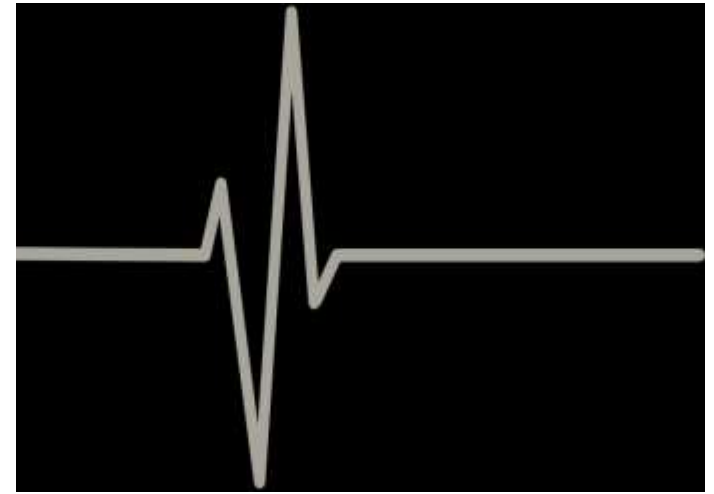


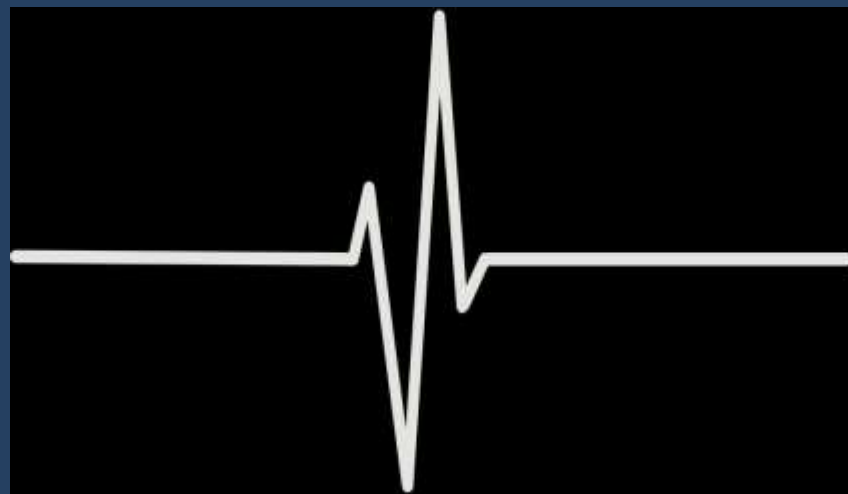
C O D E
BLUE
C L E A R



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

@REGHARNISH

C O D E
BLUE
C L E A R



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

@REGHARNISH

CBSN  ON ASSIGNMENT

E C M C

ERIE COUNTY
MEDICAL CENTER

Great Lakes
Health System of WHP

UB
The University of Buffalo

Welcome

NO
PARKING
ANY TIME

RESERVED
PARKING


THE
ACCESSIBLE

Providing Ambulatory, Wheelchair and Stretcher Services

PLEASE TAKE
TICKET WITH YOU
You will not be allowed
to enter the building
without a valid ticket.

NO
PARKING
ANY TIME



ERIE COUNTY
MEDICAL CENTER

3

↑ EMERGENCY

→ Main Entrance

→ Parking

→ David Miller Bldg.

