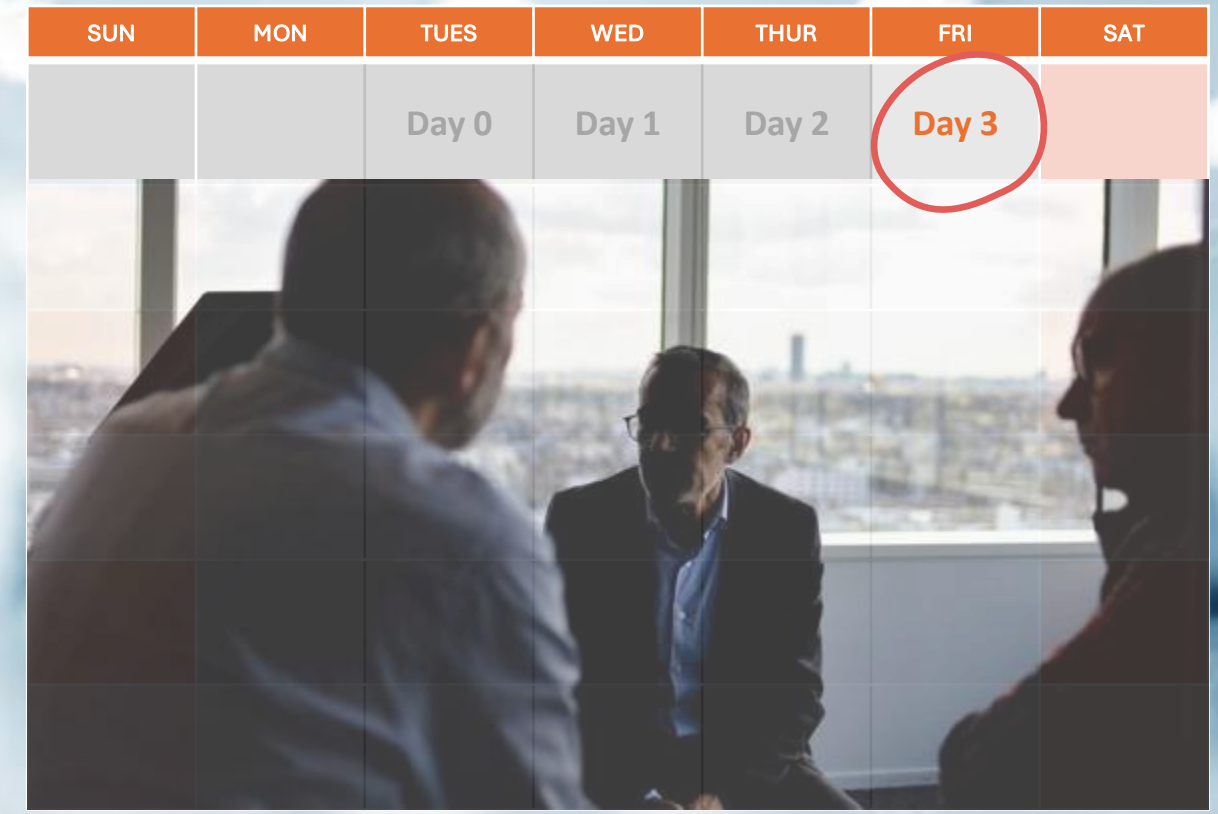
Do you have a written Incident Response Plan?

Have you practiced it?

Do you have out of band crisis communications ready to activate?

DAY 3

- IT is trying to pick up the pieces:
  - External firms enlisted to assist
  - Digital forensics and initial investigation begin but take time



The hospital is at a standstill – do you pay the ransom or not?

What are your options?

After declaring an incident…who must be notified?

