Crowe Horwath

Smart decisions. Lasting value.™

Crowe Healthcare Webinar Series

It's 2018. Do You Know Who and What Is Connected to Your Network?

Presented by:
Chris Reffkin, MS, CISSP, Senior Manager at Crowe Horwath LLP
Jim Plasynski, Vice President at Great Bay Inc.

Housekeeping

- Please note that all of today's audio is being broadcast cast to your computer speaker
- Please submit questions through the Q&A function on your screen. Questions will be addressed at the end of the presentation.
- To download a copy of the presentation or access the resources connected to this session, please visit the resources icon at the bottom of your console

CPE Details

- **CPE Credit**
  - Login individually to the session
  - Successfully complete 3 of the 4 polling questions

- **NO CPE Credit**
  - Fail to successfully complete 3 of the 4 polling questions
  - Viewing a recording of this session (CPE is only awarded for live sessions)

- **Upon completion of this program you will receive a post event evaluation**

- **Your feedback is important**
  - CPE certificate of completion
  - E-mailed within two weeks of upon successfully passing this program

Crowe Horwath

Smart decisions. Lasting value.™

Crowe Healthcare Webinar Series

It's 2018. Do You Know Who and What Is Connected to Your Network?

Presented by:
Chris Reffkin, MS, CISSP, Senior Manager at Crowe Horwath LLP
Jim Plasynski, Vice President at Great Bay Inc.

Learning Objectives

As a result of participating in this webinar, you should be able to:

- Identify the benefits of a holistic approach to cybersecurity management that includes clinicians, risk management, and IT professionals
- Recognize the benefits of a renewed focus on "Security 101" while evolving to proactively managing the ever-changing IT environment
- Recognize that these emerging issues are not only a risk to IT systems but can directly affect patient safety and the overall organization

Agenda

This webinar will cover the following topic areas:

- Current State of Healthcare Security and Medical Devices
- Benefits versus Risks
- Impact on Patient Trust and Revenue
- The Visibility Challenge
- Security 101
- Medical Device Risk Landscape and Journey
- Where to Begin

The Current State of Healthcare Security and Medical Devices

The state of healthcare security

More devices than ever

Uncertain device security

Concern for patient safety

Sources:
Icons by corpus delicti and Luis Prado from Noun Project

Healthcare has more devices than ever before

- By 2020, IoT devices will outnumber users with laptops, tablets or smartphones **by more than three times**.—*Gartner*
- Today's hospitals have **15-17 devices per bed**.—*ECRI*
- Hospitals typically have **300-400% more medical equipment** than IT devices.—*HIMSS*

Built-in medical device security is lacking

Only 9%

of manufacturers say they test medical devices at least annually.

Only 51%

of device makers say they follow guidance from the FDA to mitigate or reduce inherent security risks in medical devices.

Unsurprisingly, 67%

of device makers believe it is likely there will be an attack on one of the devices they've built within the next 12 months. —*Ponemon 2017*

Sources:
Ponemon Institute: Medical Device Security: An Industry Under Attack and Underprepared to Defend, May 2017

Balancing Benefits and Risks of Medical Devices

Medical Device Benefits

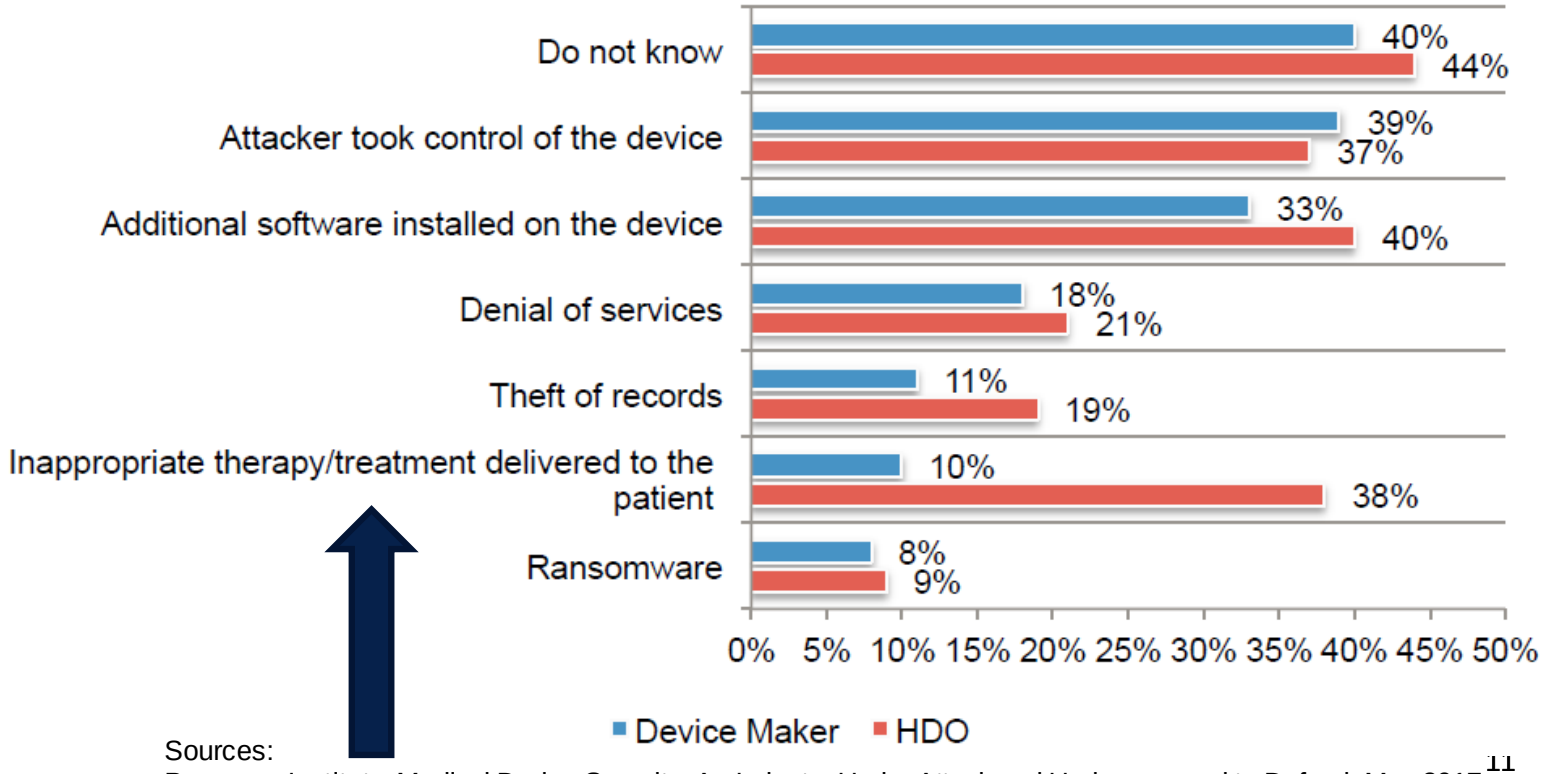
Today's medical devices help reduce healthcare costs while allowing people to better manage their conditions.

