HACKING HOSPITALS

Eli Mezei| Executive Partner

emezei@securityevaluators.com

independent security evaluators

ISE

independent security evaluators

About ISE


independent security evaluators


independent security evaluators

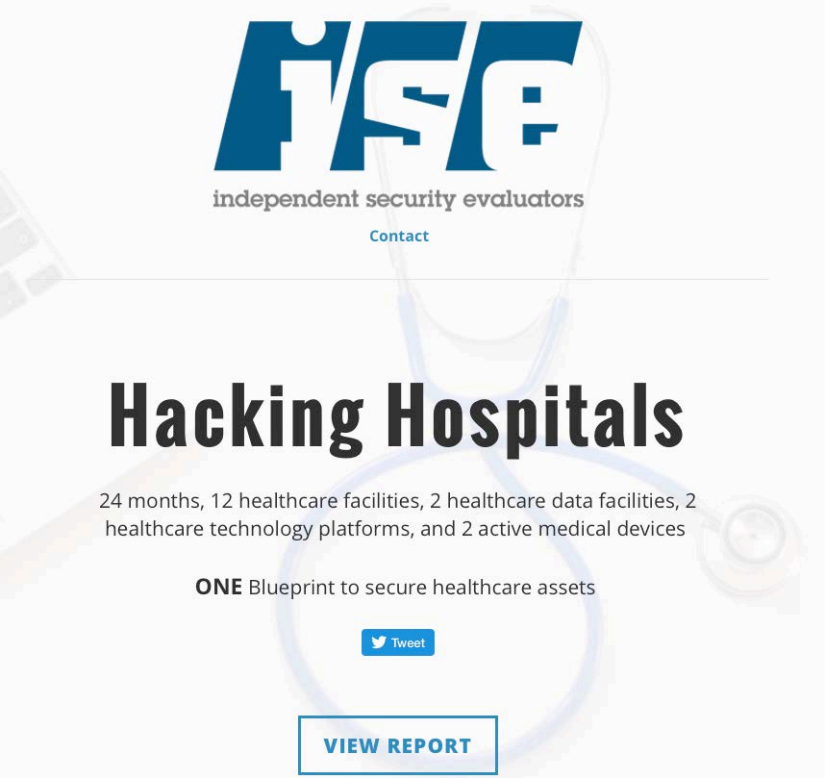

android


Ford


DIEBOLD

RESEARCH OVERVIEW

independent security evaluators



24 Months

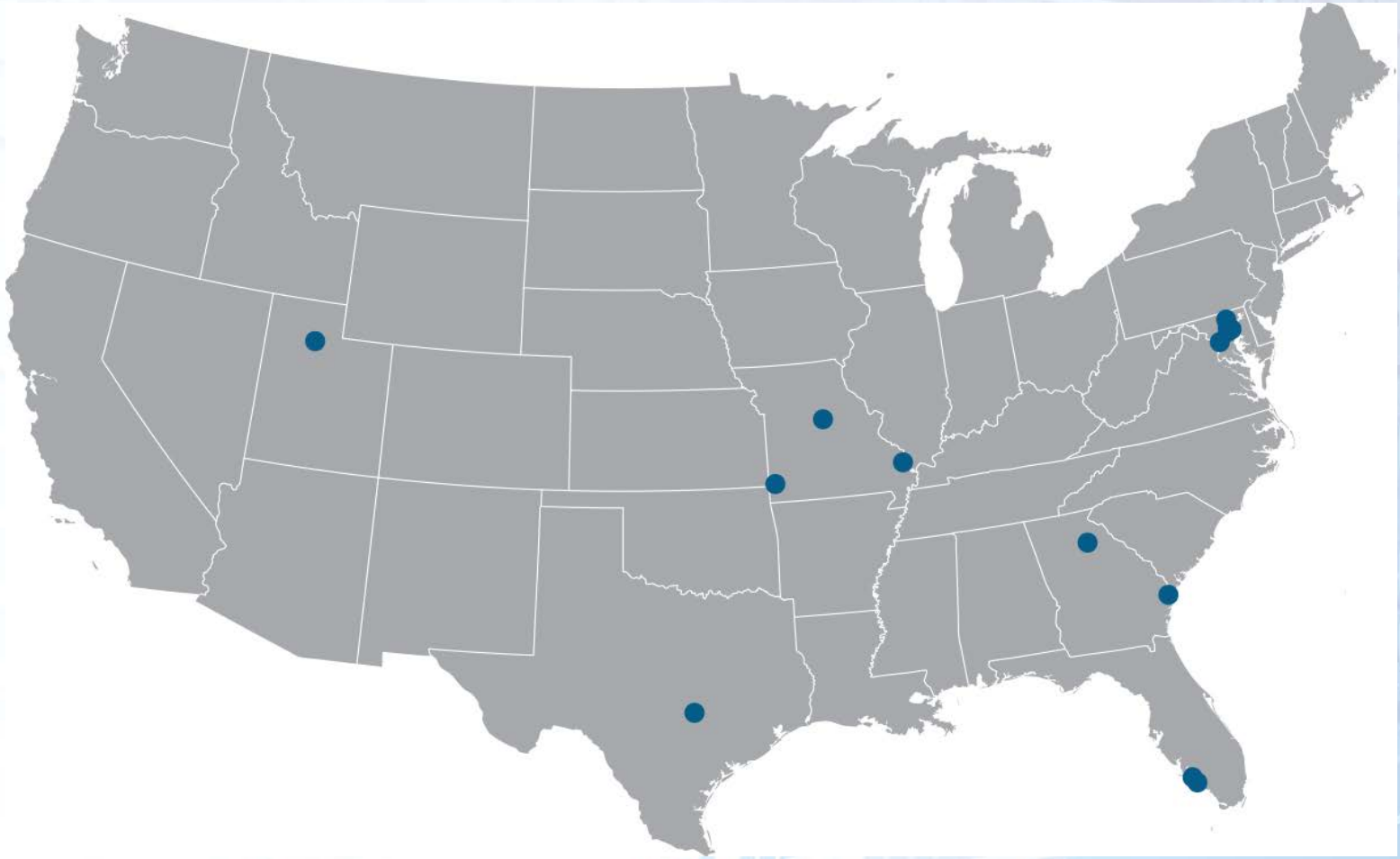
12 Hospitals

2 Healthcare data facilities

2 Medical devices

Cyber attacks = kill patients

independent security evaluators



Baltimore, MD
Towson, MD
Washington, D.C.
Athens, GA
Savannah, GA
Cape Girardeau, MO
Columbia, MO
Joplin, MO
Salt Lake City, UT
Naples, FL
Bonita Springs, FL
Austin, TX

independent security evaluators

