Medical Device Security: The Transition From Patient Privacy To Patient Safety

Scott Erven

Who I Am

Scott Erven

Scott Erven is an Associate Director at Protiviti with over 17 years of information security and information technology experience with subject matter expertise in medical device and healthcare security. **Scott has advised the US Department of Homeland Security, Health and Human Services, Food and Drug Administration as well as national policymakers.** His research on medical device security has been featured in Wired, Forbes, BBC and numerous media outlets worldwide. He has been involved in numerous IT certification development efforts as a subject matter expert in information security. His current focus is on research that affects human life and patient safety issues inside today's healthcare landscape.

- ***Associate Director – Medical Device & Healthcare Security***
- ***Security Researcher***
- ***Over 17 Years Experience - 5 Years Experience Managing Security Inside Healthcare Systems***
- ***Over 4 Years Researching Medical Device Security***

Agenda

Why Research Medical Devices

Phase 1 Research: Device Vulnerabilities

Phase 2 Research: Internet Exposure

Phase 3 Research: Admin Access

Honeypot Research: Are Attacks A Reality?

Problem Awareness

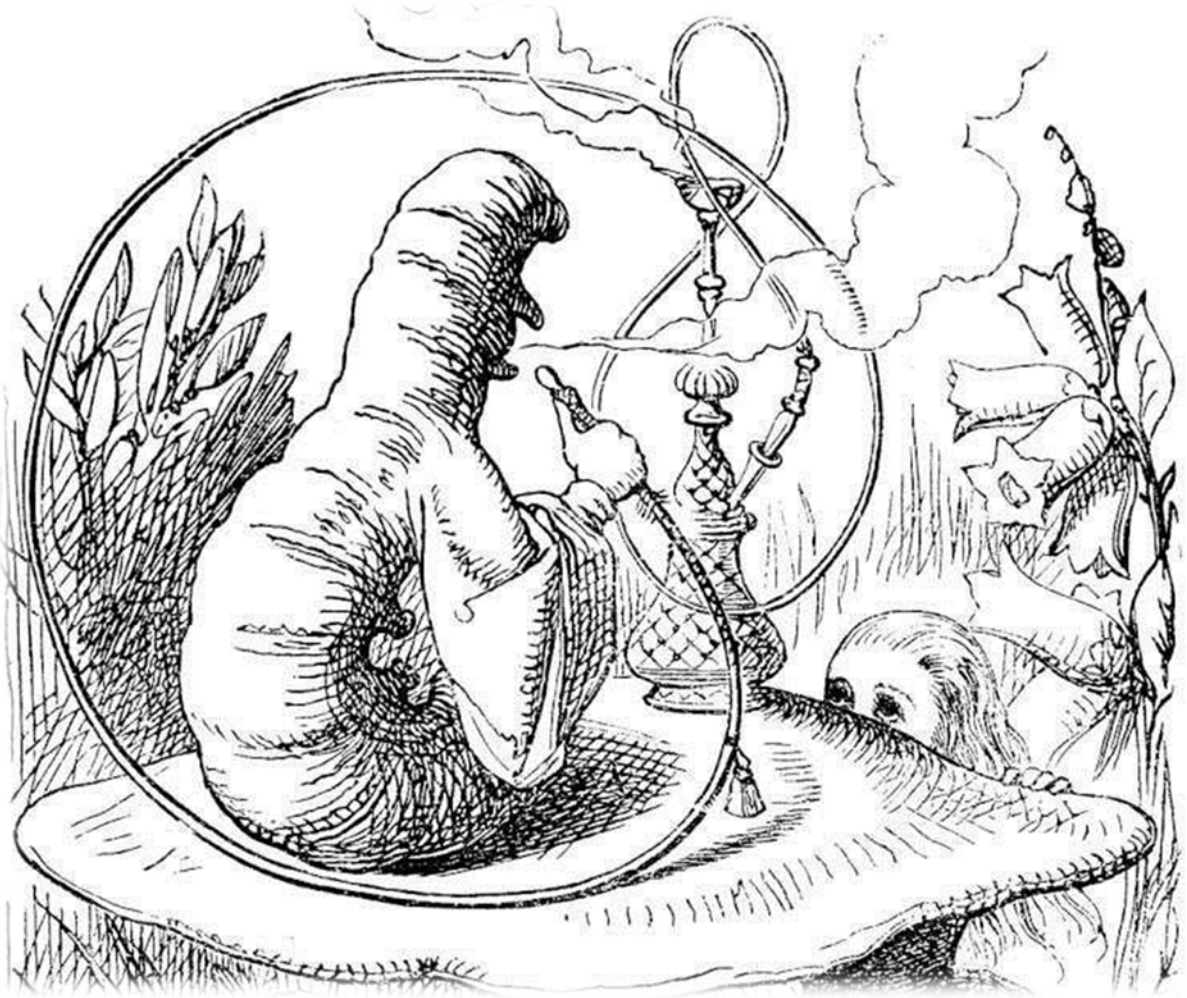
Treatment Plans

Why Research Medical Devices

Personal & Professional Impact

- Many individuals rely on these devices daily.
- Even at times when we aren't personally affected, people we care about may be.
- Patient safety and quality care is at the core of healthcare's mission and values.