- *The use of remote monitoring to improve the health of people with chronic diseases is estimated to save as much as $1.1 trillion per year by 2025.*

Medical Device Risks

But these devices aren't without risks to patient safety and continuity of care.

- *Ransomware attacks*
- *Vulnerabilities in implantable devices*
- *Tele-care or tele-health interruptions*
- *Vulnerabilities in medical devices such as imaging, diagnostic, etc.*



Sources:
Ponemon Institute: Medical Device Security: An Industry Under Attack and Underprepared to Defend, May 2017

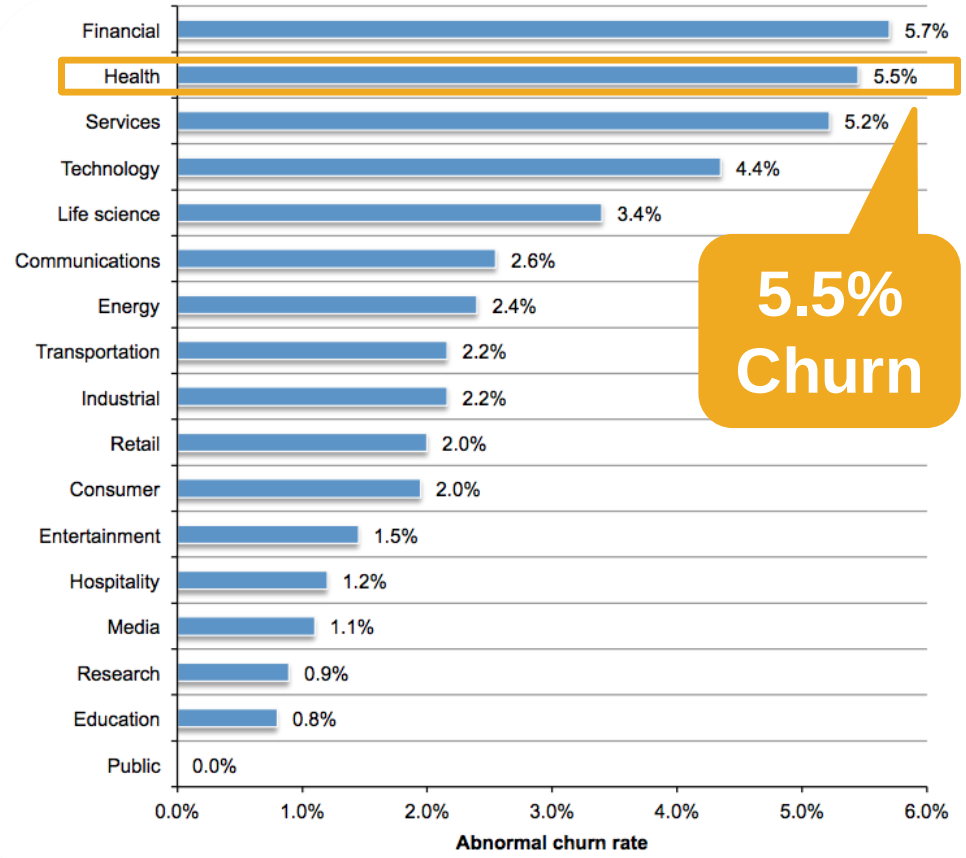
Impact of patient trust on HDO revenue – post breach

Why such high churn?

- 63% of consumers say their privacy is most important to them when they visit their healthcare provider—more than any other activity they do (social media, internet searches, filing tax returns, conducting bank transactions).

The result of broken trust:

- Revenue loss for your organization. When customer churn is greater than 4%, the cost to the organization is estimated to be more than $5.1 million.