Forbes / Security

The Little Black Book of Billiona

FEB 23, 2016 @ 12:55 PM 9,130 VIEWS

White Hat Hackers Hit 12 American Hospitals To Prove Patient Life 'Extremely Vulnerable'

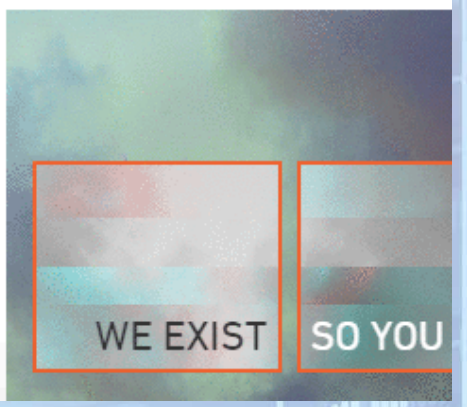
Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms.

FOLLOW ON FORBES (173)

FULL BIO

A two-year research project into the security of 12 hospitals and a variety of medical technologies has concluded that patient health is “extremely vulnerable” to digital



independent security evaluators

FINDINGS

independent security evaluators

patient data v. patient health

independent security evaluators

Status Quo

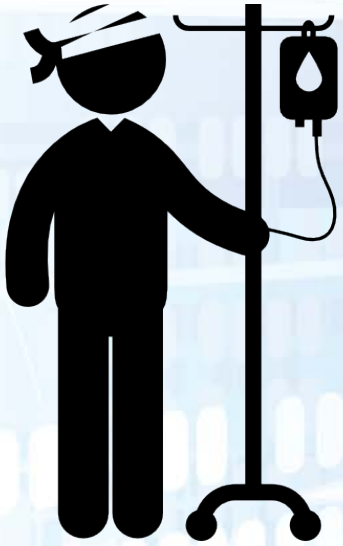
Wrong mission x Outdated approach = Failure