ECMC



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

| 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

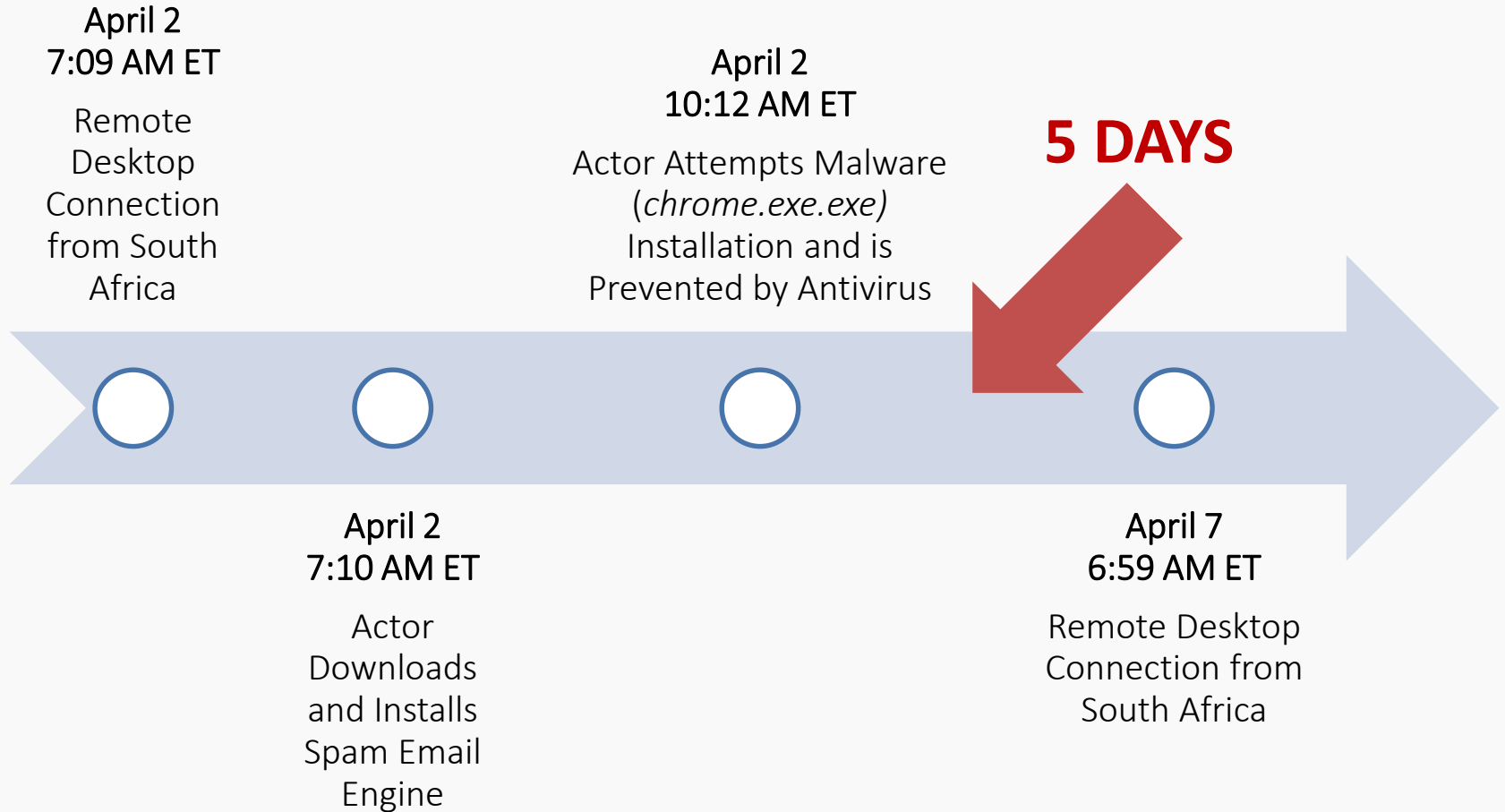
April 1 - 2
1:15 AM – 12:15
AM

Multiple
Additional
Remote
Desktop
Connections
(11 Hours)

April 2
4:54 AM ET

Actor Queries
whoer.net
to Gather Public IP
Address

INSTANT REPLAY



INSTANT REPLAY



April 7
7:02 AM ET

Actor Downloads
Contact List for
Spam

April 7
8:29 AM – 10:58 AM

Multiple Additional Remote Desktop
Connections
(2.25 Hours)