Sources:
Ponemon Institute: Medical Device Security:
An Industry Under Attack and Underprepared to Defend, May 2017

Polling Question 1

What area do you feel is the least risky (most well managed) for patient safety and organizational impact:

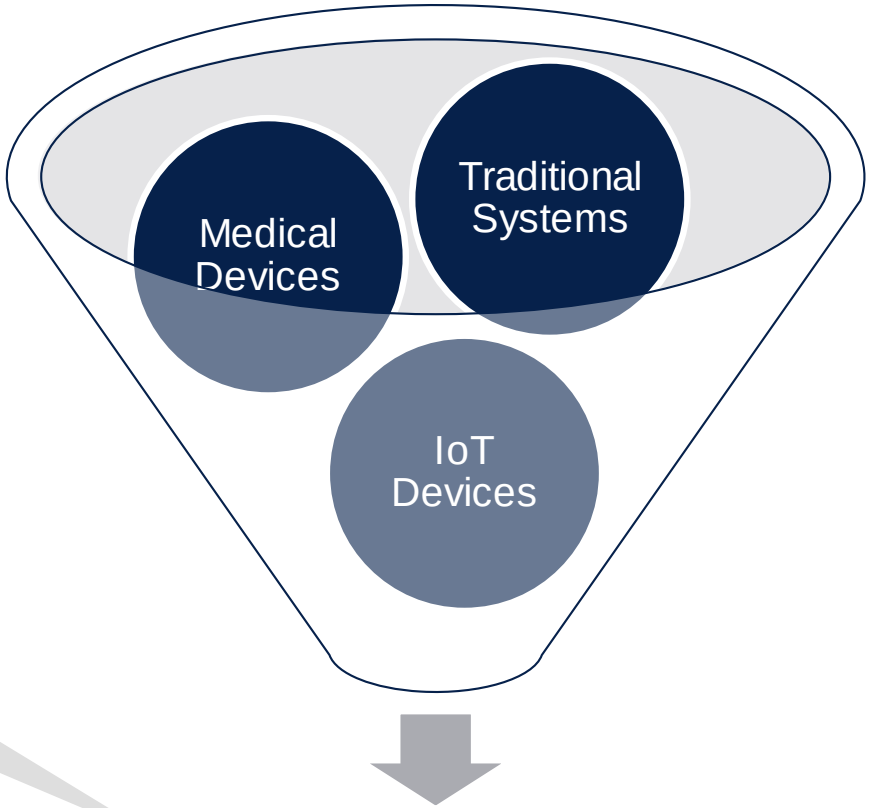
1) Traditional Systems (e.g. applications, workstations, etc.)
2) Medical Devices (networked attached)
3) Medical Devices (all)
4) IoT Devices (e.g. IP cameras, HVAC, etc.)
5) None

Defining the Entire Visibility Challenge

Where's the Risk?

Technology in the path of care

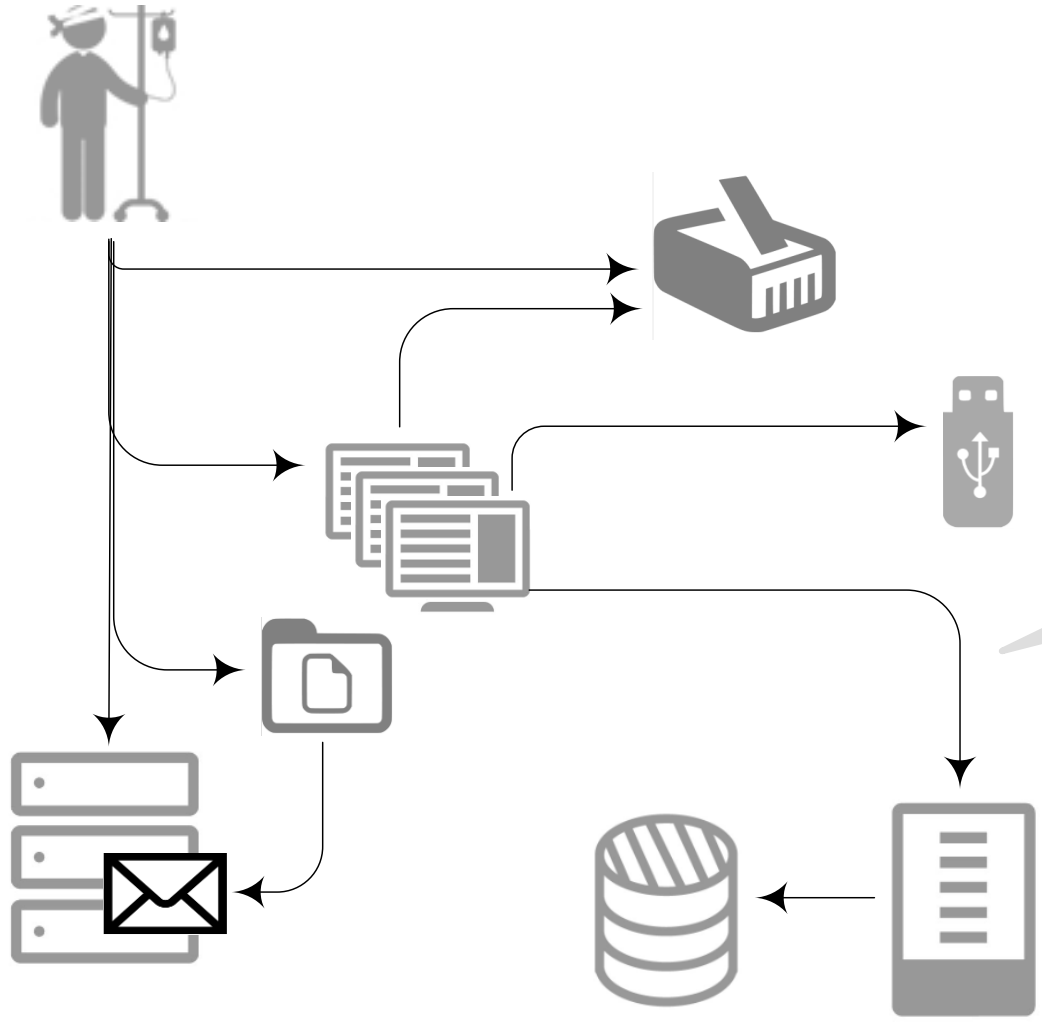
Direct impact to patient care **does not stop at the infusion pump**. Any device or networked technology in the **path of care** can represent a risk to patient safety and security.