independent security evaluators

WRONG MISSION

independent security evaluators

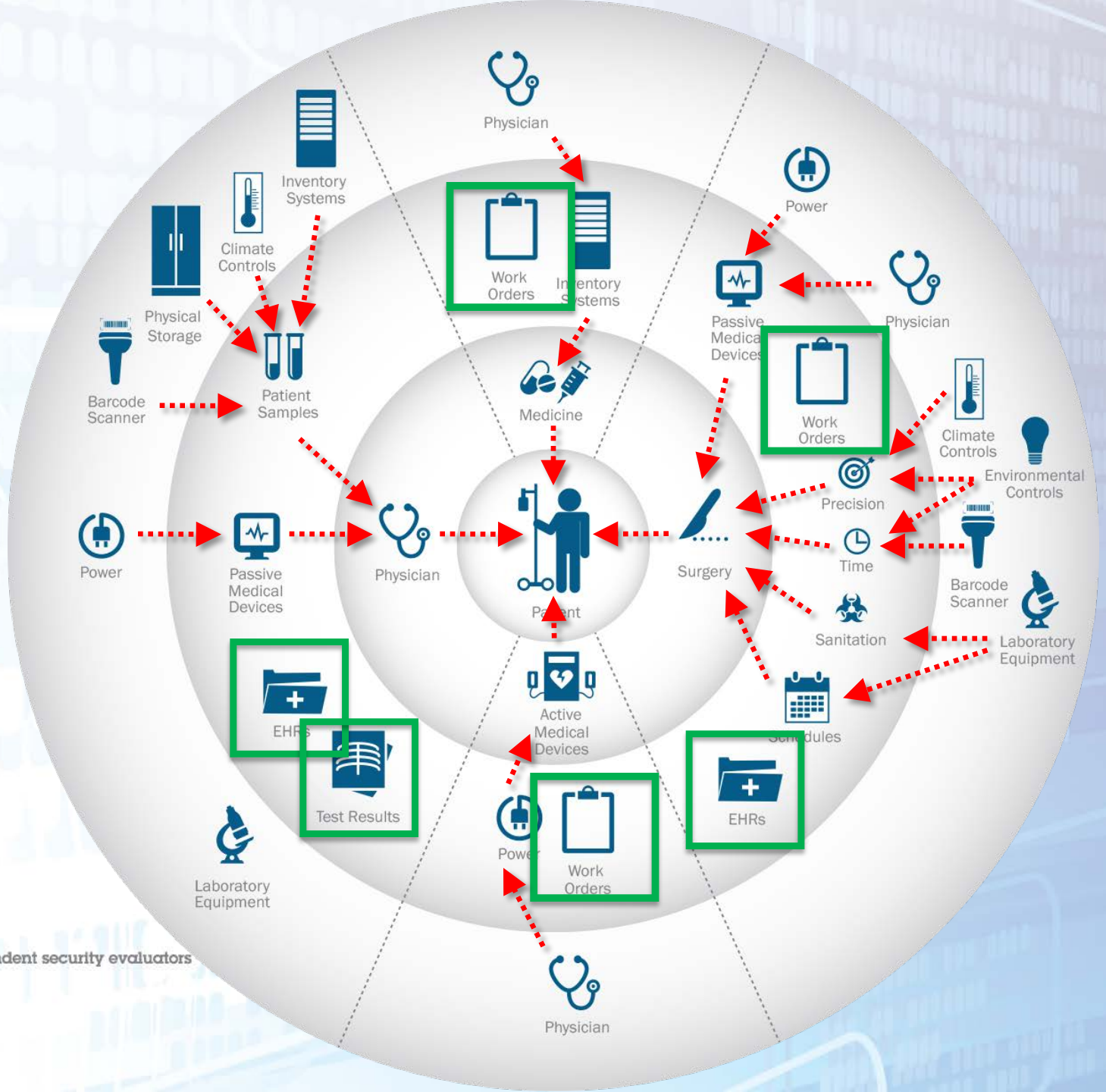
Patient Health v. Patient Data



HARM

PROFIT

independent security evaluators



independent security evaluators

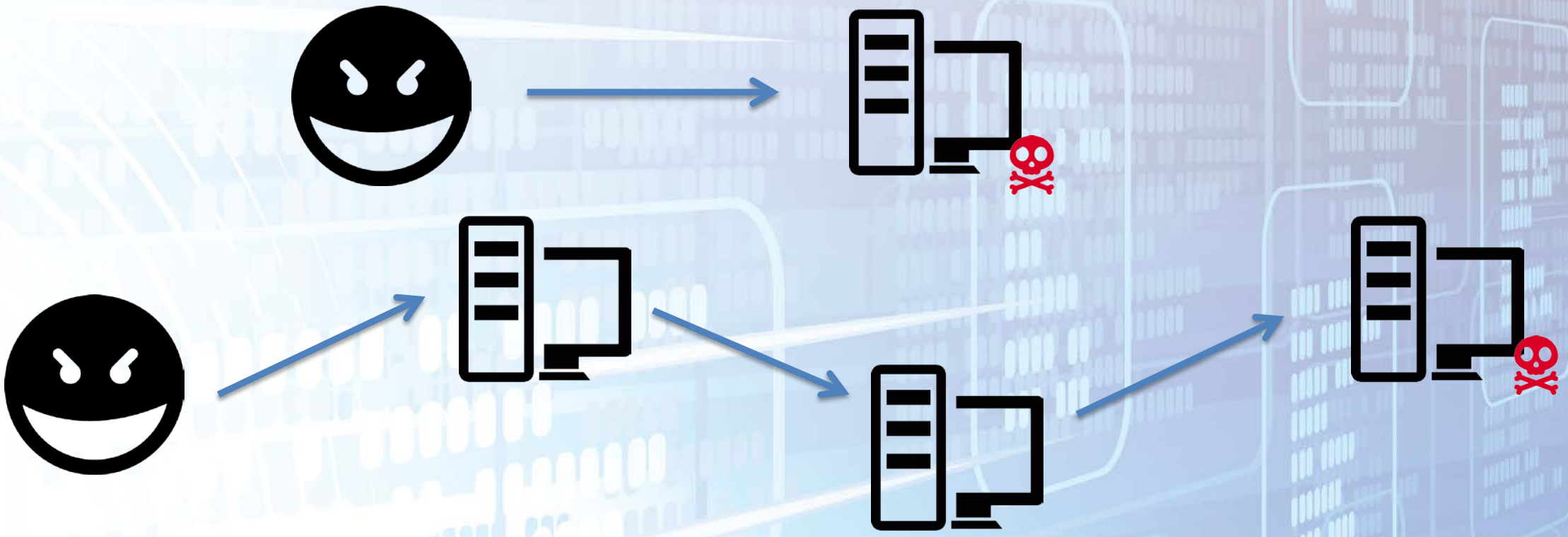
