RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: STR-R03

Separating Fact From Fiction: The Real Risks Within Medical Device Security

Chris Sherman

Analyst, Security & Risk

Forrester

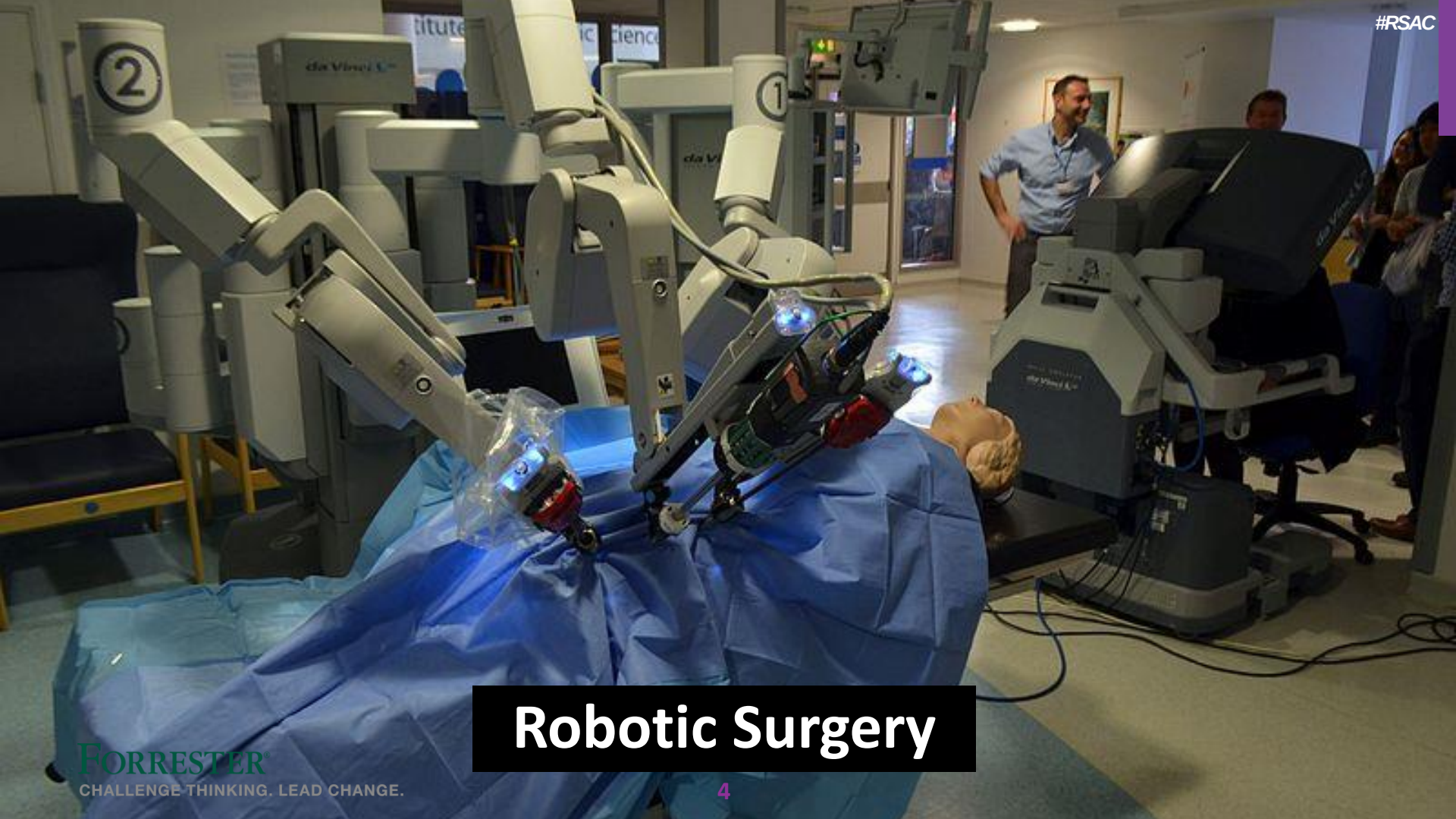
