RISK RANSOMWARE RESILIENCE

THE NEXT GENERATION OF PATIENT SAFETY

GreyCastle security

RISK RANSOMWARE RESILIENCE

THE NEXT GENERATION OF PATIENT SAFETY

REG HARNISH
CHIEF EXECUTIVE OFFICER
GREYCASTLE SECURITY

SHEETAL SOOD
SENIOR EXECUTIVE COMPLIANCE OFFICER
NEW YORK CITY HEALTH + HOSPITALS

GreyCastle security

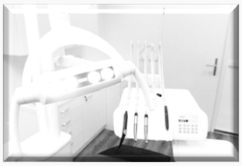
RISK UNIVERSE

CLINICS

PHARMACY

NUSING HOME

EHR



BIOMEDICAL DEVICES

ER

GreyCastle security

TRADITIONAL IT SYSTEMS AND APPLICATIONS

- Electronic Health Record Applications
- Clinical Systems
- Medical Billing/Claims Processing Applications
- Email Applications
- HR Applications
- Network File Sharing Applications
- Payment Processing Systems
- Financial Management/Reporting Applications

Point: Consider all possible traditional IT systems that could have sensitive data.

GreyCastle security

BIOMEDICAL DEVICES

- Patient monitoring devices, smart rooms
  - Smart medical devices, infusion pumps, ventilators, incubators, telemetry, medical imaging
  - Electrocardiogram (ECG), pulse oximetry, ventilators, capnography monitors
  - Pulmonology machines
  - Smart beds, fall detection
  - Remote ICU telemetry, Tele-ology

- Remote wellness and chronic disease management
  - Pacemakers, defibrillators and neuro-stimulators
  - Wearable wristbands, bio-patches, smartwatches, clinical monitors pio meter, pulse oximeter

Point: No longer an "IT issue." Compromise of biomedical equipment directly affects patient safety.

GreyCastle security

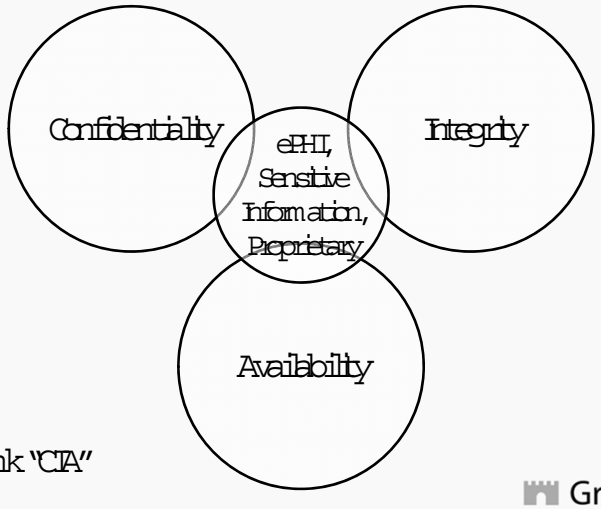
INTERNET OF THINGS

- Facilities Security, Building Management
  - Video surveillance, door locks and entry systems, and fire alarms
  - Power monitoring, power distribution, energy consumption and management, and elevators
  - HVAC, lighting, room control, water quality, humidity monitoring, tissue and blood refrigeration
  - Asset tags
- Networking Hardware, Software, Security, Services
  - Routers, Switches, LAN, Wireless routers
  - Operating systems, Network Security and Services

Point: Think beyond the known systems and applications. Don't forget background systems and infrastructure.

GreyCastle security

AND THE RISKS ARE...



Point: Think "CIA"

GreyCastle security

RISK ASSESSMENT FUNDAMENTALS

- Likelihood: The inherent probability of a threat occurring, without considering existing controls
- Impact: The potential significance of a threat, without considering existing controls
- Risk Factor: The estimated percentage of unmitigated risk, considering existing controls
- Critical Output: Risk Register

Point: Must have asset-threat-vulnerability-impact to have risk.

GreyCastle security

RISK ASSESSMENT FOR HEALTHCARE

CRASH COURSE

1. DETERMINE SCOPE AND RISK UNIVERSE

2. IDENTIFY DATA SOURCES

3. FINALIZE RISK CATEGORIES TO BE ASSESSED

4. EVALUATE CONTROLS FOR RISK MITIGATION

5. CALCULATE RISK SCORES AND PRIORITIZE

6. CATEGORIZE KEY COMPLIANCE PROGRAM CONTROLS

7. IDENTIFY CONTROL GAPS AND DEFICIENCIES

8. SUBSTANTIATE RISK ASSESSMENT RESULTS WITH SENIOR MANAGEMENT

9. IMPLEMENT CORRECTIVE ACTION PLAN

10. INCORPORATE RESULTS INTO REVIEWS AND MONITORING

NIST RISK ASSESSMENT PROCESS

- Finalize Information Asset Inventory
- Identify Threats & Vulnerabilities
- Determine Likelihood & Impact
- Determine Risk Level
- Determine Risk Treatment

Point: Comprehensive risk assessment is to determine how sensitive information may be compromised.