Malicious Intent Is Not A Prerequisite To Patient Safety Issues



What We Are Doing

Medical Device Assessment	Discover patient safety issues

- Security-Focused Technical Assessment (not HIPAA)
- Research serves healthcare mission and values
- Equip defenders against accident and adversaries

Coordination & Notification	Alert affected parties

- Healthcare Providers
- Medical Device Manufacturers
- Government Agencies (FDA and ICS-CERT)

Public Awareness	Inoculate against future issues

- Security and Healthcare Conferences
- 1-on-1 with healthcare providers
- Educating FDA and Healthcare Providers

Phase 1 Research: Device Vulnerabilities

Phase 1 Research: Device Vulnerabilities

Weak default/hardcoded administrative credentials

- Treatment modification
- Cannot attribute action to individual

Known software vulnerabilities in existing and new devices

- Reliability and stability issues
- Increased deployment cost to preserve patient safety

Unencrypted data transmission and service authorization flaws

- Healthcare record privacy and integrity
- Treatment modification

Phase 2 Research: Internet Exposure

Shodan Search Initial Findings

Doing a search for anesthesia in Shodan and realized it was not an anesthesia workstation.

Located a public facing system with the Server Message Block (SMB) service open, and it was leaking intelligence about the healthcare organization's entire network including medical devices.

Initial Healthcare Organization Discovery

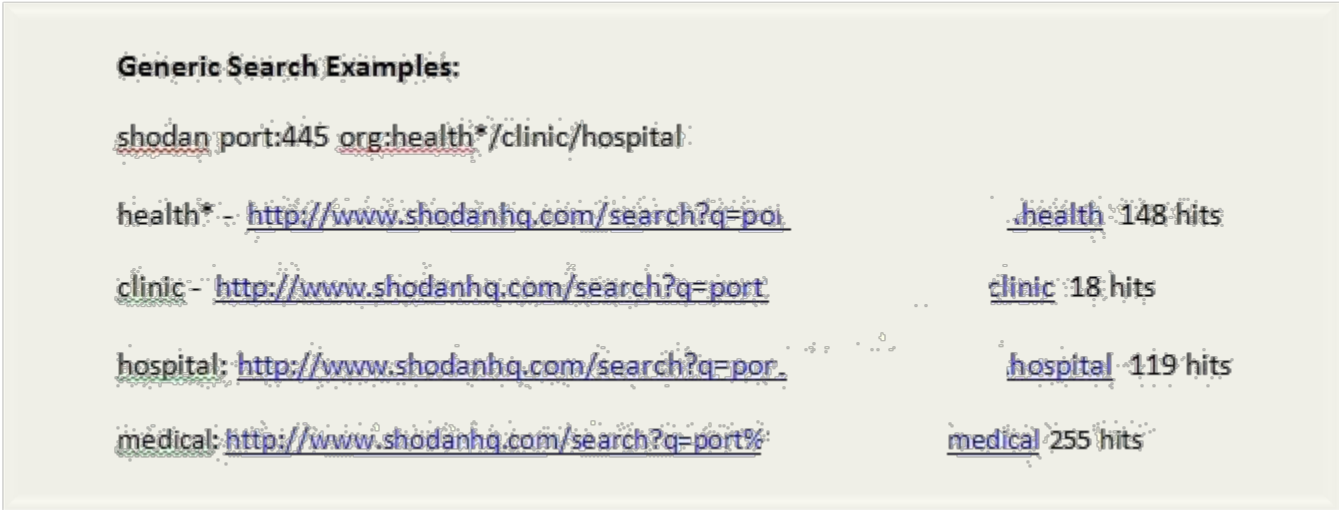
Very large US healthcare system consisting of over 12,000 employees and over 3,000 physicians. Including large cardiovascular and neuroscience institutions.