@ChrisShermanFR

#RSAC

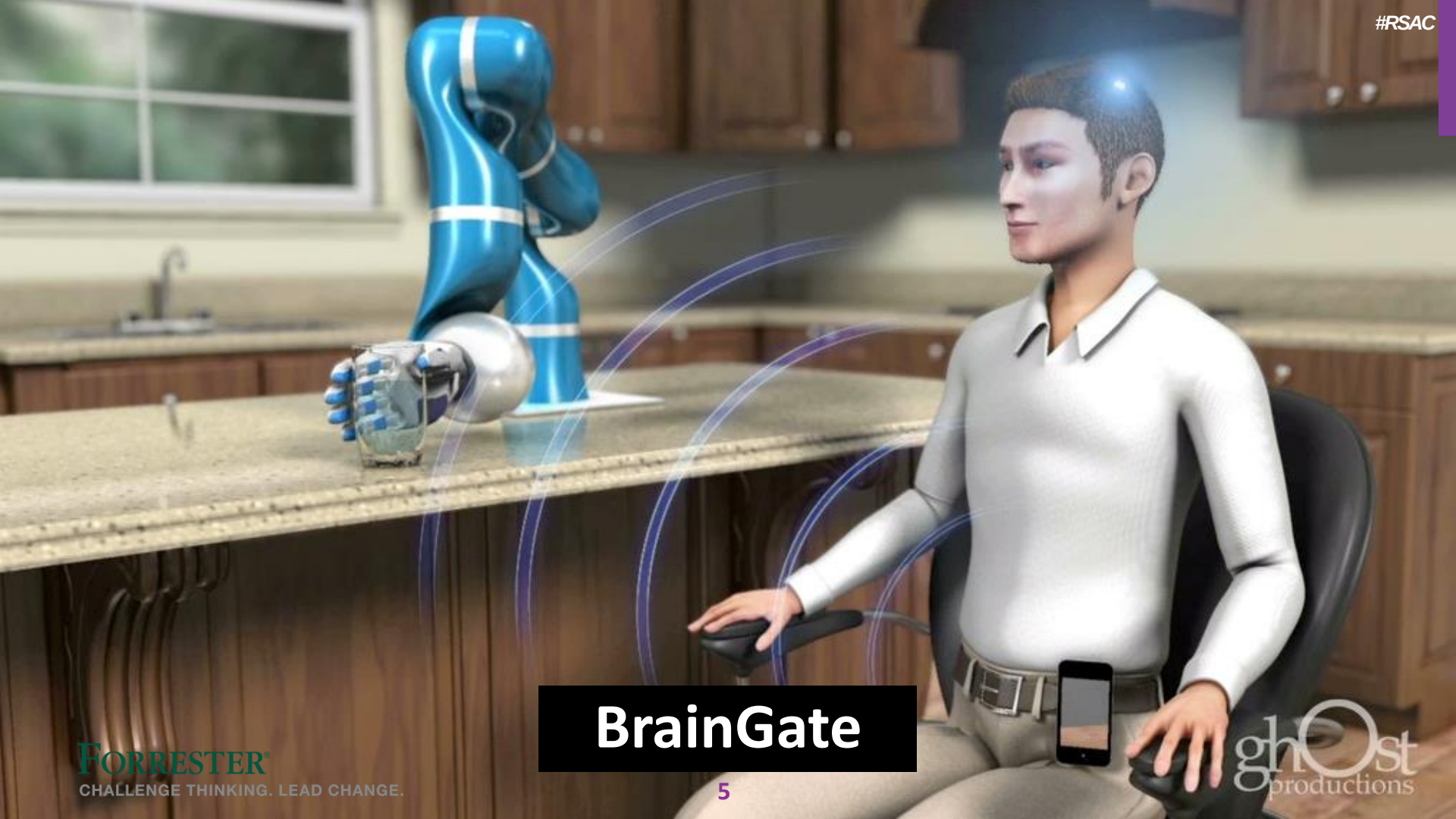
Agenda

- Balancing Innovation With Security In Healthcare
- The Medical Device Threat Landscape
- Attack Scenarios
- The Path Forward

