

RISK
RANSOMWARE
RESILIENCE



THE NEXT GENERATION OF PATIENT SAFETY



RISK
RANSOMWARE
RESILIENCE



THE NEXT GENERATION OF PATIENT SAFETY



REIHANEH
CHIEF EXECUTIVE OFFICER
GREYCASTLE SECURITY




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




RISKUNIVERSE





CLINICS


PHARMACY


NURSING HOME


EHR


BIOMEDICAL
DEVICES

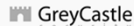

ER



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.

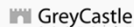


BIOMEDICAL DEVICES

- Patient monitoring devices, such as:
 - Smart medical devices, infusion pumps, ventilators, incubators, telemetry, medical imaging
- Electrocardiogram (ECG), pulse oximetry, ventilators, capnography monitors
- Pulmonology machines
- Smart beds, fall detection
- Remote I.U. telemetry, tele-ology
- Remote wellness and chronic disease management
 - Room clocks, defibrillators and neuro-stimulators
 - Wearable wristbands, bib patches, smart watches, digital vital monitors, spirometers, pulse oximeter



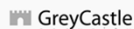
Point: No longer an "IT issue"! Compromise of biomedical equipment directly affects patient safety.



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.



AND THE RISKS ARE..

Confidentiality Integrity

eHI, Sensitive Information, Proprietary

Availability

Point: Think "CIA"

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.

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



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?

RISK ASSESSMENT: BIOMEDICAL EQUIPMENT

Issues	Resultant Risks
1. Inaccurate Inventory	1. Scope and Universe of assets not known
2. Inproper 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