Exposed intelligence on over 68,000 systems and provided direct attack vector to the systems.

Exposed numerous connected third-party organizations and healthcare systems.

Did We Only Find One?

No. We found hundreds!!



Change the search term and many more come up. Potentially thousands if you include exposed third-party healthcare systems.

Summary Of Devices Inside Organization

- Anesthesia Systems – 21
- Cardiology Systems – 488
- Infusion Systems – 133
- MRI – 97
- PACS Systems – 323
- Nuclear Medicine Systems – 67

Potential Attacks - Physical

We know what type of systems and medical devices are inside the organization.

We know the healthcare organization and location.

We know the floor and office number.

We know if it has a lockout exemption.

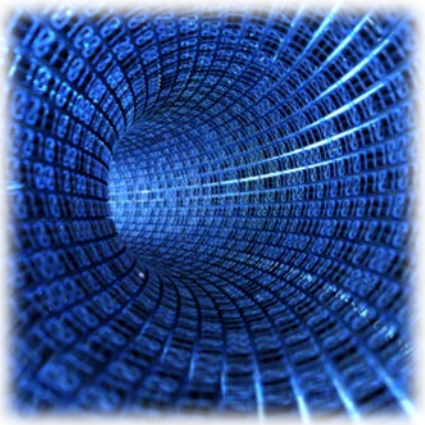
Potential Attacks - Phishing

- *We know what type of systems and medical devices are inside the organization.*
- *We know the healthcare organization and employee names.*
- *We know the hostname of all these devices.*
- *We can create a custom payload to only target medical devices and systems with known vulnerabilities.*

Potential Attacks - Pivot

We know the direct public Internet facing system is vulnerable to MS08-067 and is Windows XP.