Risk may be: 1) Accepted 2) Mitigated 3) Transferred 4) Avoided

GreyCastle security

RISK ASSESSMENT: BIOMEDICAL EQUIPMENT

Scenario: A mid-size hospital system with one ambulatory care unit and a small long-term care unit wants to start an audit of their biomedical devices. Such an audit has never been performed before.

Challenge: Where to begin? How do I assess risk?

GreyCastle security

RISK ASSESSMENT: BIOMEDICAL EQUIPMENT

Issues		Resultant Risks
1. Inaccurate Inventory	⇨	1. Scope and Universe of assets not known
2. Improper Data Management	⇨	2. Unauthorized access, use or disclosure
3. Inadequate Security Controls	⇨	3. Unauthorized access, use or disclosure
4. Insufficient Physical Controls	⇨	4. Unauthorized access, use or disclosure
5. Lack of System Hardening	⇨	5. Unauthorized access, use or disclosure
6. Insecure Transmission	⇨	6. Unauthorized access, use or disclosure

GreyCastle security

RISK ASSESSMENT: BIOMEDICAL EQUIPMENT

Audit Methodology

- Inventory: Accurate, Current, Prioritized assets list
- Data: Nature, Quantity, Storage State
- Security Capabilities of Device: Access control, Logs, role-based access
- Physical controls: Locks, Secure spaces
- System Controls: Patches, updates, system hardening
- Insecure Transmission: Removable drive or solid-state drive, peripheral, printing, network connection

Final Outcome: * Risk Chart with Assets Prioritized by Risk
* Risk Owner
* Short-term and Long-term Mitigation Plans

GreyCastle security

RISK MANAGEMENT FOR HEALTHCARE

FINAL THOUGHTS

RISK MANAGEMENT

AFFECTS PATIENT SAFETY

IF YOU ARE NOT MEASURING

YOU ARE NOT DOING

RISK ASSESSMENTS
ARE REQUIRED REGULARLY

RISK ASSESSMENTS DO NOT
PREVENT INCIDENTS

CODE BLUE CLEAR

HOW ONE HOSPITAL SURVIVED THE BIGGEST RANSOMWARE ATTACK IN U.S. HISTORY

@REGHARNISH

GreyCastle security

CODE BLUE CLEAR

HOW ONE HOSPITAL SURVIVED THE BIGGEST RANSOMWARE ATTACK IN U.S. HISTORY

@REGHARNISH

GreyCastle security


CBSN ON ASSIGNMENT
ECMC
ERIE COUNTY
MEDICAL CENTER
Welcome

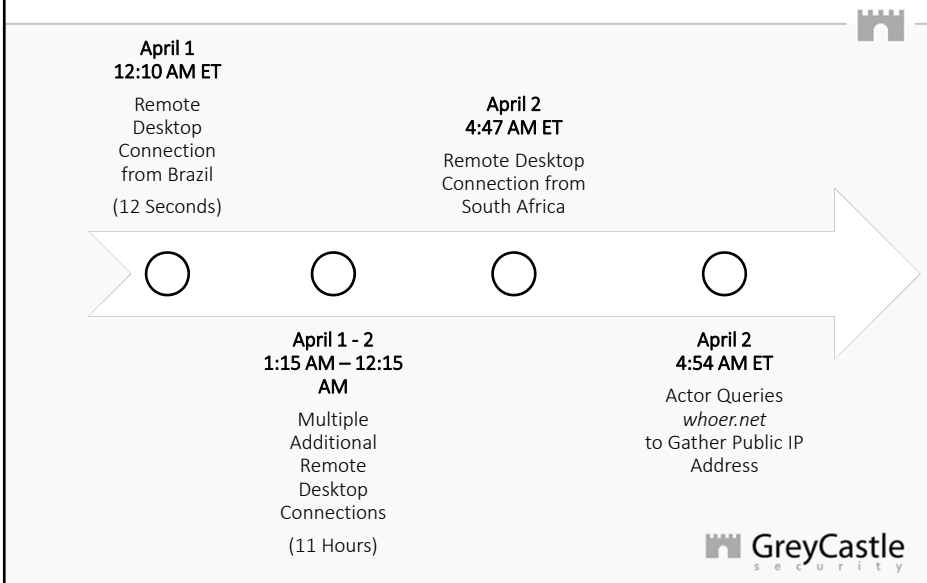
ABOUT ECMC

- 1000 beds
- Level-1 trauma center
- 30 outpatient services
- Member of Great Lakes Health consortium
- 300,000+ outpatient visits
- 12,000+ surgeries
- $600M revenue