Impact on the Path of Patient Care

Where's the Risk?

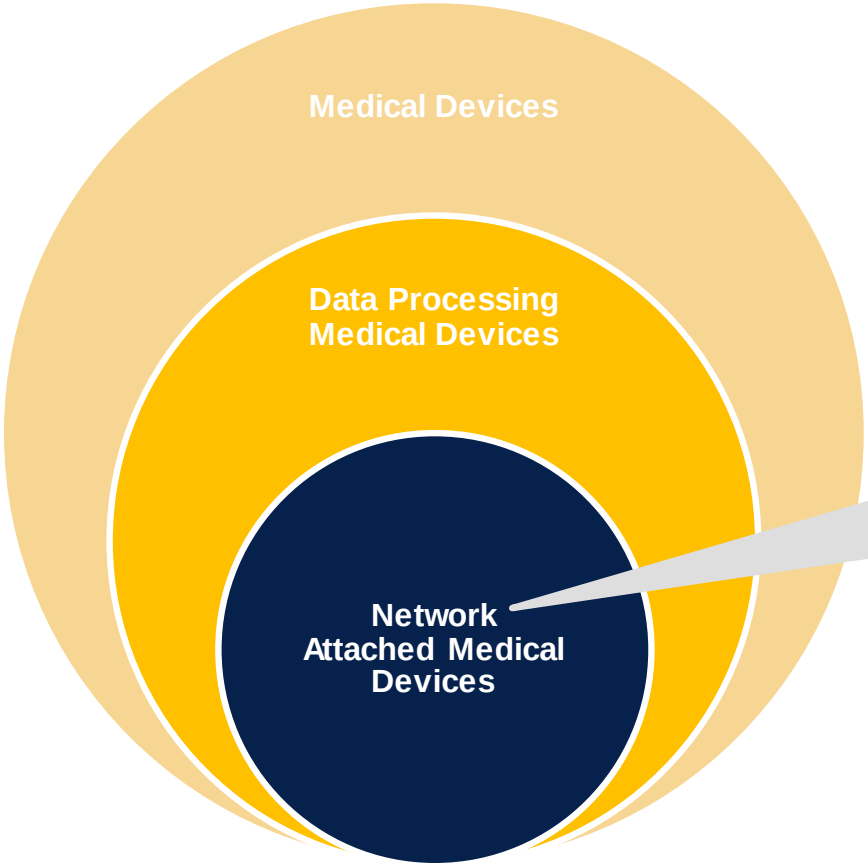
Traditional technology in the path of care



Traditionally, security has followed the flow of **patient data** which has been in pursuit of **privacy** and **confidentiality**.

Where's the Risk?

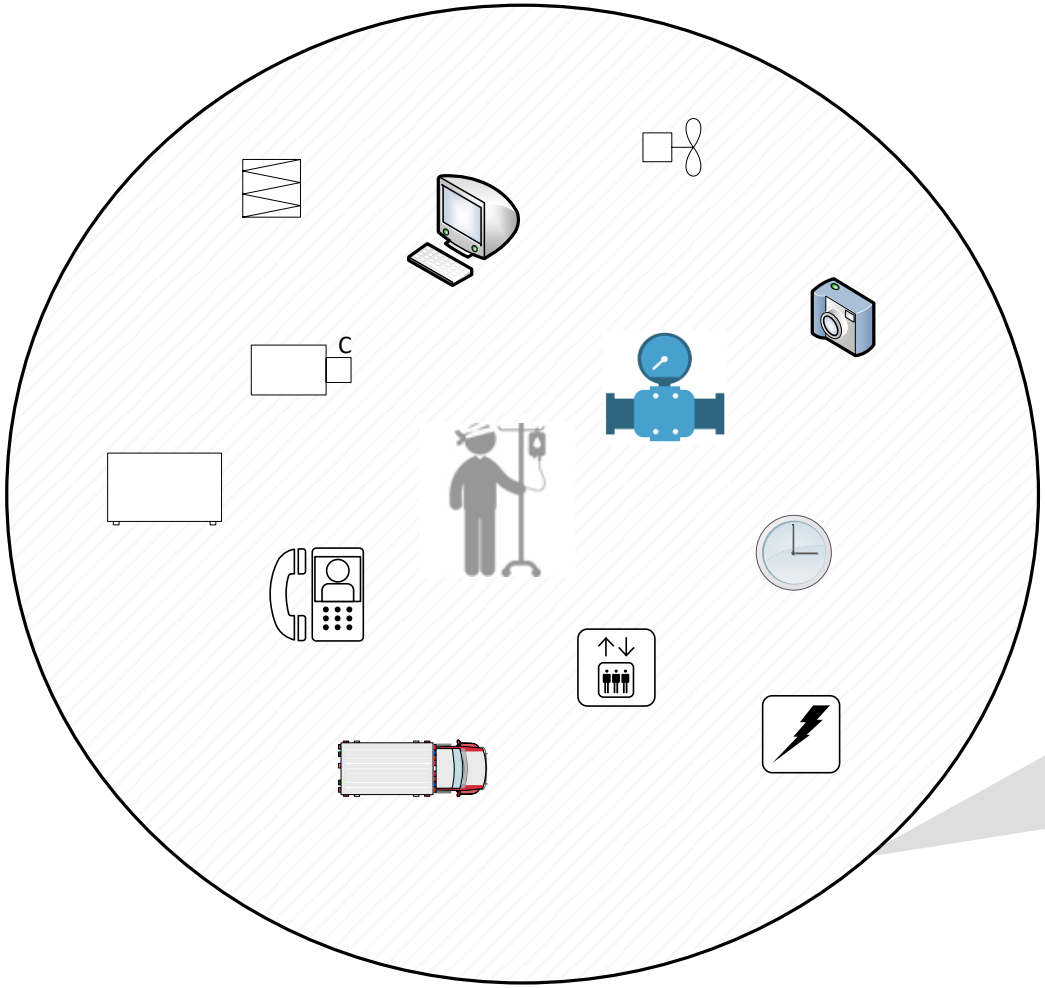
Medical device technology in the path of care