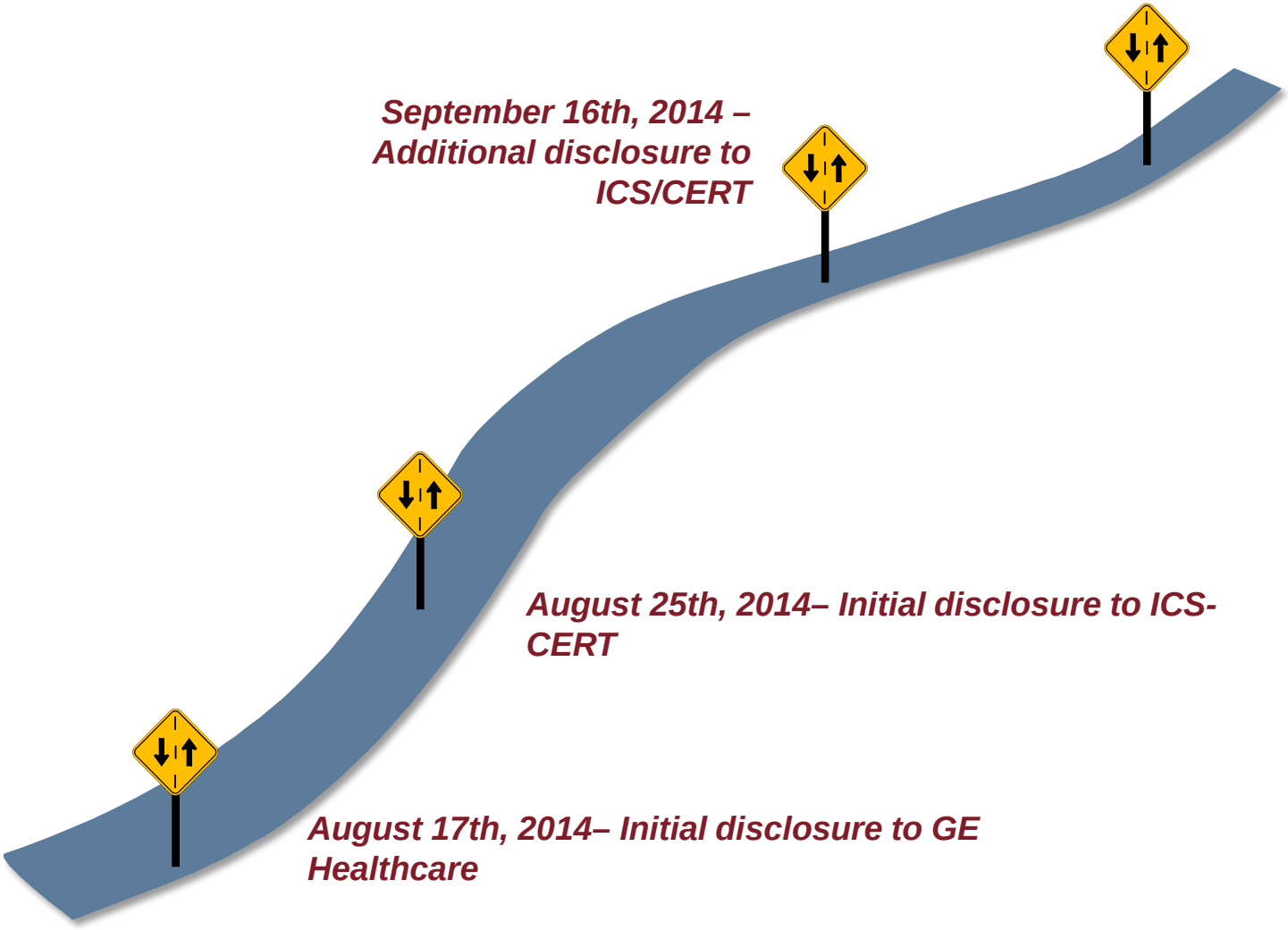
We know it is touching the backend networks because it is leaking all the systems it is connected to.



We can create a custom payload to pivot to only targeted medical devices and systems with known vulnerabilities.

Phase 3 Research: Admin Access

Disclosure Timeline



September 16th, 2014 – Additional disclosure to ICS/CERT

December 3rd, 2014 – Confirmation from ICS-CERT on completion of GE investigation and closing of issue.

August 25th, 2014– Initial disclosure to ICS-CERT

August 17th, 2014– Initial disclosure to GE Healthcare

NOTE: ALL INFORMATION DISCLOSED WAS PUBLICLY AVAILABLE ON GE HEALTHCARE'S WEBSITE.

CVE-2013-7404 CVSS = 10

GE Discovery NM750b – Nuclear Imaging

Manufacturer	*Model*	*Version*	*Type of Device*	*Type of Account*	*Login info*
GE	Discovery	NM 750b	Nuclear Imaging	Telnet- Root	UserID = "insite" Password = "2getin"
GE	Discovery	NM 750b	Nuclear Imaging	FTP- Admin	UserID = "insite" Password = "2getin"