Balancing Innovation With Security In Healthcare



Robotic Surgery

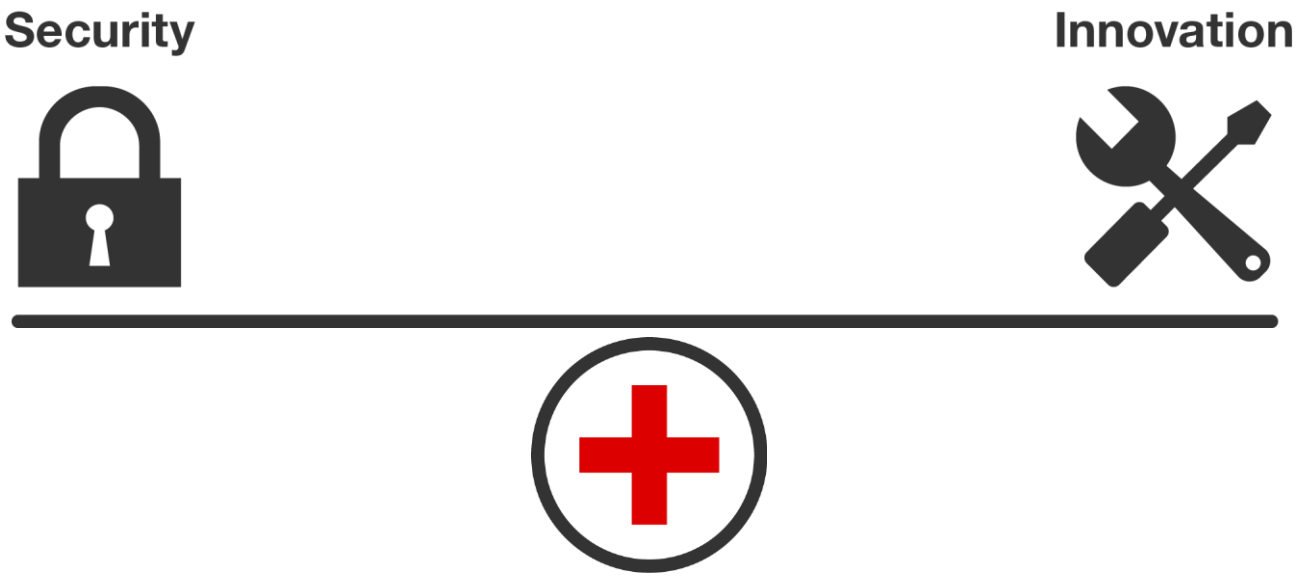

BrainGate

Telemedicine

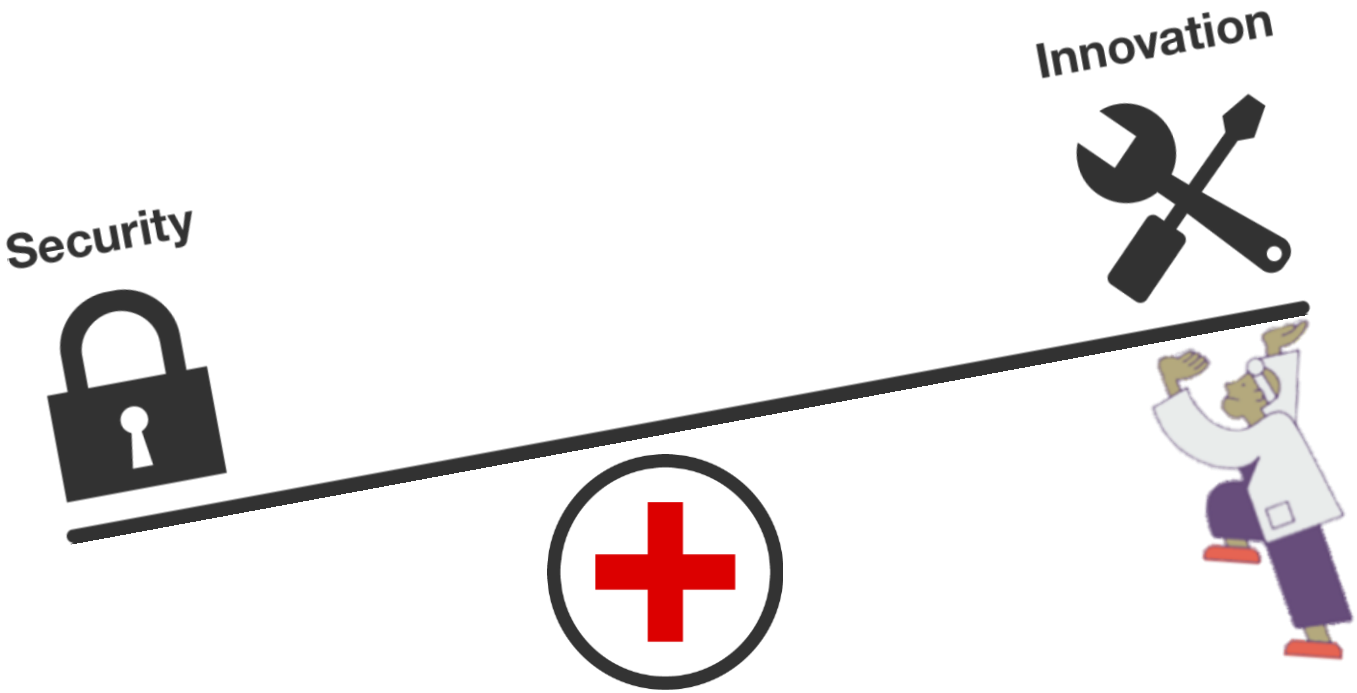
mHealth

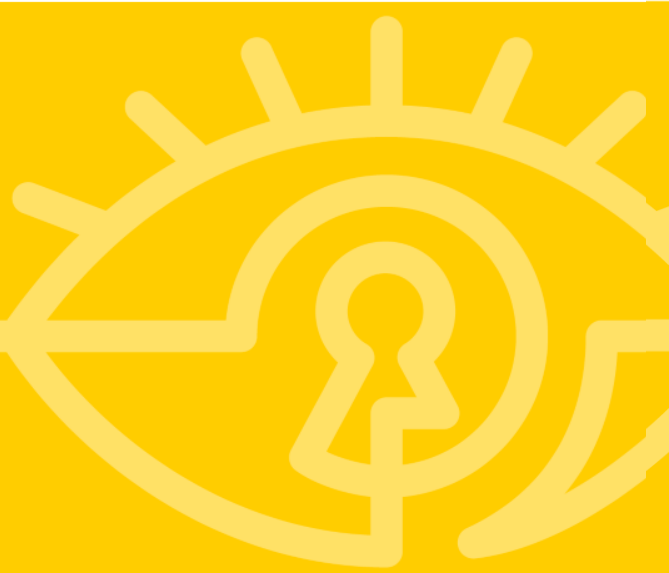
FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