OUTDATED APPROACH

independent security evaluators

Untargeted v. Targeted Attacks

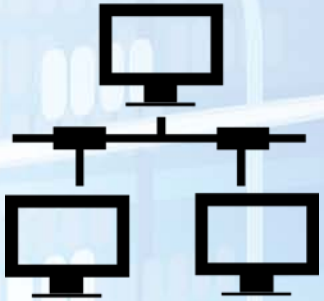
independent security evaluators

Unsophisticated v. Sophisticated Attacks



independent security evaluators

Unsophisticated v. Sophisticated Adversaries



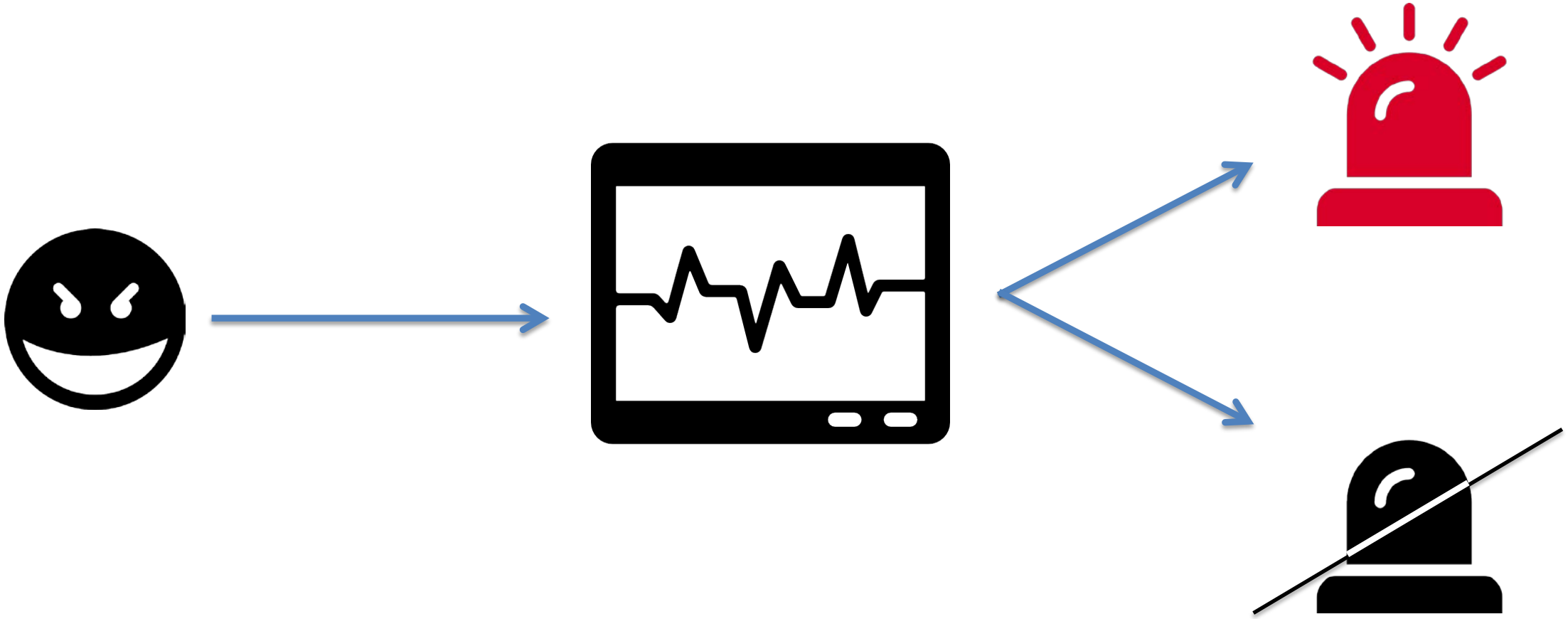
independent security evaluators

	Health		Data	
Adversaries	**Targeted**	**Untargeted**	**Targeted**	**Untargeted**
Small Group	X	X	X	✓
Hacktivists	X	X	X	X
Organized Crime	X	X	X	X
Terrorists	X	X	X	X
Nation States	X	X	X	X