CVE-2011-5374 CVSS = 10

CVE-2011-5374 GE Discovery NM670/NM630 - Nuclear Imaging/CT

Manufacturer	*Model*	*Version*	*Type of Device*	*Type of Account*	*Login info*
GE	Discovery	NM670	Nuclear Imaging/CT	SU Account	UserID = "su" Password = "install"
GE	Discovery	NM670	Nuclear Imaging/CT	Service Account	UserID = "service" Password = "#bigguy1"
GE	Discovery	NM670	Nuclear Imaging/CT	Root Account	UserID = "root" Password = "install"
GE	Discovery	NM630	Nuclear Imaging	SU Account	UserID = "su" Password = "install"
GE	Discovery	NM630	Nuclear Imaging/CT	Service Account	UserID = "service" Password = "#bigguy1"
GE	Discovery	NM630	Nuclear Imaging/CT	Root Account	UserID = "root" Password = "install"

GE Login Credentials Word Cloud

So If They Are Indeed Default Are There Still Issues

- Documentation instructs in some cases to not change credentials and not allow password reset.
- Documentation instructs in some cases to not change password or your account will not be able to be supported.
- Documentation not updated with how to change default credentials and secure configuration guides are lacking.
- Support personal often rely on implementation documentation so these logins are heavily utilized in the healthcare industry.

Examples

3. When the *User Properties* screen appears, verify/change the following parameters and click ***OK***.
   - ***User Must Change Password at Next Login***: Unchecked
   - ***User Cannot Change Password***: Checked
   - ***Password Never Expires***: Checked
   - ***Account Disabled***: Uncheck

3.3.2 Changing Passwords

You can change any of the account passwords with the following procedure.

Important

Do not change the InSite password. Remote access will be disabled for InSite support if the password is changed.

Examples

Table 3-8: Acquisition Passwords

Account User Name	Default Password
root	root.genie
service	service.
insite	insite.genieacq **(Do not change this password!)**
admin	admin.genie
reboot	reboot
shutdown	shutdown

Examples

Name	Password
MuseAdmin	Muse!Admin

NOTE: Tech Support will logon to the system with pcAnywhere using this user name and password.

Examples

Ask the remote station operator for your assigned username and password.

This resets the user's confirm password to **password**.

NOTE: To perform the following steps, you must generate X-ray radiation. Follow proper safety precautions with the X-ray system.

1. Turn on the digital system and login as service: (user: **serviceapp** password: **orion**)
2. When the service application starts, select the ***Calib*** function on the *Main Menu.*
3. Select ***System Manual*** *Tab.*
4. Select ***Overlay*** *Tab.*
5. You should now see a white circle in the image display (you may want to minimize the calibration window). Activate fluoro radiation; center the II output phosphor within the outline circle by moving the camera/lens assembly position on the image intensifier (II).

Honeypot Research: Are Attacks A Reality?

Real World Attacks

What we were looking for…

- Using known default login information for remote access?
- Leveraging existing exploits for remote command execution?
- Custom malware?
- Malicious intent to interfere with the device (or worse, someone using the device)?
- Campaigns against specific vendor devices?

Real World Attacks – The Data

Data	
Honeypots	*10*
Successful logins (SSH/Web):	*55,416*
Successful exploits (Majority is MS08-067)	*24*
Dropped malware samples	*299*
Top 3 Source Countries	*Netherlands, China, Korea*
HoneyCreds login	*8*

HoneyCred logins are unique to the honeypot ssh/web service, someone did some research.

