# Top 3 Cyber Risk Reductions
## Your HTM Team Can Start Today

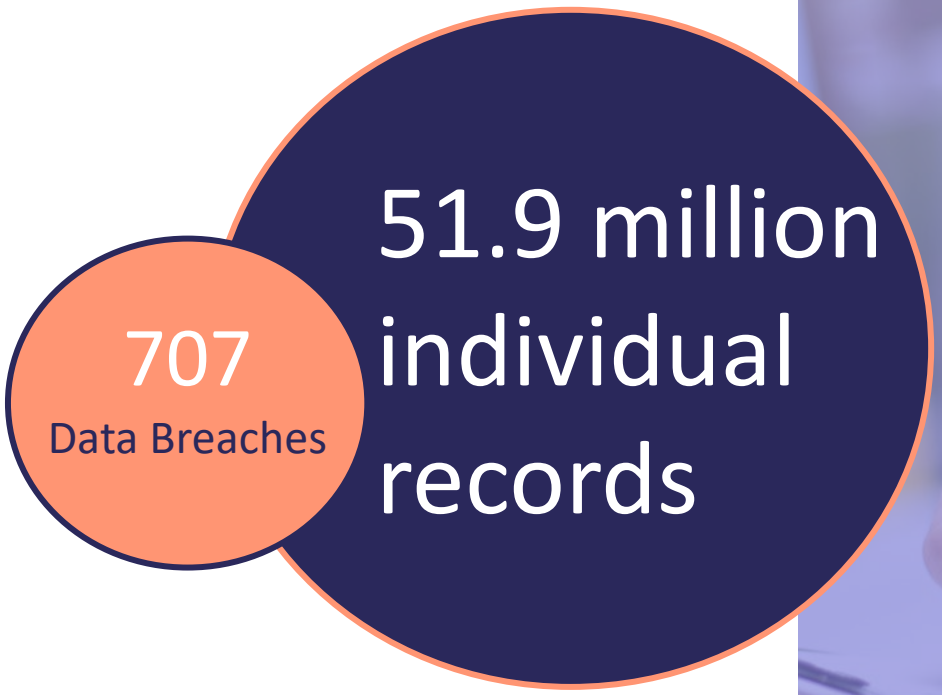
October 31, 2023

# Introductions

**Ryan Gonzalez**
Director, HTM Cybersecurity
Sodexo Healthcare

sodexo
HEALTHCARE

# How is healthcare impacted?




2022 Healthcare Statistics

Source: Healthcare Data Breach Statistics, HIPAA Journal, Feb. 2023

# Cybersecurity for Network Capable Medical Devices

## Biomed

- Patient Monitors
- IV Pumps
- Laboratory
- Ventilators
- Anesthesia Machines
- Defibrillators
- Cath Lab Physiological Monitoring
- EEG/EMG
- Etc.

## Imaging

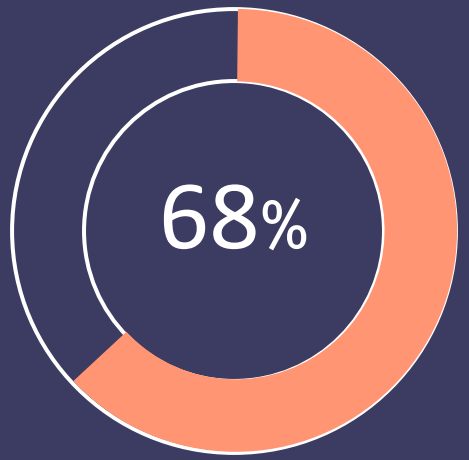
- CT Scanner
- MRI
- Fluoro (Cath Lab and ED)
- Ultrasound
- C-Arms
- Mammography
- Etc.