With Innovation Comes Risk



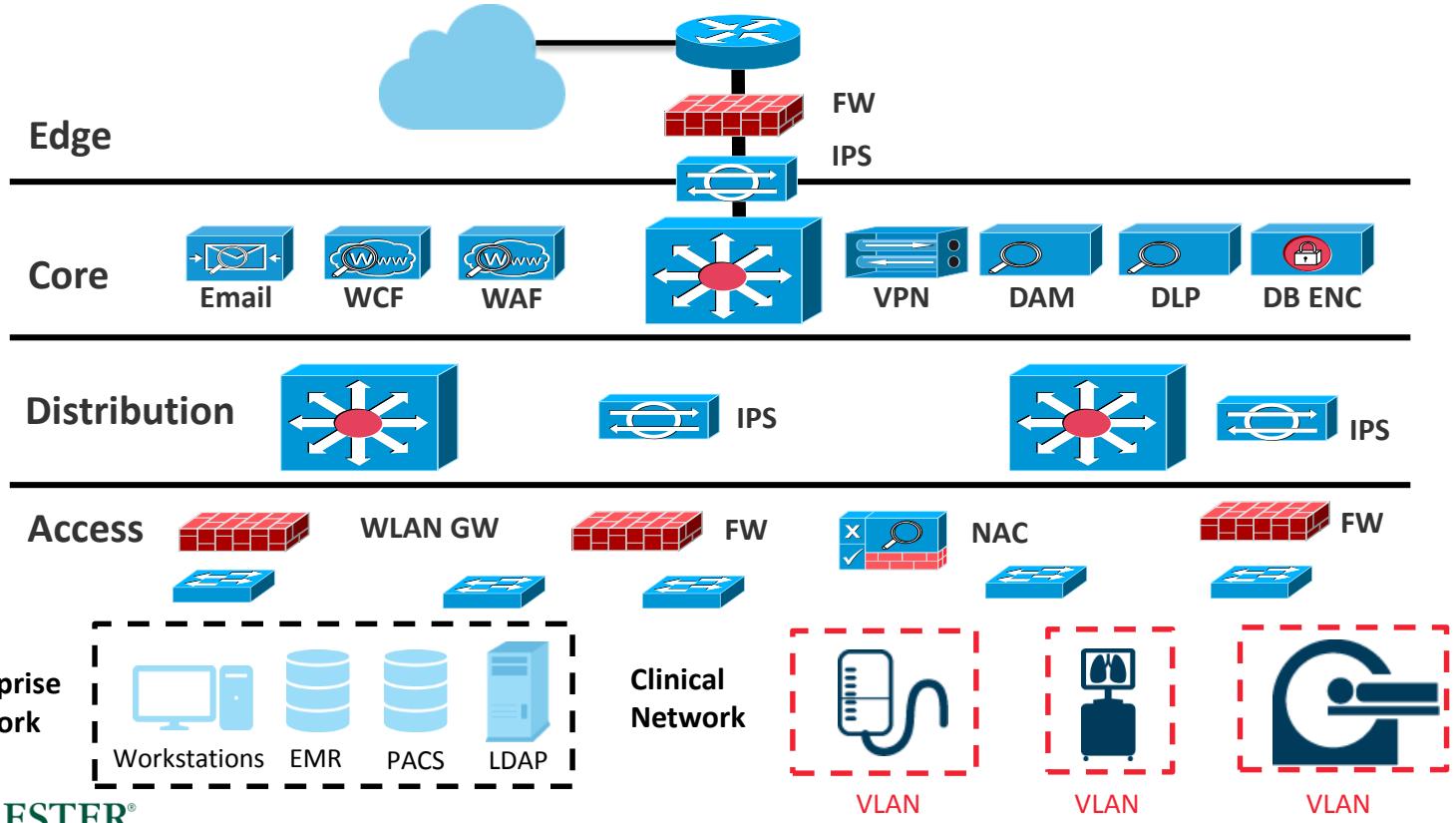
With Innovation Comes Risk



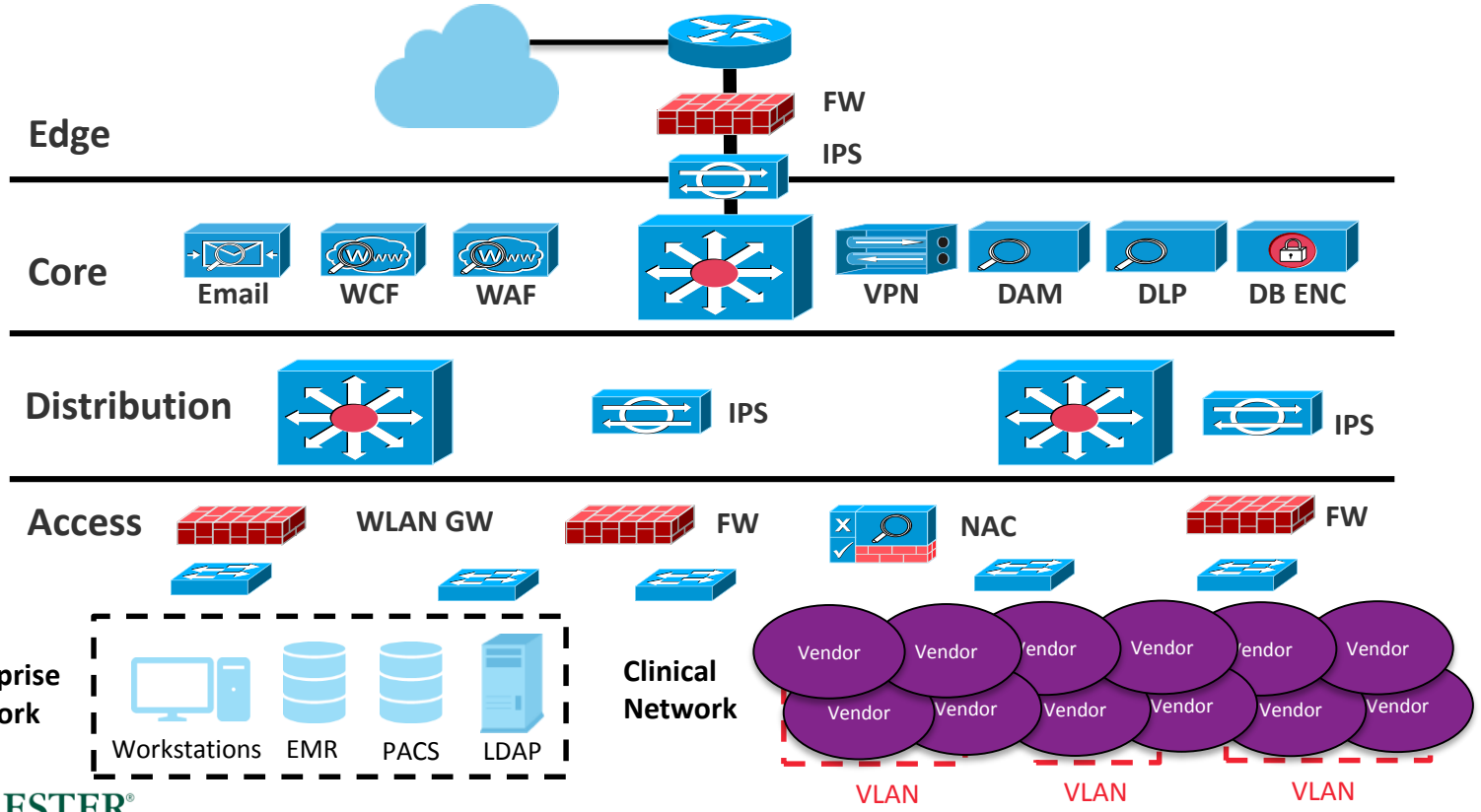


The Medical Device Risk Landscape

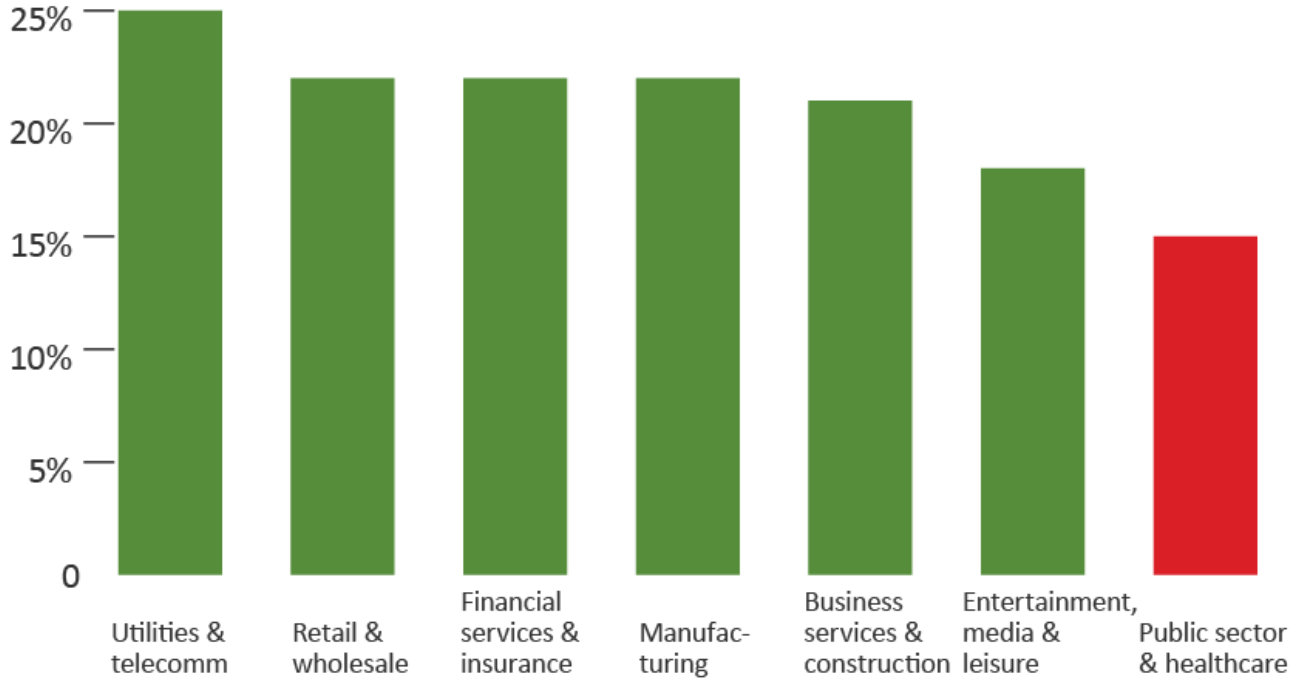
A Typical Hospital Network is Flat



Complexity Is The Primary Enemy

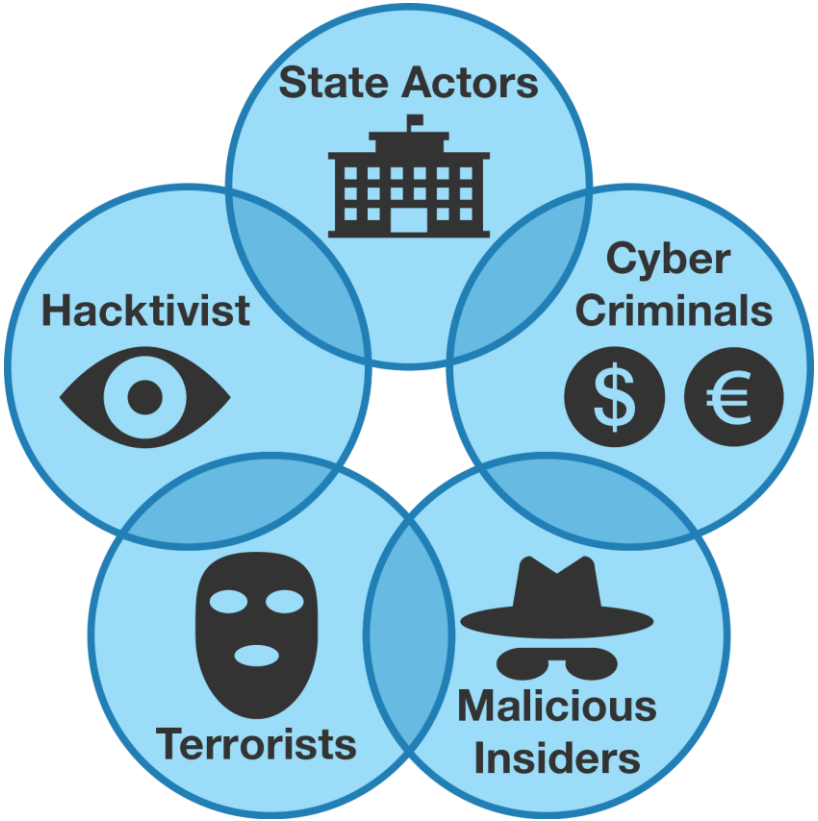


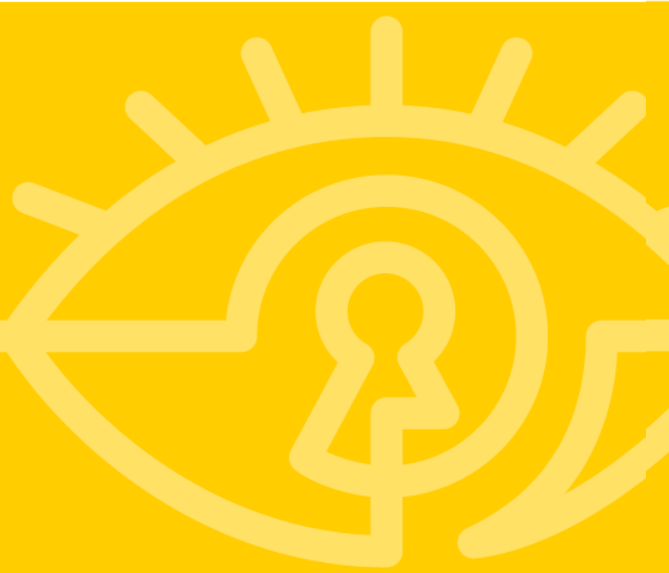
Healthcare Security Spending Lags



Base: 315 Global security decision-makers (20+ employees) in public sector and healthcare
Source: Forrester's Global Business Technographics® Security Survey, 2015

Threat Actor Motivations





Attack Scenarios

Collection of Evidence

- Conducted 70+ medical device security stakeholder interviews
- Surveyed 400+ US-based hospital security decision makers in Q2 2015; 1,900 hospital information workers in Q3
- Identified public and non-public sources of incident data with the help of Cyberfactors, the FDA, MDISS, HIMSS, and various industry experts