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

INSTANT REPLAY



April 8
2:51 AM ET

Remote Desktop
Connection from
Romania

April 8
7:53 AM ET

Remote Desktop
Connection from
Netherlands



April 8
3:29 AM ET

Multiple Shell
Commands
Executed to Install
SamSam Malware

April 8
8:04 AM ET

Windows Login
Service
Compromised

INSTANT REPLAY



April 9
1:12 AM ET

Remote Desktop
Connection from
Netherlands

April 9
1:24 – 1:30 AM ET

Actor Deletes All
Online Backup
Files

April 9
1:15 AM ET

Actor Collects
Server List from
Active Directory

April 9
1:55 AM ET

Ransomware is
Deployed and
Executed

ATTRIBUTION



<https://malwr.com/analysis/YmJlMDY5M2FjZTIhNDc5N2IzY2QxNGFmNmI0MzlxODc/>

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

INCIDENT RESPONSE FOR HEALTHCARE

CRASH COURSE

INCIDENT RESPONSE FOR HEALTHCARE



1. GO TO DEFCON 1 ASAP

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

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

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

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

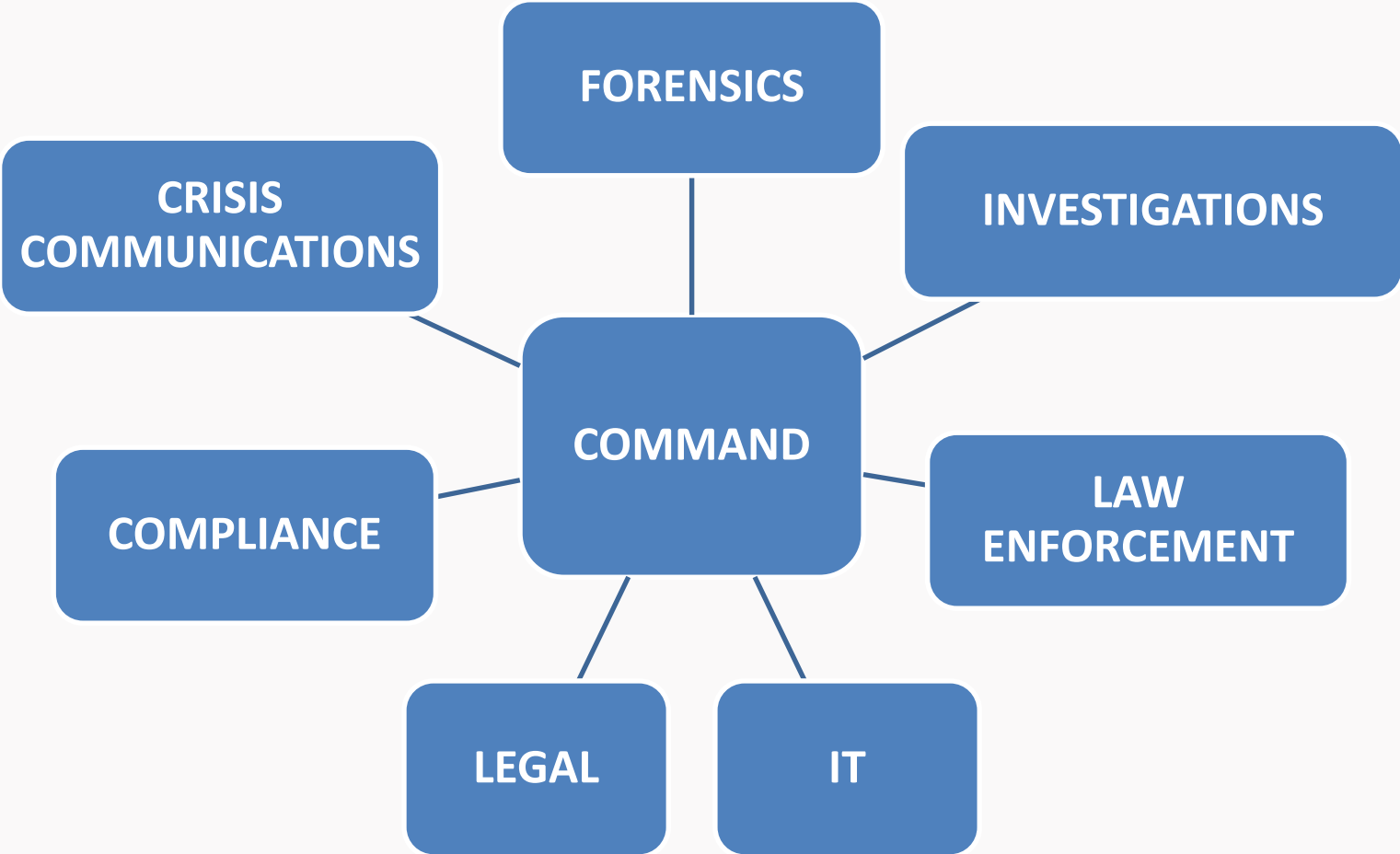
INCIDENT RESPONSE FOR HEALTHCARE



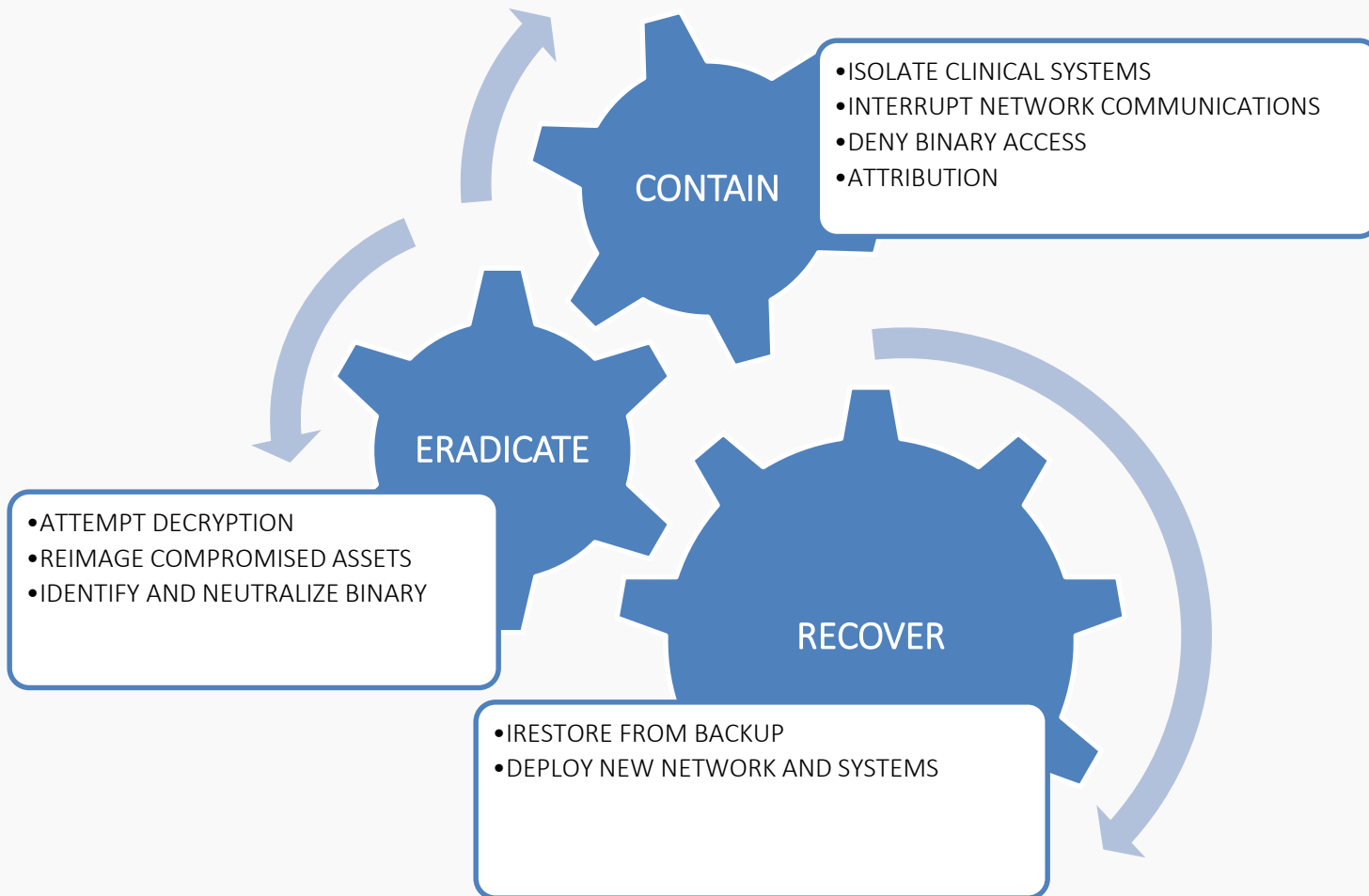
5. MINIMIZE EXPOSURE

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

RESPONSE TEAM



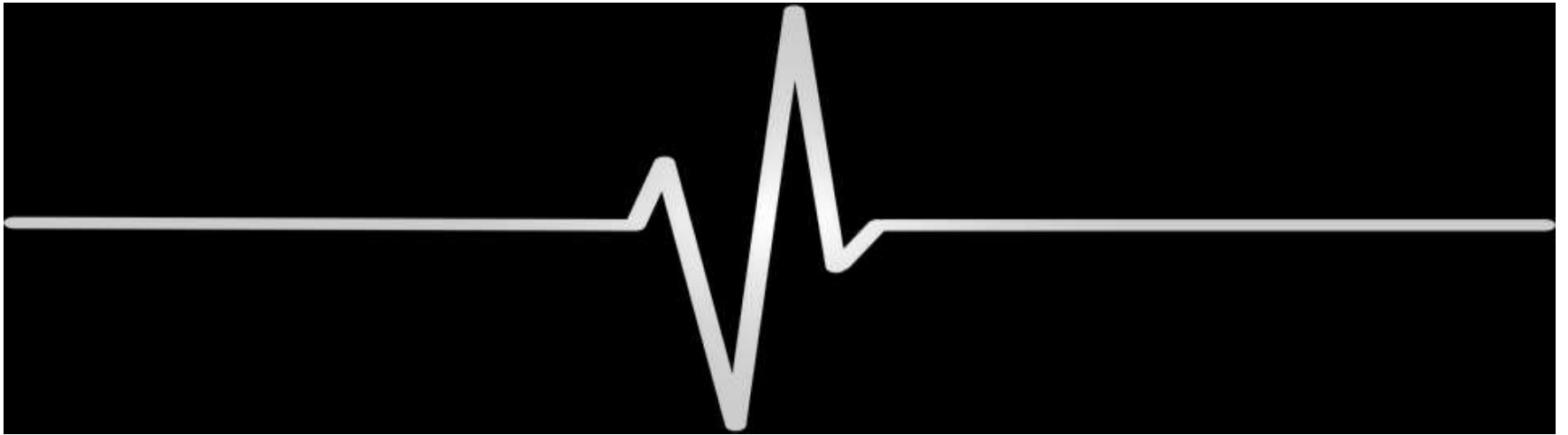
RESPONSE PROCESS



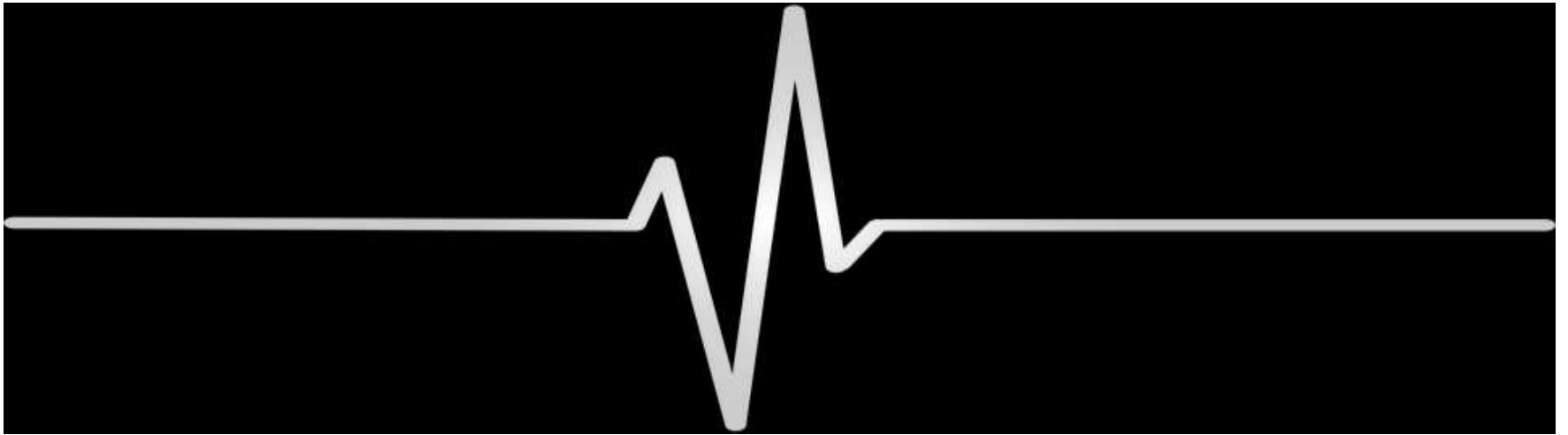
INCIDENT RESPONSE FOR HEALTHCARE

FINAL THOUGHTS