In the world of ransomware, botnets, and data exfiltration, network attached medical devices pose **substantial risk** the security of healthcare organizations of the **safety of their patients**.

Where's the Risk?

IoT technology in the path of care



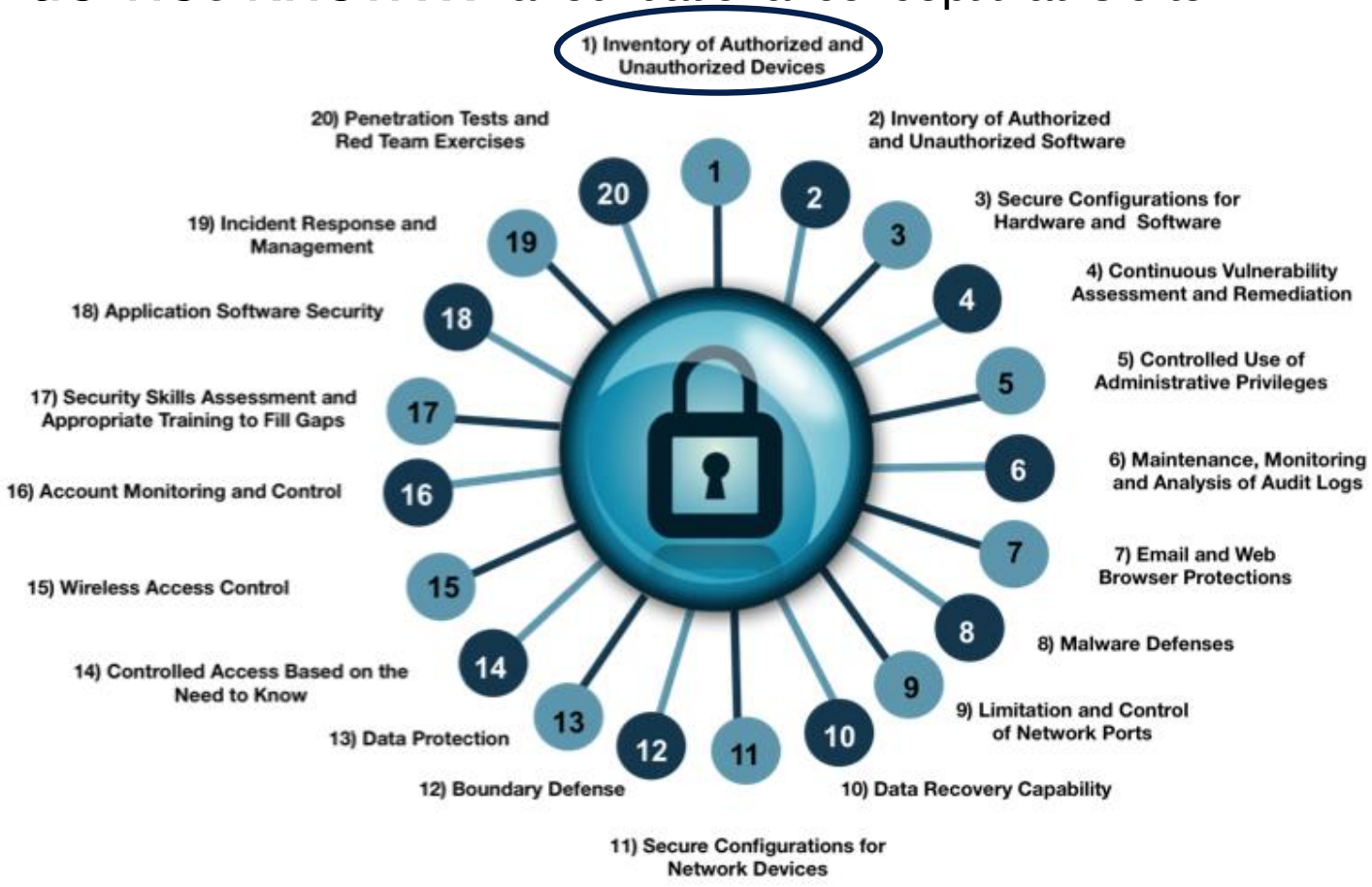
Beyond traditional systems, and medical devices, there are more systems and devices that can have the equivalent or greater impact on patient safety.