Collection of Evidence (Cont.)

Dream Market

SHODAN
Computer Search Engine

TheRealDeal

Grams

AlphaBay Market

Medical Device Security - Risk Categories

Denial-of-Service

Therapy Manipulation

Patient Data Theft

Asset Damage

Denial-Of-Service: Scenario

Causes

> Network attack

> Malware

> Hardware/software exploitation

> Radio frequency (RF) exploitation

Impacts

> Clinical workflow disruption

> IT/Clinical engineering staff disruption

Outcomes

> Patient harm

> Reputational damage

> Regulatory fines/Lawsuits

> Request for ransom

Denial-Of-Service: Evidence

- Case #1: Catheter lab incident
- Case #2: 20 patient monitoring systems taken down in a California-based hospital (unreported)
- Case #3: MA-based hospital ward shut down due to malware infecting medical devices (unreported)
- Case #4: CA-based hospital shutdown due to ransomware infecting medical devices

Denial-Of-Service: Outlook

Impact		Likelihood		Existing Controls
Patient Safety **High**	+	Existing Vulnerabilities **High**	−	**Medium**
Clinical Workflow **High**		Existing Exploits **Medium**		

= **High Severity Risk**

Therapy Manipulation: Scenario

Causes

> MALWARE

> HARDWARE/SOFTWARE EXPLOITATION

> POOR ACCESS CONTROLS

> PHYSICAL TAMPERING

Impacts

> CHANGES IN DEVICE FUNCTION/PARAMETERS

> CHANGES TO PATIENT DATA

Outcomes

> PATIENT HARM

> REPUTATIONAL DAMAGE

> REGULATORY FINES/LAWSUITS

> REQUEST FOR RANSOM

> CHANGES IN FUTURE TREATMENT DECISIONS

Therapy Manipulation: Evidence

- Case #1: PCA Pump exploited by Austrian patient
- Case #2: PCA Pump exploited by researcher
- Case #3: Insulin Pump exploited by researcher
- Case #4: Implantable Defibrillator exploited by researcher

Therapy Manipulation: Outlook

Impact		Likelihood		Existing Controls
Patient Safety **High**	+	Existing Vulnerabilities **Medium**	−	**Medium**
Clinical Workflow **High**		Existing Exploits **Low**		