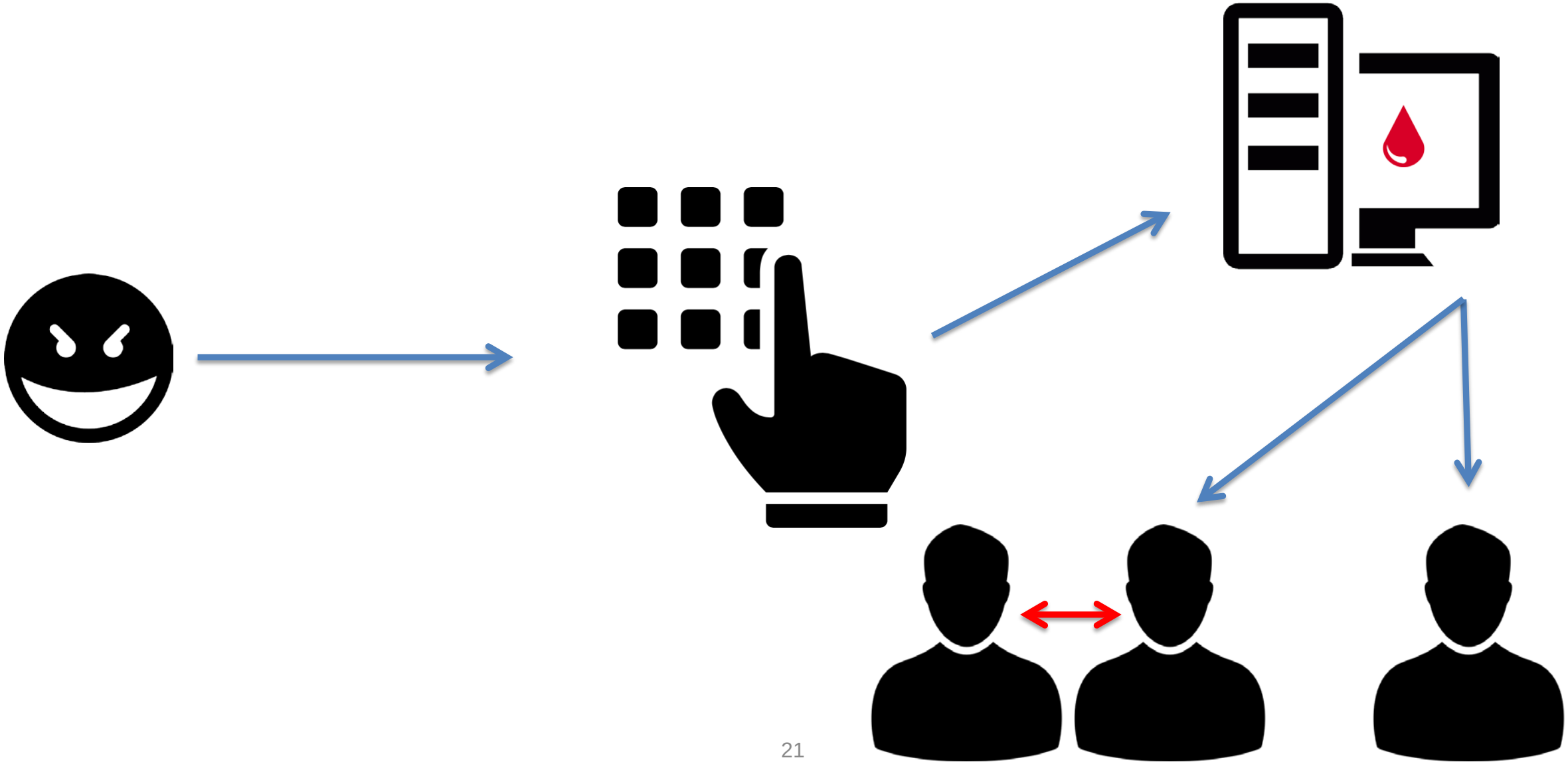
ATTACK ANATOMIES

independent security evaluators

Patient Monitor



Lobby Kiosk / Bloodwork



COMMON ISSUES

independent security evaluators

Design Issues


funding


staffing

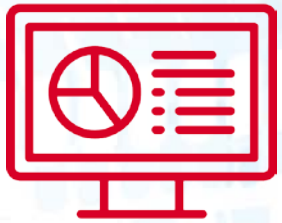

training

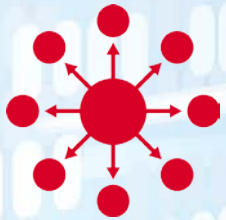

hierarchy


policy


Network awareness


audit


logging/ monitoring


architecture


access control


legacy systems


remote access

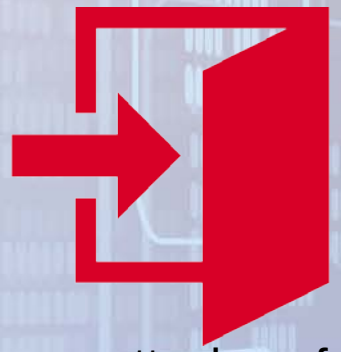
ISE independent security evaluators

Design Issues

hospital-built,
non-assessed software

vendor-built,
non-assessed software

critical uptime
prevents security



primary attack surfaces
on non-restricted subnets

local physical access
to critical networks

local physical access
to systems & devices

credentials entered
in presence of patients

ISE
independent security evaluators

Implementation Issues

use of
insecure services

broken
access controls

default
configurations

shared
credentials

unpatched
systems

independent security evaluators

BLUEPRINT

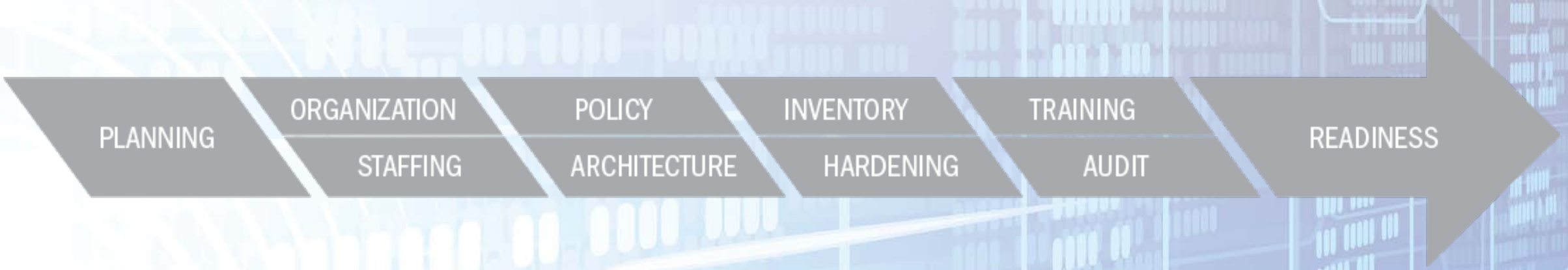
independent security evaluators

~~"Are we secure?"~~

~~"How secure are we?"~~

"How do we get there?"

independent security evaluators



independent security evaluators

Planning

- Understand the blueprint
- Create a threat model
- Understand the risks
- (Re)design security framework