Real World Attacks – Conclusion

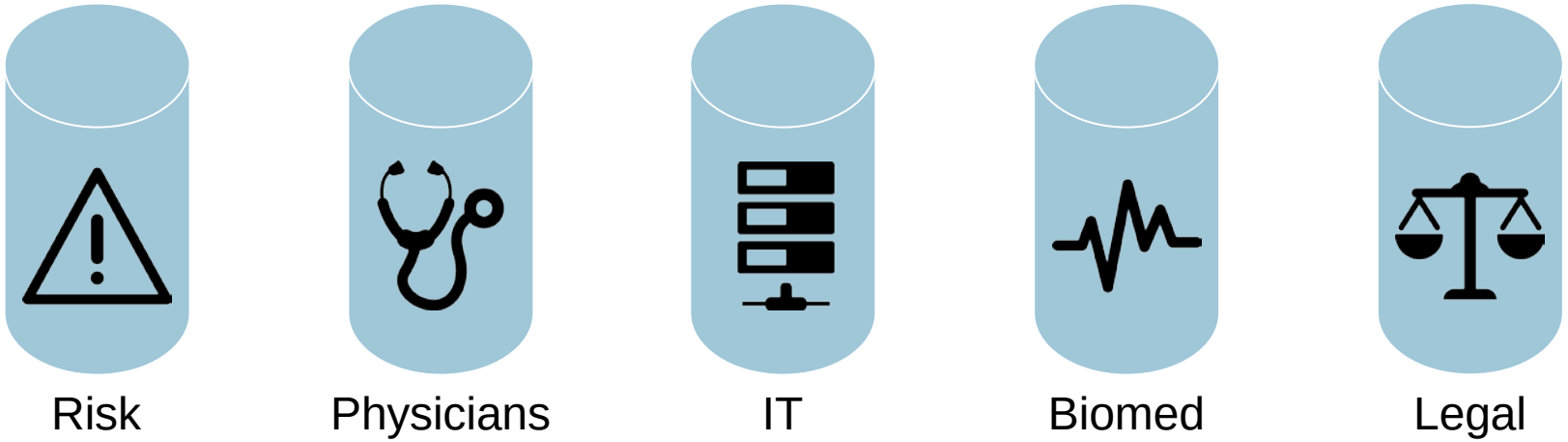
What did the attacker do once he got in?	*Nothing yet*
Did they realize they had root on a MRI machine?	*Probably not*
Are there owned medical devices calling back to a C2?	*Absolutely*
Do the C2 owners know what the information they are sitting on?	*Didn't appear so*