GreyCastle security

	HOLLYWOOD PRESBYTERIAN	ERIE COUNTY MEDICAL
ATTACK SOPHISTICATION	LOW	HIGH
COMPROMISED ASSETS	700	6,000
DAYS OFFLINE	7	13
DAYS TO RECOVERY	10	45
RANSOM PAID	$17,000	$0

INSTANT REPLAY



INSTANT REPLAY

April 2
7:09 AM ET
Remote Desktop Connection from South Africa

April 2
7:10 AM ET
Actor Downloads and Installs Spam Email Engine

April 2
10:12 AM ET
Actor Attempts Malware (*chrome.exe.exe)* Installation and is Prevented by Antivirus

5 DAYS

April 7
6:59 AM ET
Remote Desktop Connection from South Africa

GreyCastle security

INSTANT REPLAY

April 7
7:02 AM ET
Actor Downloads Contact List for Spam

April 7
7:12 AM ET
Actor Visits *match.com* to Send Spam

April 7
8:29 AM – 10:58 AM
Multiple Additional Remote Desktop Connections
(2.25 Hours)

GreyCastle security

INSTANT REPLAY

April 8
2:51 AM ET
Remote Desktop Connection from Romania

April 8
3:29 AM ET
Multiple Shell Commands Executed to Install *SamSam* Malware

April 8
7:53 AM ET
Remote Desktop Connection from Netherlands

April 8
8:04 AM ET
Windows Login Service Compromised

GreyCastle security

INSTANT REPLAY

April 9
1:12 AM ET
Remote Desktop Connection from Netherlands

April 9
1:15 AM ET
Actor Collects Server List from Active Directory

April 9
1:24 – 1:30 AM ET
Actor Deletes All Online Backup Files

April 9
1:55 AM ET
Ransomware is Deployed and Executed

GreyCastle security

ATTRIBUTION

https://malwr.com/analysis/YmJlMDY5M2FjZTlhNDc5N2EzY2QxNGEwNmI0MzIxODc/

ATTRIBUTION

- SamSam ransomware variant
- 6,000+ compromised assets
- Default password was Patient0
- Attack did not start with a social engineering

SILVER LININGS

- Immediate incident detection and response
- Emergency Management Plan fluency due to recent drill
- Offline backup availability
- Negligible impact to patient care and safety
- Community and peer support
- Legal non-breach determination

GreyCastle security

43

INCIDENT RESPONSE FOR HEALTHCARE

CRASH COURSE

INCIDENT RESPONSE FOR HEALTHCARE

1. GO TO DEFCON 1 ASAP

- Formally activate your Incident Response Plan
- Let your PHI inventory drive response
- Decide on your communications strategy
- Assume that response activities will be scrutinized after the incident

GreyCastle security

INCIDENT RESPONSE FOR HEALTHCARE

2. ASSEMBLE THE RIGHT TEAM

- Get leadership involved immediately
- Get communications, legal and clinical leaders in the room – IT is secondary
- Escalate to cybersecurity and investigation experts

GreyCastle security

INCIDENT RESPONSE FOR HEALTHCARE

3. INITIATE "LOCKDOWN"

- Change passwords on critical assets
- Power down or disconnect non-critical assets
- Disable outbound network traffic
- Disable off-hours access
- Disable Internet access
- Freeze bank accounts

GreyCastle security

INCIDENT RESPONSE FOR HEALTHCARE

4. UNDERSTAND IOCs

- Know what Indicators of Compromise (IOCs) are and where to look for them
- Focus on IOCs when ePHI assets show signs of compromise

GreyCastle security

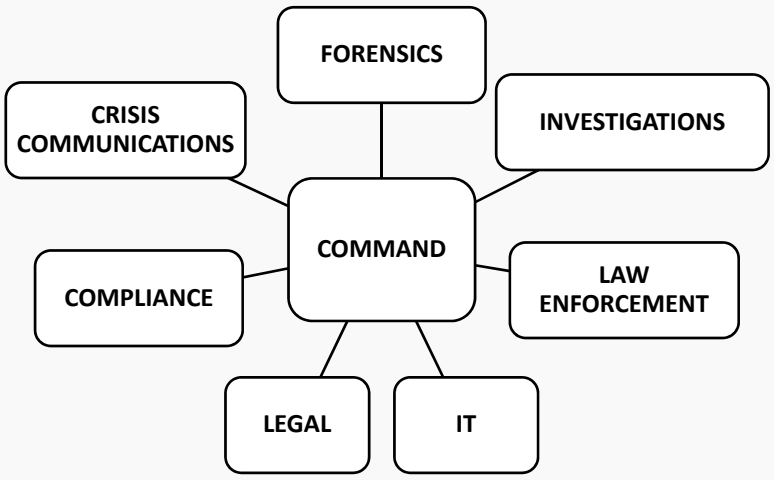
INCIDENT RESPONSE FOR HEALTHCARE

5. MINIMIZE EXPOSURE

- Engage a HIPAA-fluent attorney
- Collect and document all evidence that proves – or even merely suggests – integrity of ePHI