sodexo HEALTHCARE

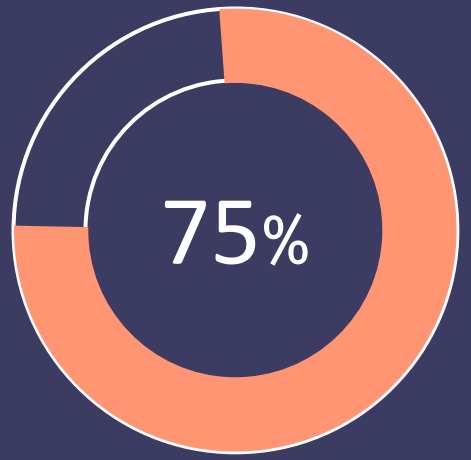
# How Ransomware Works


sodexo HEALTHCARE

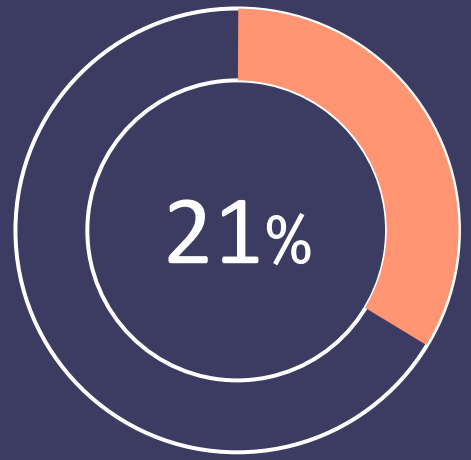
# Impact of Ransomware on Patient Care




Reported **longer** lengths of stay




Reported an increase in **patient transfers** or **facility diversions**



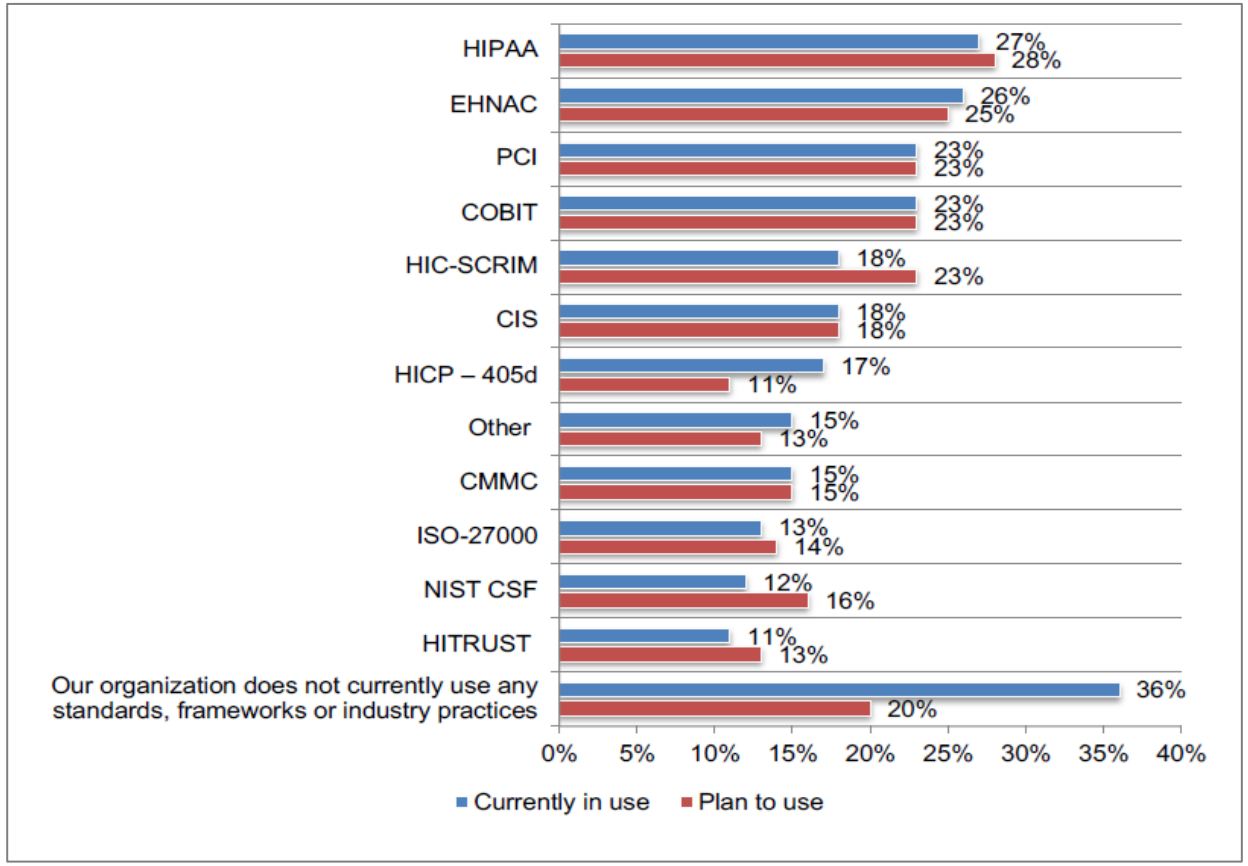

Reported an impact on **mortality** rates

Source: The Cost of a Data Breach Report 2022, IBM, Jul. 2022
Source: The Impact of Ransomware Patient Safety and the Value of Cybersecurity Benchmarking, Ponemon Institute, Jan. 2023

sodexo HEALTHCARE

# Frameworks and Resources

A survey of 579 IT and IT security professionals in healthcare delivery organizations (HDOs) on "What are the top standards, frameworks or industry practices currently used or plan to use as the basis for its cybersecurity program?"