- HHS/OCR
- State Attorneys General
- Federal/International
- Media

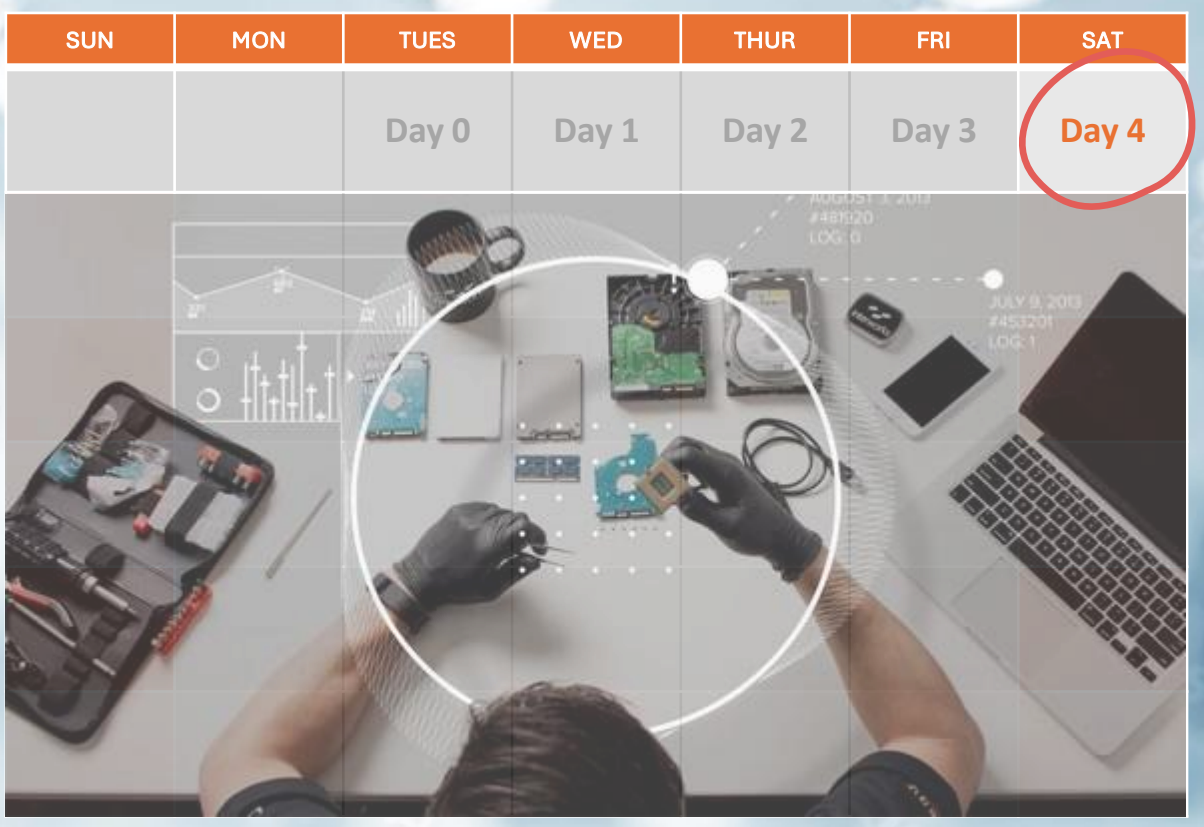
What is the penalty?

Plus, follow-up OC R investigations

	Annual Penalty Limit	Minimum Penalty per Violation	Maximum Penalty per Violation	Annual Penalty Cap
Tier 1	Lack of Knowledge	$141	$35,581	$35,581
Tier 2	Reasonable Cause	$1,424	$71,162	$142,355
Tier 3	Willful Neglect	$14,232	$71,162	$355,808
Tier 4	Willful neglect (not corrected within 30 days	$71,162	$2,134,831	$2,134,831