Anything attached to the network is a risk and most HC systems do not have proper segmentation that is effective… so HVAC, elevators, IP cameras, payment systems, security systems, etc.

Forgotten element of Security Fundamentals

- You cannot secure what you do not know… a foundational concept that is often overlooked but is not hidden…

- CISSP Domains
- SANS - #1 CIS Top 20
- NIST Cybersecurity Framework
- PCI
- HIPAA
- And the list goes on…



Source: Center for Internet Security 2016

Polling Question 2

Where do you believe your organization has the greatest opportunity to enhance its posture with:

1) Physical and digital risk assessments
2) Network design
3) Device visibility

Back to Basics… Security 101

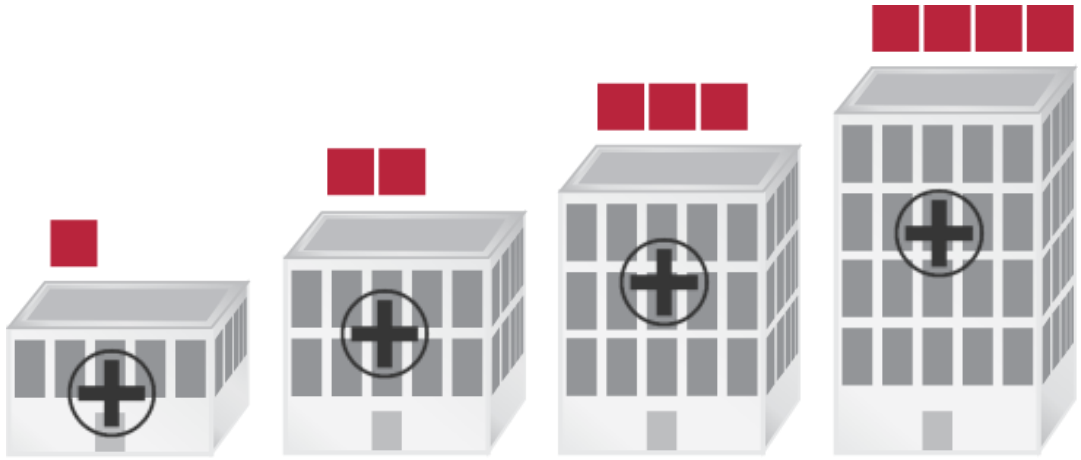
Strengthening security maturity is multi-faceted effort

Security functions must work together along with other key stakeholders.

Governance, Risk & Compliance

Security Architecture

Security Operations & Incident Response



<u>One size does not fit all</u>

But there are foundational principles.

Understanding Fundamentals is Key

Current State Assessments

- Do we understand the current state of **people, process, and controls** related to the overall security program?
- Do we understand the impact to patient safety, operations, reputation, revenue, etc.?

IT and Network Strategy

- Does our **business strategy** align with our **IT strategy** and does our **security strategy support both?**
- Is our security strategy **risk-centric** or is it **threat or compliance centric?**

Real-Time Network & Device Visibility

- Do we have a clear line of sight into devices on the network, their location and their activity?
- Is inventory information intelligent and actionable?

Critical questions to ask:

- Do I know what devices are connected to the network?
- Do I know how the device is behaving?
- Do I have a way to determine if a device should be trusted?
- Do I know where a device is located?
- Do I know this information at all times?

Highlighting the impact

This history has led to..

- Technology historically **developed without security & risk** considerations
- **Long lifecycles** of medical devices
- **Numerous stakeholders**, and competing interests
- Limited regulatory guidance
- Lack of **patching** and technical support
- Confusion of terms and **scope**
- Clinical/cultural **awareness**

This reality.

WannaCry attack in summer 2017 crippled 40+ hospitals in the UK affecting CT scanners, x-ray machines, and overall treatment, payment, and operations