= **Medium Severity Risk**

Patient Data Theft: Scenario

Causes

> Malware

> Hardware/software exploitation

> Poor access controls/device theft

> Device used as entry point into data network

Impacts

> Direct theft of data from device

> EMR database compromise

Outcomes

> Patient harm due to fraud

> Patient privacy loss

> Request for ransom

> Reputational damage

> Regulatory fines/ Lawsuits

Patient Data Theft: Evidence

- Case #1: HIPAA fines due to CT Scanner breach
- Case #2: Russian gang used medical devices as entry point into hospital network; stole patient data from EMR

Patient Data Theft: Outlook

Impact		Likelihood		Existing Controls
Patient Safety **Medium**	+	Existing Vulnerabilities **High**	−	**Medium**
Clinical Workflow **Low**		Existing Exploits **High**		

= **Medium Severity Risk**

Asset Damage: Scenario

Causes

> Network attack

> Malware

> Hardware/software exploit

Impacts

> Clinical workflow disruption

> IT/Clinical engineering staff disruption

Outcomes

> Patient harm

> High replacement costs

> Reputational damage

> Regulatory fines/ Lawsuits

> Request for ransom

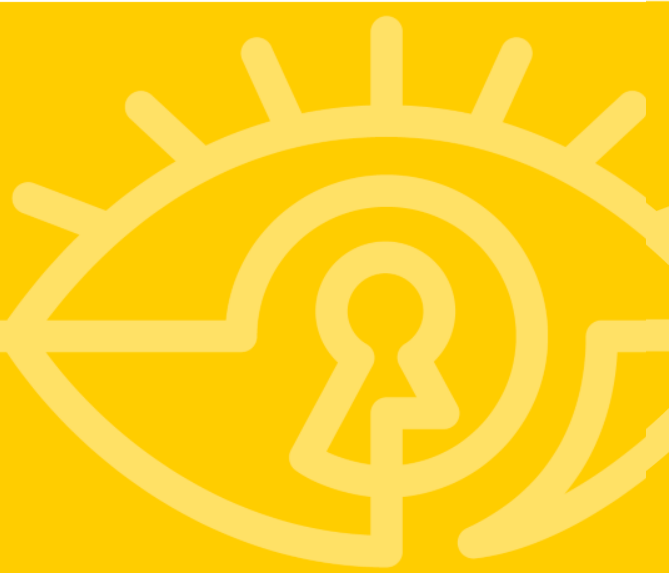
Asset Destruction: Evidence

- No examples found
- Difficult to track due to lack of consideration over security event causation in MDRs

Asset Destruction: Outlook

Impact		Likelihood		Existing Controls
Patient Safety **High**	+	Existing Vulnerabilities **Low**	−	**High**
Clinical Workflow **High**		Existing Exploits **Low**		

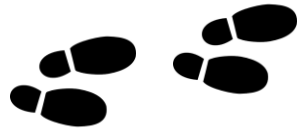
= **Low Severity Risk**



The Path Forward

5 Steps Forward: Apply At Your Organization

1. Categorize Existing Devices Based On Risk
2. Implement A Clinical Risk Management Framework
3. Follow Basic Security Hygiene
4. Include Security Requirements In New Device RFPs
5. Move Toward A “Zero-Trust” Networking Architecture