DAY 4

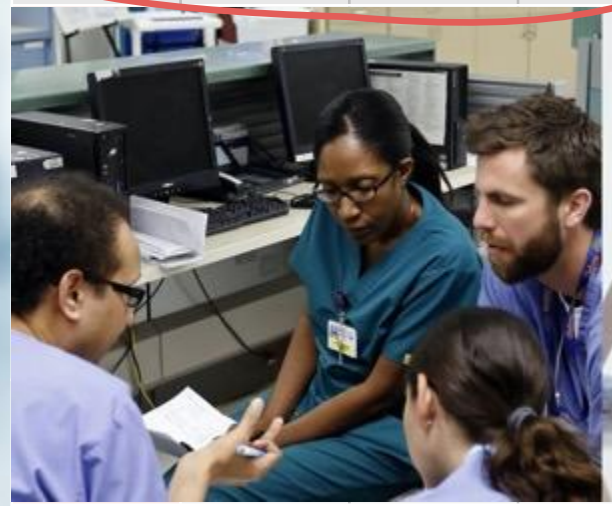
- Containment process is underway
  - This must be achieved before any restoration plans are implemented
  - Restoring to a compromised environment will exacerbate issues



DAYS 5-8

- Recovery is underway, and systems are slowly beginning to come back online
- Hospital operations remain disrupted, but some processes are gradually resuming

SUN	MON	TUES	WED	THUR	FRI	SAT
		Day 0	Day 1	Day 2	Day 3	Day 4
Day 5	Day 6	Day 7	Day 8			

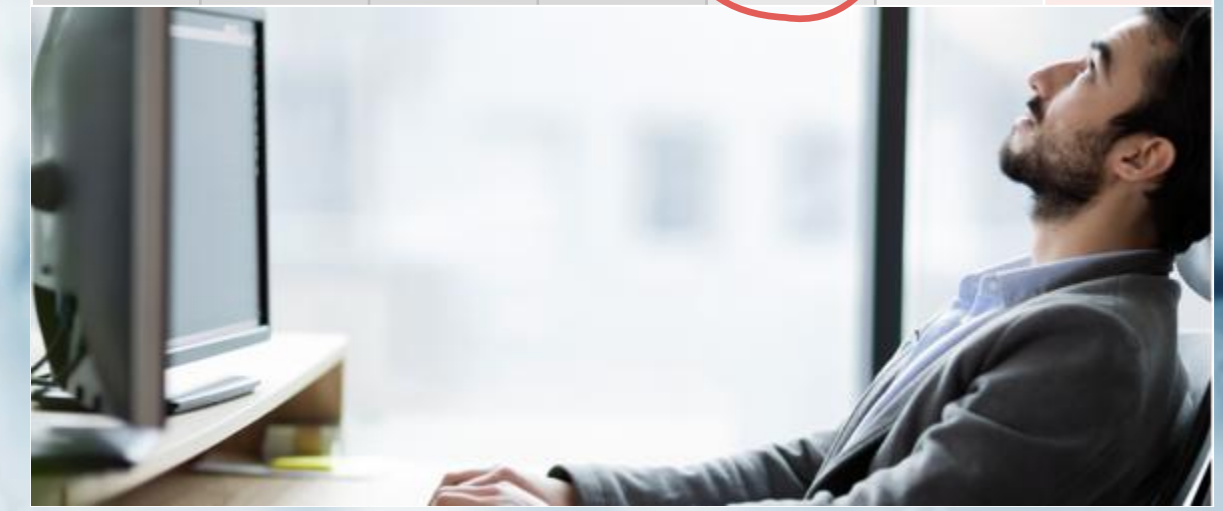


DAY 9

- Most systems are back online
- The IR team has identified critical issues requiring immediate attention to prevent further attacks

What happens now?

SUN	MON	TUES	WED	THUR	FRI	SAT
		Day 0	Day 1	Day 2	Day 3	Day 4
Day 5	Day 6	Day 7	Day 8	Day 9		



Parting Thoughts:

- Legal
- Communications
- Law Enforcement
- Cybersecurity

Questions?

Panelists

Craig Horbus
Partner
Dinsmore
craig.horbus@Dinsmore.com

Kevin Baker
CISO
Fortress Security
Risk Management
kbaker@FortressSRM.com

Ben Brugler
CEO
Akhia
ben@akhia.com

Herb Stapleton
Retired Special Agent
FBI Cyber

Moderator

Will Hudec
Director, Security Consulting
Fortress Security
Risk Management

Dinsmore

AKHIA

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

FORTRESS®
SECURITY RISK MANAGEMENT
FULCRUM IT PARTNERS