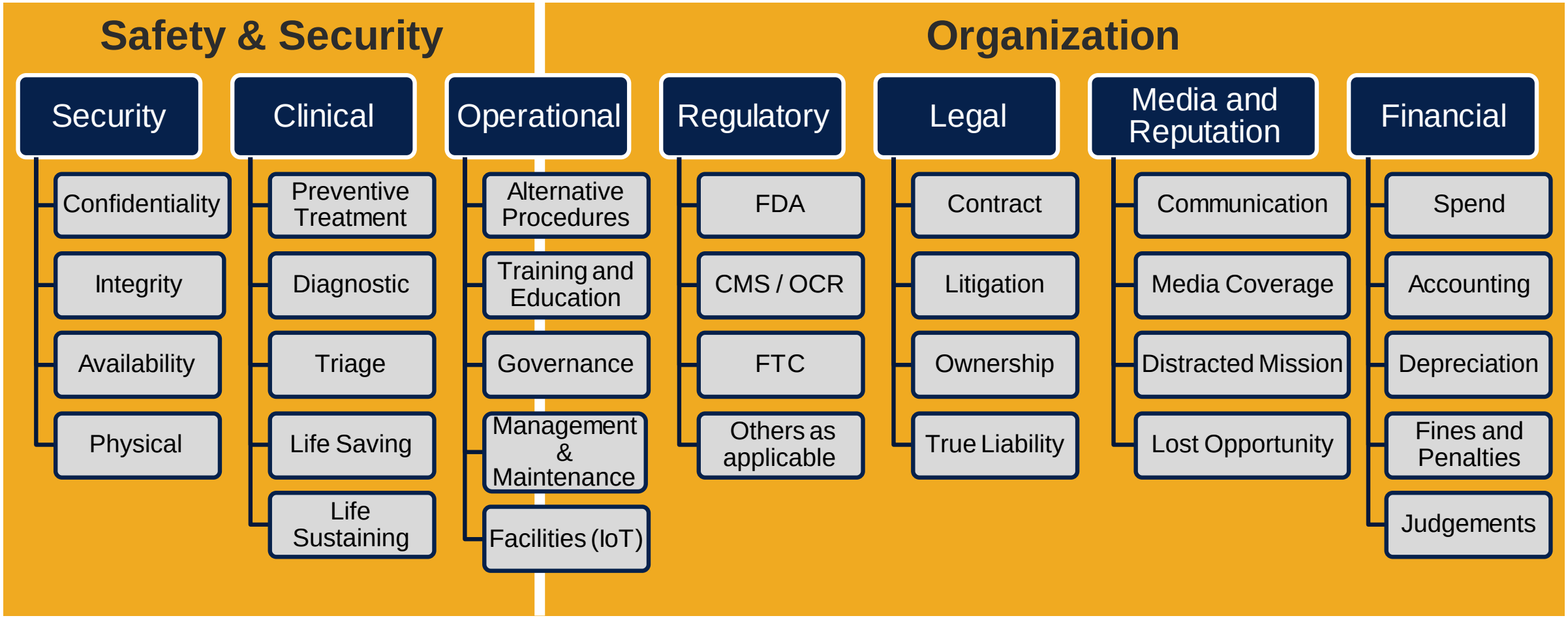
Sources:
https://blog.knowbe4.com/eu-to-declare-cyber-attacks-act-of-war.-usa-likely-to-follow
http://www.wired.co.uk/article/nhs-trusts-affected-by-cyber-attack

Polling Question 3

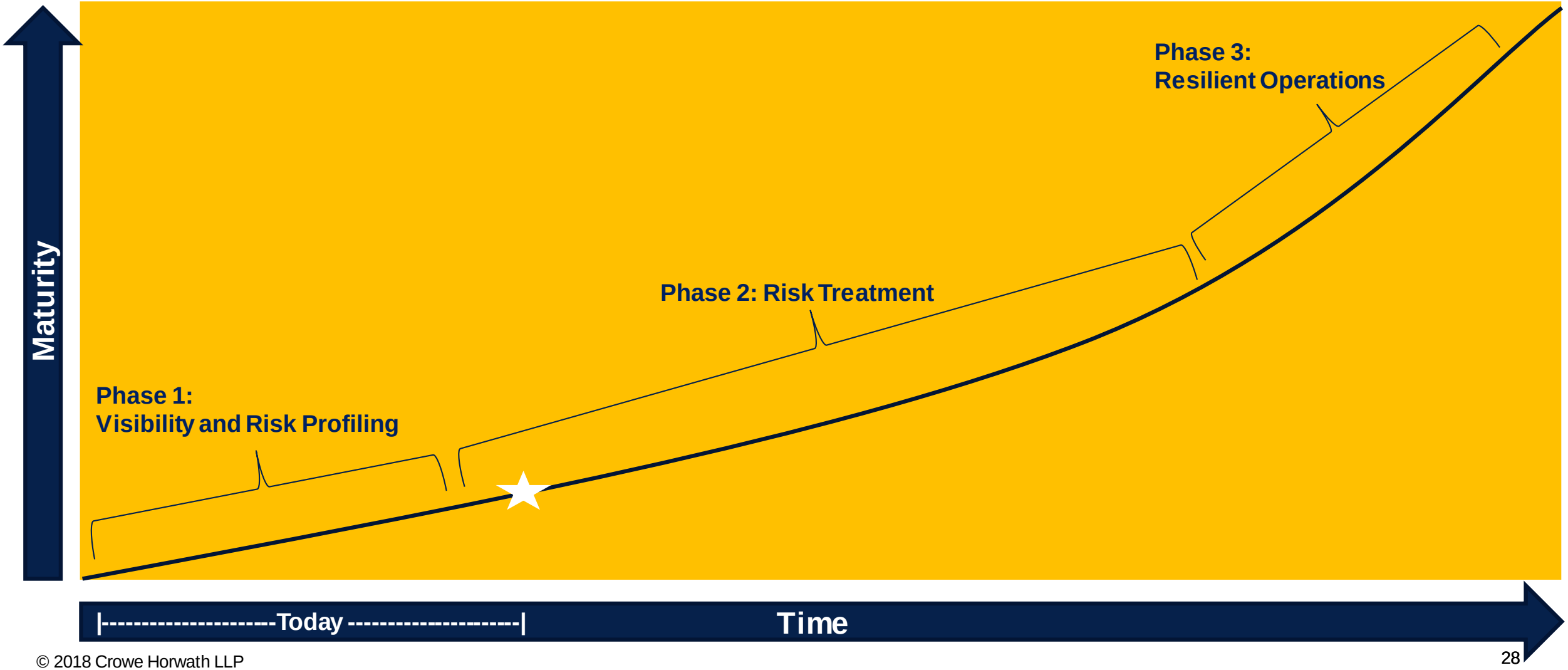
How does the organization educate the workforce as well as the C-Suite and Board as to the ramifications of good security practices:

1) Only focus on workforce
2) Occasional reporting to the Board
3) Not much, the Board gets what it needs from the Wall Street Journal
4) Established quarterly reporting

Medical Device Risk Landscape



Journey to Medical Device Security Maturity



Sample – Comprehensive Medical Device Risk Scorecard

		Risk Landscape						
		Patient Safety	Security	Operations	Regulatory	Legal	Media & Reputation	Financial
Medical Device Risk Management	Visibility & Inventory	High	High	High	Moderate	Moderate	Moderate	High
	Program Management	High	High	High	Moderate	High	Moderate	Moderate
	Risk Profiling	High	High	Moderate	High	Moderate	Moderate	Low
	Risk Treatment	High	High	High	High	Moderate	Moderate	High
	Resilient Operations	High	Moderate	Moderate	Moderate	Moderate	Low	High

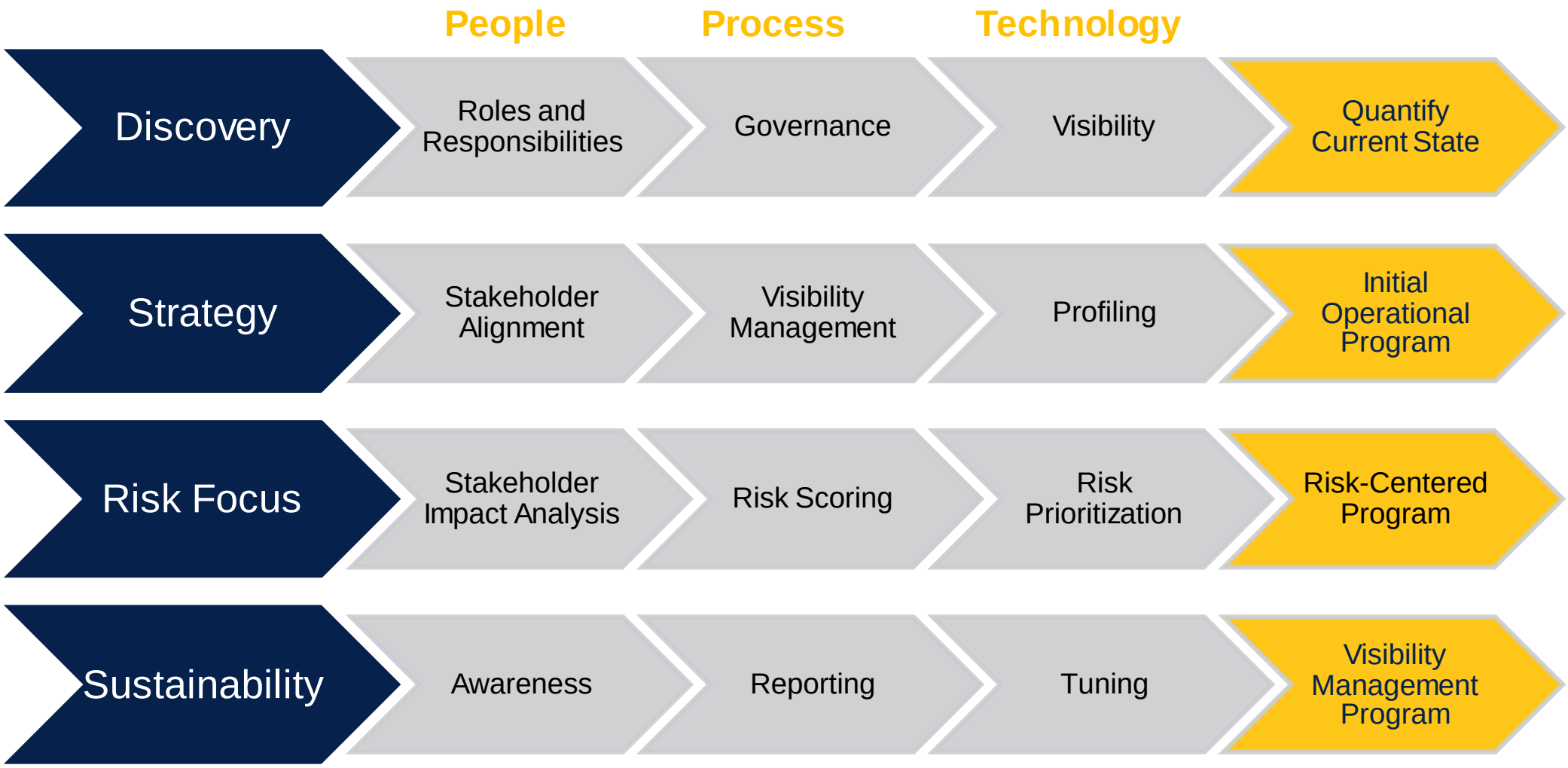
Polling Question 4

What area do you believe your organization is most likely to invest (financially, resources, etc.) to reduce risk:

1) Traditional security (passwords, patching, etc.)
2) Insurance
3) Evolving security capabilities such as network visibility and control
4) Device-specific security mitigation
5) Other

Where to begin…

Focus on achieving a sustainable visibility management program



Questions

Thank You

Chris Reffkin, MS, CISSP

Phone +1 317 208 2547
chris.reffkin@crowehorwath.com
https://www.crowehorwath.com/cybersecurity

Jim Plasynski

Phone +1 763 251 1418
jplasynski@greatbaysoftware.com
https://greatbaysoftware.com