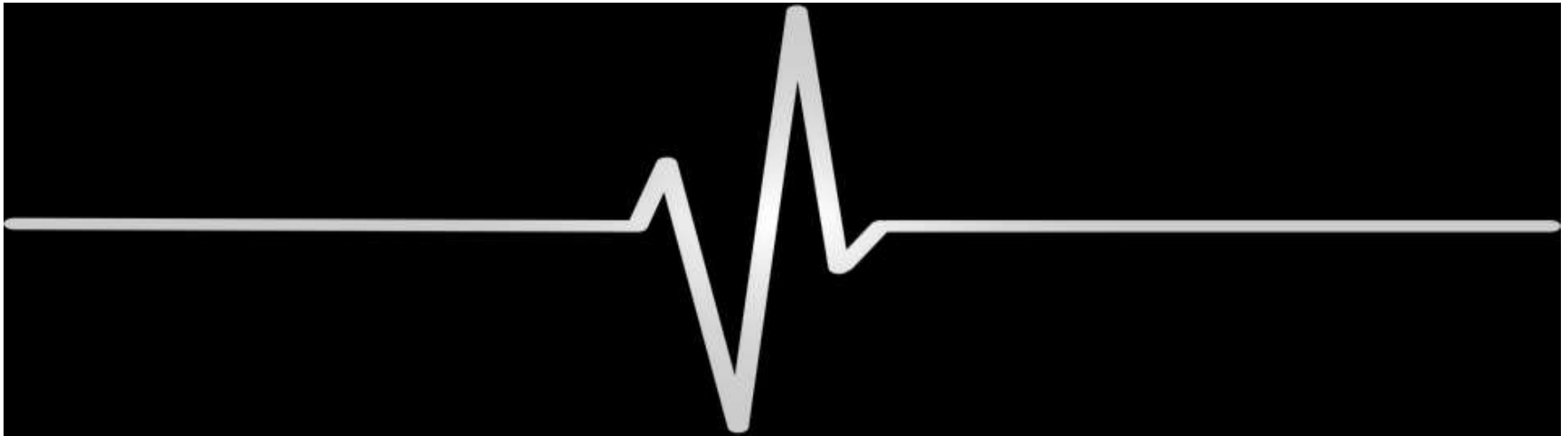
CREATE A
CULTURE OF SECURITY



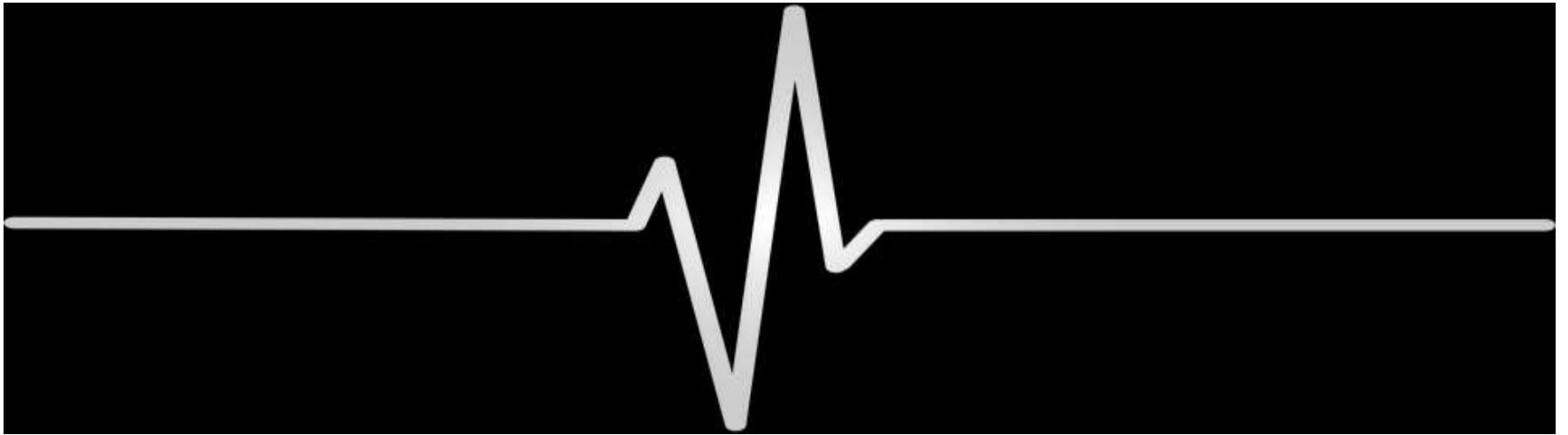
CONSIDER
PAYING THE RANSOM?



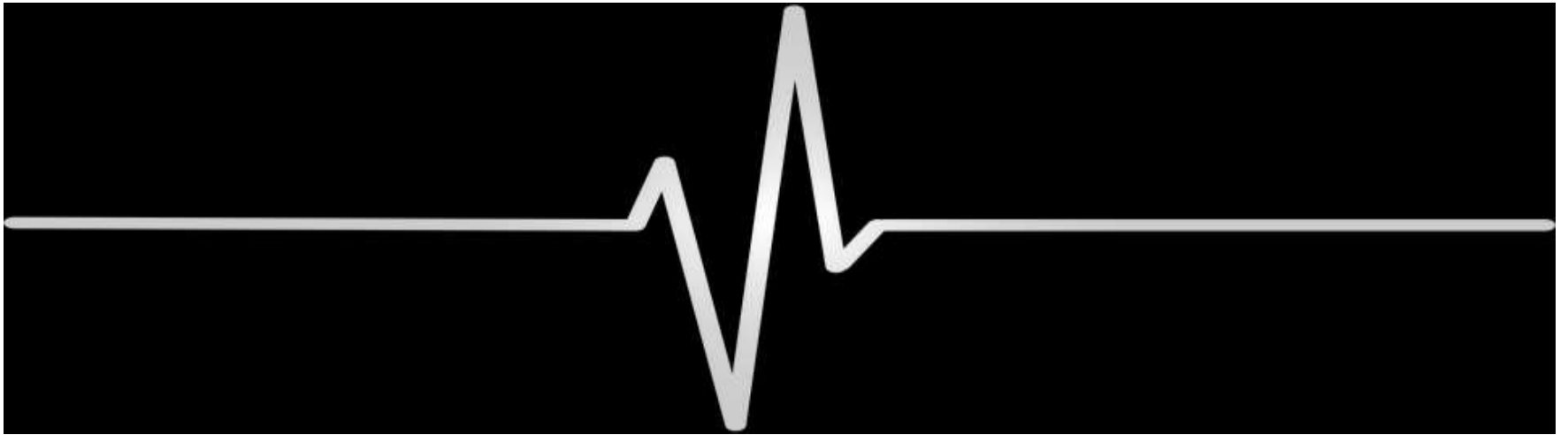
KNOW THE DIFFERENCE BETWEEN
EXPOSURE AND BREACH



FOCUS RECOVERY EFFORTS ON
PATIENT CARE AND SAFETY



FOR THE LOVE OF ALL THINGS GOOD DO
“THE BIG THREE”





ANY
QUESTIONS
?

@REGHARNISH