Problem Awareness

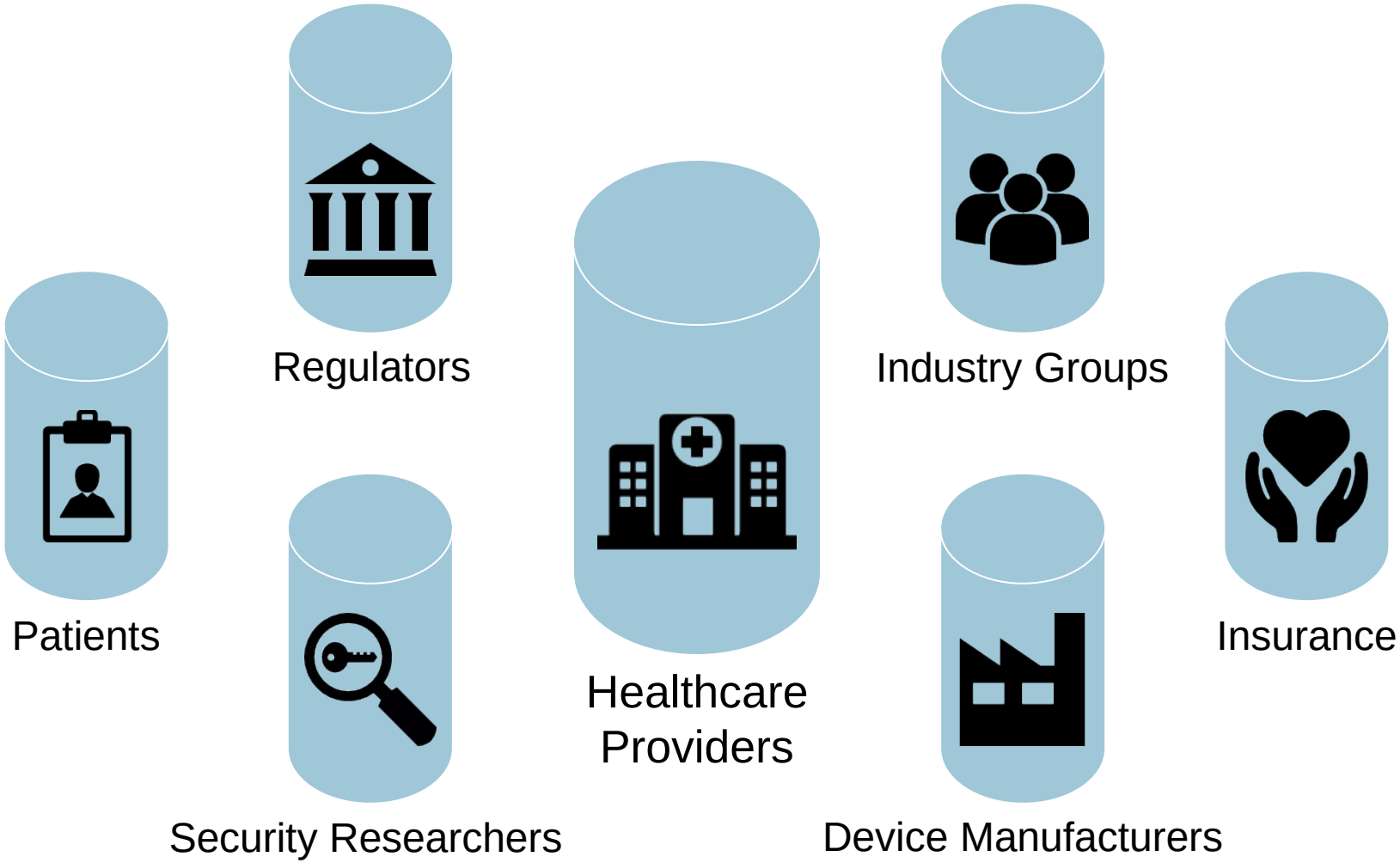
Problem Awareness

1. ***Medical devices*** *are* ***increasingly accessible*** *due to the nature of healthcare*
2. *HIPAA focuses on patient privacy, not* ***patient safety****.*
3. *FDA* ***does not*** *validate* ***cyber safety*** *controls.*
4. ***Malicious intent*** *is* ***not*** *a prerequisite for adverse patient outcomes.*

Isolation and Silos



Stakeholder Ecosystem



Treatment Plans

Treatment Plans

*It **falls to all of us. Patient safety** is not a **spectator sport.***

- **Stakeholders** must **understand** prerequisites
- **Multi-stakeholder** teams and conversations
- Engage with **willing allies** where domains of expertise overlap
- Incorporate **safety** into **existing processes**