GreyCastle security

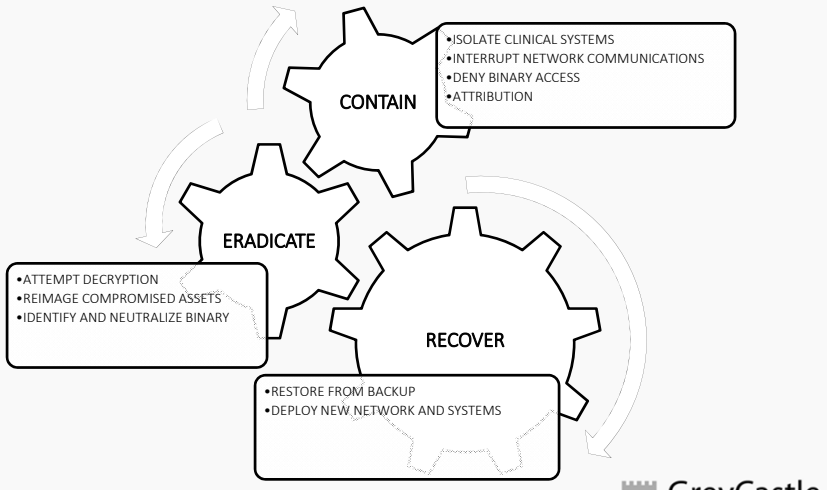
RESPONSE TEAM



GreyCastle security

50

RESPONSE PROCESS

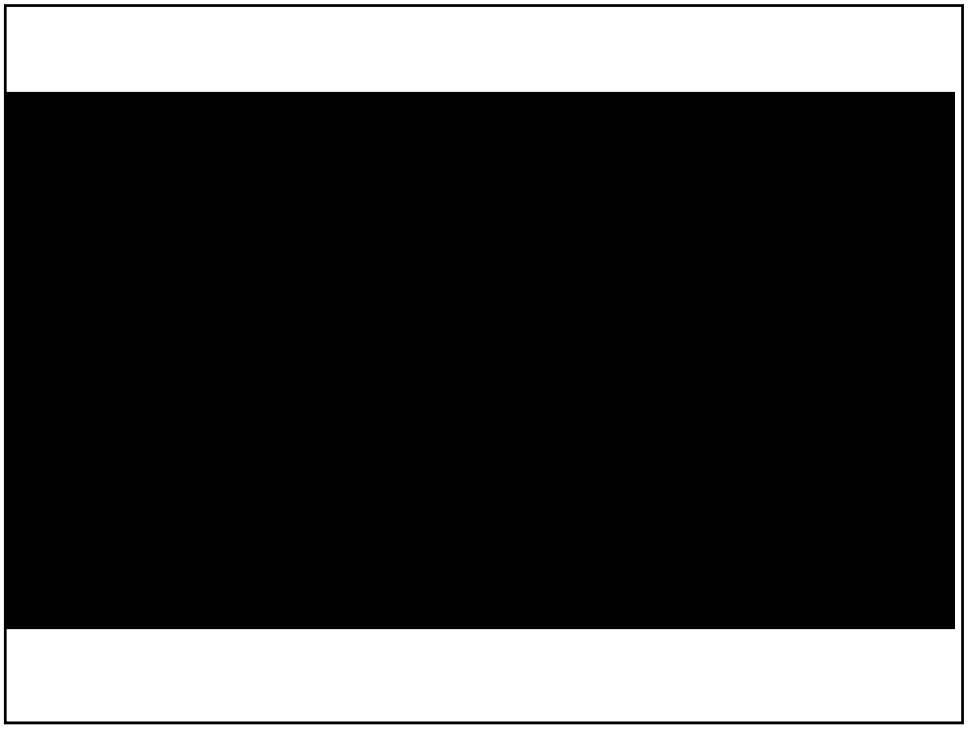


GreyCastle security

51

INCIDENT RESPONSE FOR HEALTHCARE

FINAL THOUGHTS



CREATE A

CULTURE OF SECURITY

CONSIDER
PAYING THE RANSOM?

KNOW THE DIFFERENCE BETWEEN
EXPOSURE AND BREACH

FOCUS RECOVERY EFFORTS ON

PATIENT CARE AND SAFETY

FOR THE LOVE OF ALL THINGS GOOD DO

"THE BIG THREE"


ANY
QUESTIONS
?

THANK YOU

GreyCastle security