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

**RISK MANAGEMENT
FOR HEALTHCARE
FINAL THOUGHTS**

RISK MANAGEMENT
AFFECTS PATIENT SAFETY



IF YOU ARE NOT MEASURING
YOU ARE NOT DOING



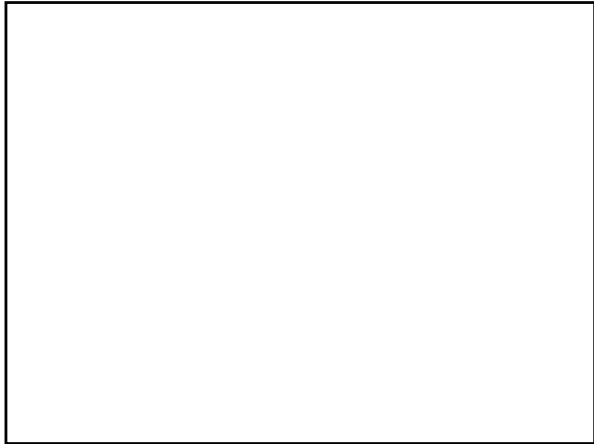
RISK ASSESSMENTS
ARE REQUIRED REGULARLY

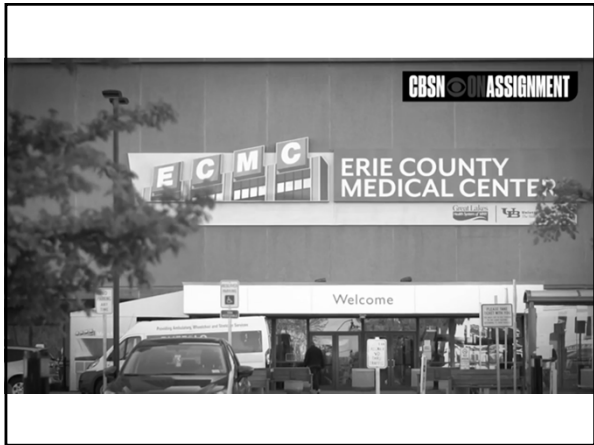















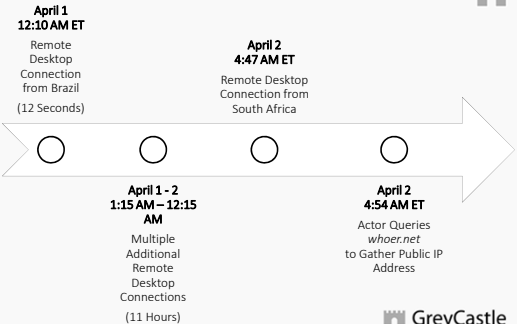
ABOUT ECMC

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



	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




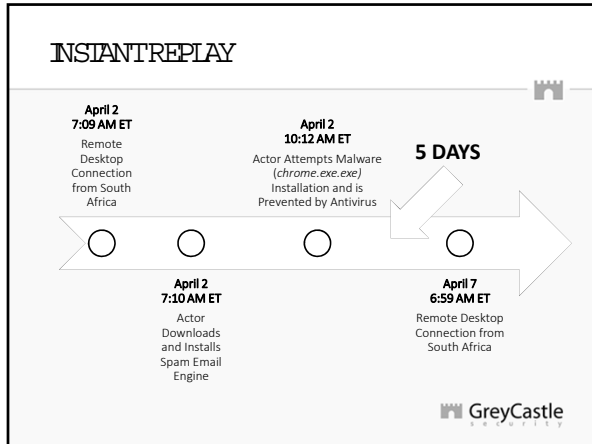
April 1 12:10 AM ET
Remote Desktop Connection from Brazil (12 Seconds)

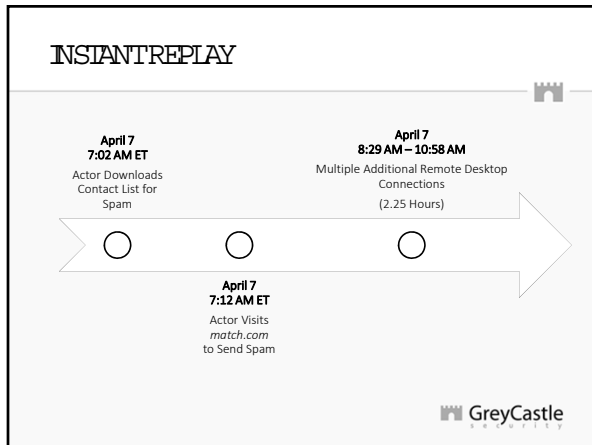
April 2 4:47 AM ET
Remote Desktop Connection from South Africa

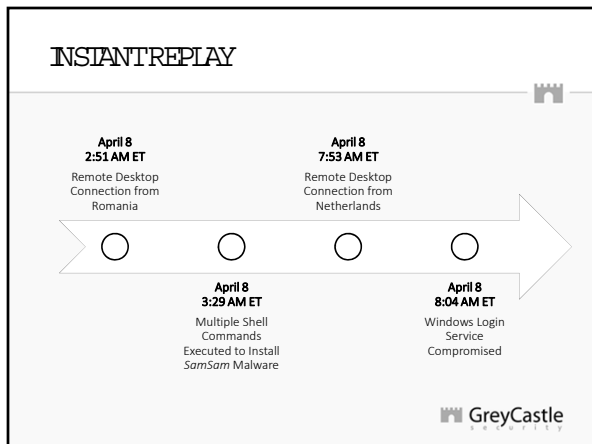
April 1 - 2 1:15 AM - 12:15 AM
Multiple Additional Remote Desktop Connections (11 Hours)

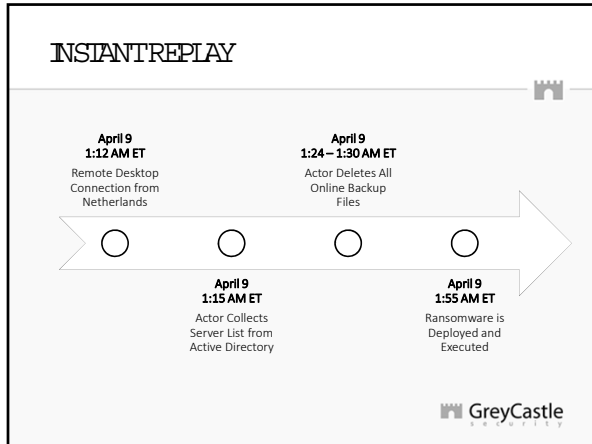
April 2 4:54 AM ET
Actor Queries *whoer.net* to Gather Public IP Address