- Perform gap analysis
- Create long term plan

Organization

- Separate IS from IT
- Biomed under IT and/or IS

Staffing

- Understand roles
- Full time vs. part time
- Determine quantity

Policy

- Formally define security
- Needed policies
- Needed procedures
- Audit preparation
- Review

Architecture

- Information workflows
- Segmentation
- Network appliances
- Security appliances
- Administration
- Remote access
- Physical access

Inventory

- Employees
- Vendors
- Systems
- Software
- Devices

Hardening

- Configuration management
- Endpoint security
- Monitoring

Training

- Security fundamentals
- Policy training
- Business training
- Subject matter training

Audit

- Internal assessment
- Outside assessment
- Internal audit

Readiness

- Incident response
- Disaster recovery
- Red teaming
- Contingency plans

independent security evaluators

Recap

Wrong mission x Outdated approach = Failure

Correct mission x Modern approach = Success

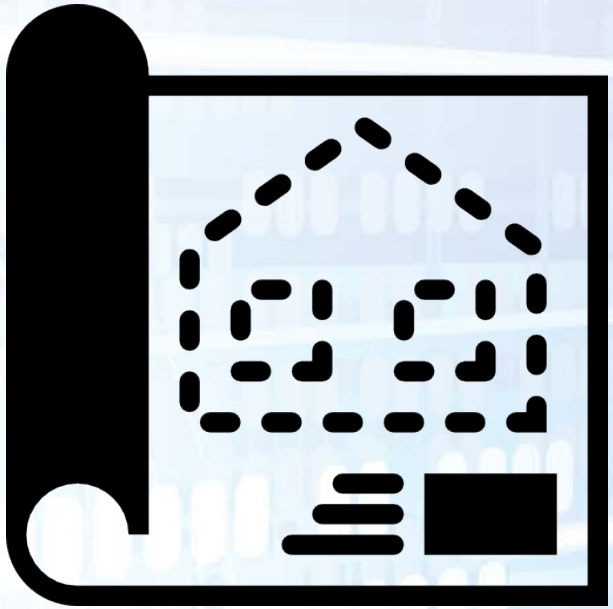
independent security evaluators

Recommendations

- Follow the **Blueprint**
- Distinguish between **patient health v. patient data**
- Adopt an **adversarial** mindset

independent security evaluators

How Can ISE Help?



BLUEPRINT

vCISO

independent security evaluators

independent security evaluators

emezei@securityevaluators.com
https://www.securityevaluators.com/hospitalhack