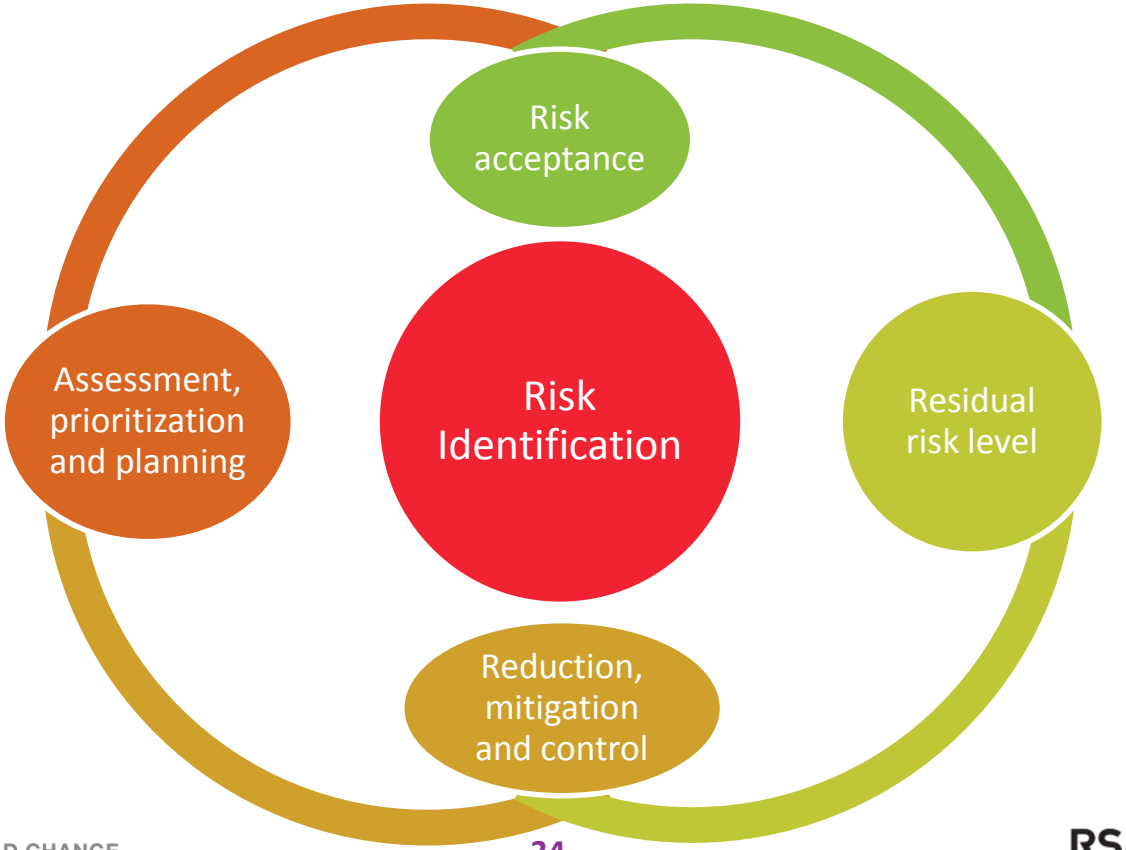


Step 1: Categorize Existing Devices Based On Risk

- Base your risk categories on:
  - Potential impact to patient safety
  - Network Connectivity
  - Data Sensitivity
  - Attack likelihood
  - Upgradability

Step 2: Implement A Clinical Risk Mgmt Framework

IEC 80001-1



Step 3: Follow Basic Security Hygiene

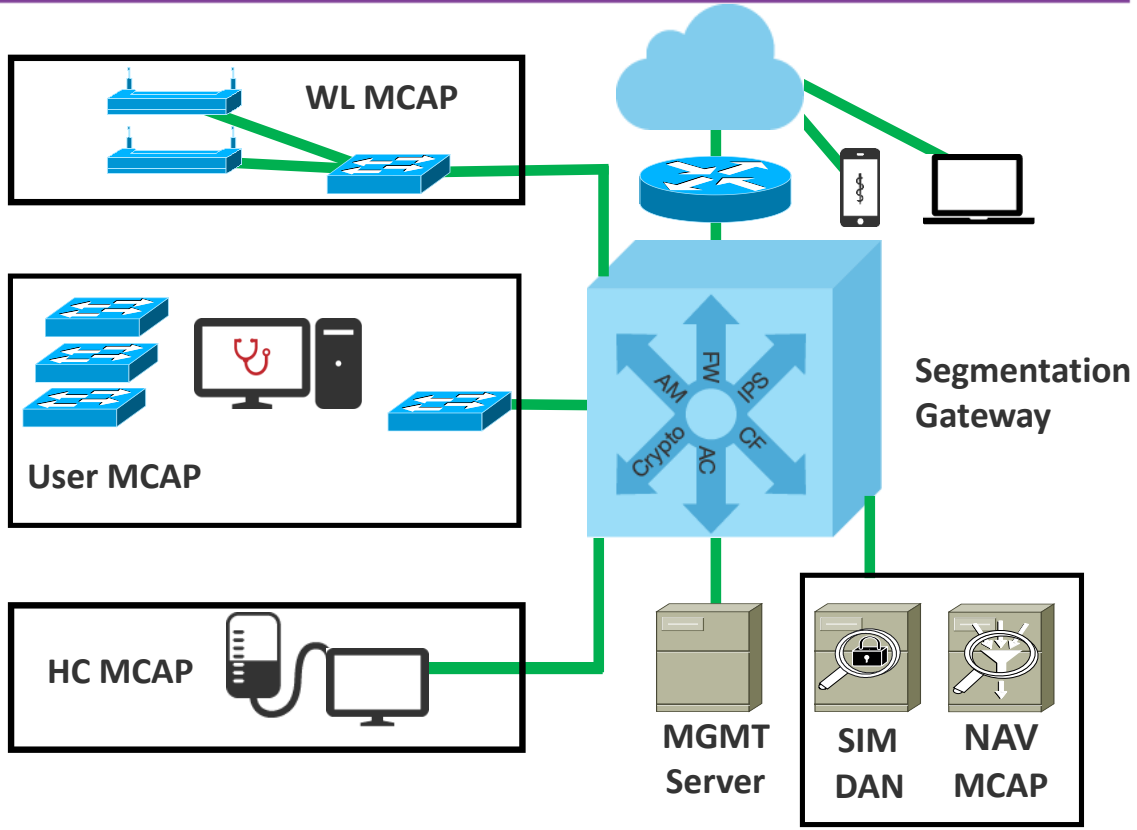
- Foster a culture of security awareness within clinical engineering and clinical departments
  - Blogs, security champions, rotationships
- Eliminate default passwords

Step 4: Include Security Requirements In RFPs

- Request that device manufacturers:
  - Follow current application security security best-practices
  - Conduct threat modeling/pen testing
  - Have roadmap to build security logging into software
  - Present a completed MDS^2 form

Step 5: Move Toward A "Zero-Trust" Architecture

- Segment devices based on risk
- Inspect network data as it flows between segments
- Require secure authentication into network



Need to Know

- IEC 80001-1
- MDS^2
- NH-ISAC
- ICS-CERT
- FDA Pre-Market and Post-Market (Draft) Cybersecurity Guidance

Thank you

Chris Sherman
csherman@forrester.com

@ChrisShermanFR