A Better Way

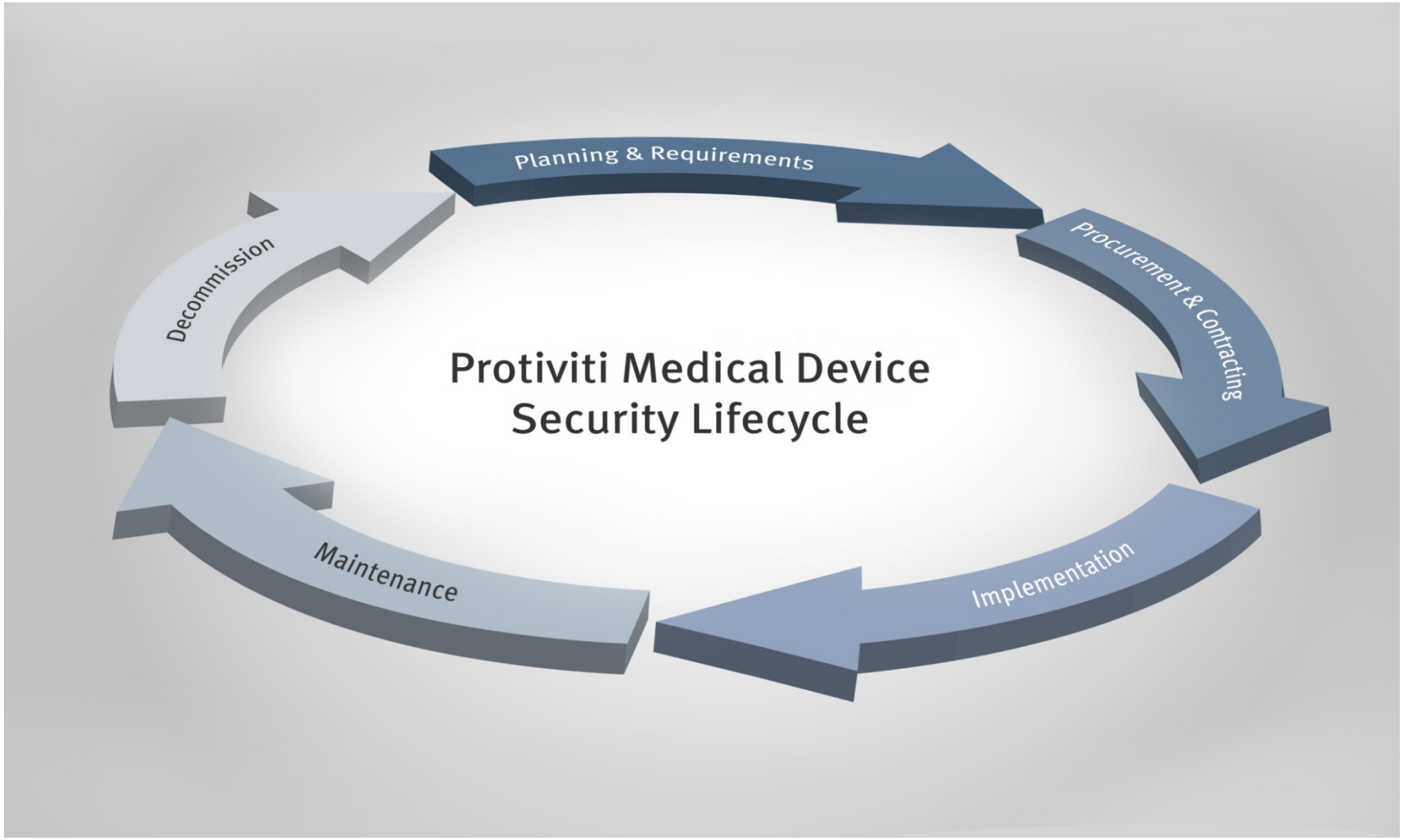
Summary of Recommended Treatment

- Patient safety as the overriding objective
- Avoid failed practices and iteratively evolve better ones
- Engage internal and external stakeholders
- Safety into existing practices and governance

Projected Outcomes

- “Reliable medical devices to market without undue delay or cost.”
- Collaboration among willing allies on common terms
- Medical devices resilient against accidents and adversaries

Medical Device Security Lifecycle



Medical Device Security Lifecycle: Addressing Risks

- **Planning & Requirements Phase**
  - Risk assessment, vulnerability assessment and threat modeling
  - Obtain Manufacturer Disclosure Statement for Medical Device Security (MDS2)
- **Procurement & Contracting Phase**
  - Risk reduction prior to procurement
  - Liability reduction for contracting
- **Implementation Phase**
  - Architecture and system design validation
  - Post implementation security validation
- **Maintenance Phase**
  - Vulnerability assessment and penetration testing
  - Liaison with manufacturers, federal agencies and working groups
- **Decommission Phase**

Where To Start – Two Approaches

- **Medical Device Security Risk Assessment**
  - Gap assessment to evaluate governance of medical device lifecycle
  - Most common starting point for organizations that accept the risk exposure of medical devices
- **Vulnerability Assessment & Penetration Testing**
  - Device specific assessment to identify current risk in medical devices
  - Initial approach for organization wanting to identify current risk
  - Most often utilized to assess maturity after initial risk assessment

Highlights From The Last 18 Months

- *FDA Premarket & Draft Postmarket Guidance and Workshops*
- *IEEE Building Code*
- *IATC Hippocratic Oath for Connected Medical Devices*
- *Coordinated Vulnerability Disclosure Policies*
- *FDA Safety Communications BEFORE evidence of harm*

Q&A

Scott Erven
Associate Director

protiviti®
Risk & Business Consulting.
Internal Audit.

Direct: (213) 327-1414
Mobile: (719) 332-6606
scott.erven@protiviti.com

Powerful Insights. Proven Delivery.®