ATTRIBUTION

<https://malwr.com/analysis/muJMDY5M2FZl1NDc5N2ZkZ0xNGRmNmIMzZkOz/>

GreyCastle
41

- ### ATTRIBUTION
- SamSam ransomware variant
 - 6,000+ companies affected
 - Default password was Patient0
 - Attack did not start with social engineering
- GreyCastle

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 peers support
- Legal non-breach determination


 Grey Castle
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 RIT inventory drive response
- Decide on your communications strategy
- Assume that response activities will be optimized after the incident

 Grey Castle

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
- Enable to cyber security and investigation experts

GreyCastle

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

INCIDENT RESPONSE FOR HEALTHCARE

4. UNDERSTAND IOCs

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

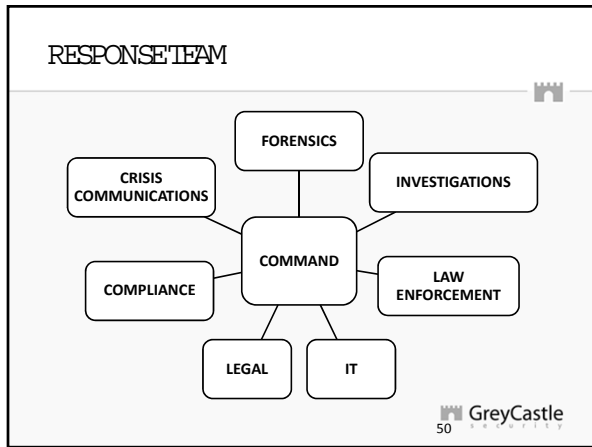
GreyCastle

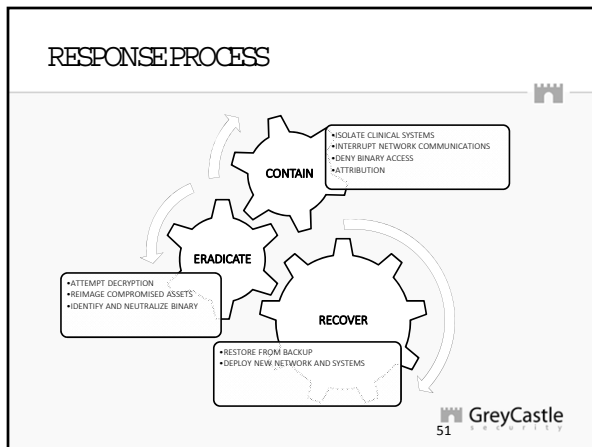
INCIDENT RESPONSE FOR HEALTHCARE

5 MINUTE EXPOSURE

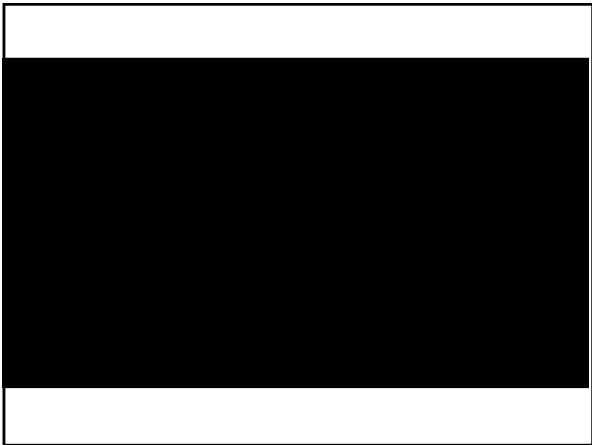
- Engage a HIPAA-fluent attorney
- Collect and document all evidence that proves
- or even merely suggests- integrity of EHI

GreyCastle






INCIDENT RESPONSE
FOR HEALTHCARE
FINAL THOUGHTS




CREATE A
CULTURE OF SECURITY

A stylized ECG line graphic, consisting of a horizontal line with a central pulse, positioned below the text.

CONSIDER
PAYING THE RANSOM ?



KNOW THE DIFFERENCE BETWEEN
EXPOSURE AND BREACH



FOCUS RECOVERY EFFORTS ON
PATIENT CARE AND SAFETY