Source: The Impact of Ransomware Patient Safety and the Value of Cybersecurity Benchmarking, Ponemon Institute, Jan. 2023

sodexo HEALTHCARE

# Other Problems We Face?

## The problem with HTM Programs

- HTM is historically underfunded and often does not have dedicated Cyber staff
- Pressured to support more equipment and more facilities with the same HTM staff
- Very tight project and inspection timelines combined with overwhelming PM lists

## Why Cybersecurity is hard

- Overwhelming number of cybersecurity standards and recommendations
- Visibility and availability of equipment is a challenge
- More vulnerabilities than time to manage
- Thousands of manufacturers and models that each have different cybersecurity capabilities and standards

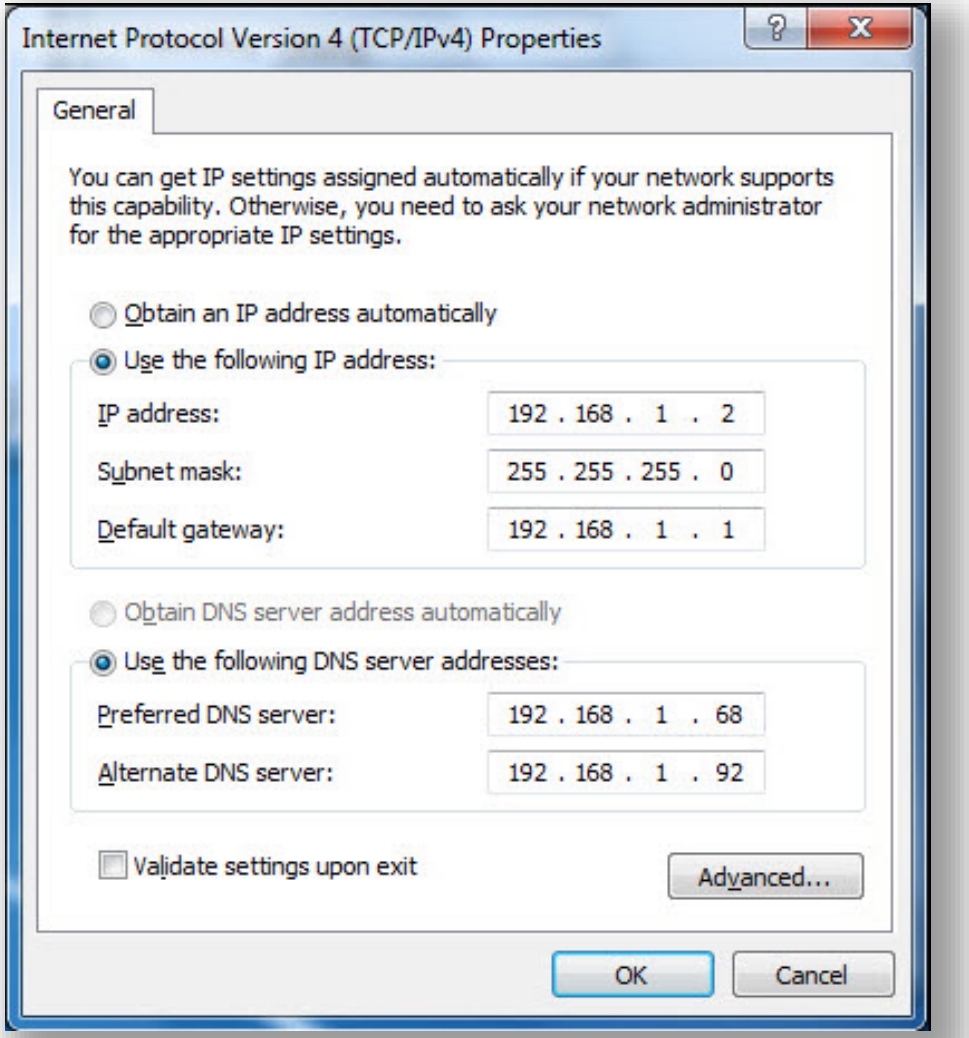
sodexo HEALTHCARE

# Where do we start?


sodexo HEALTHCARE

# 1 Identify Inventory network data elements

- Know what is in your environment
  - Network Capable?
- **Document all network data**




sodexo HEALTHCARE

# 1 Identify Inventory and Capabilities

- Patient data storage
- Network capabilities
- Password protection
- Data encryption
- Virus/Malware protection

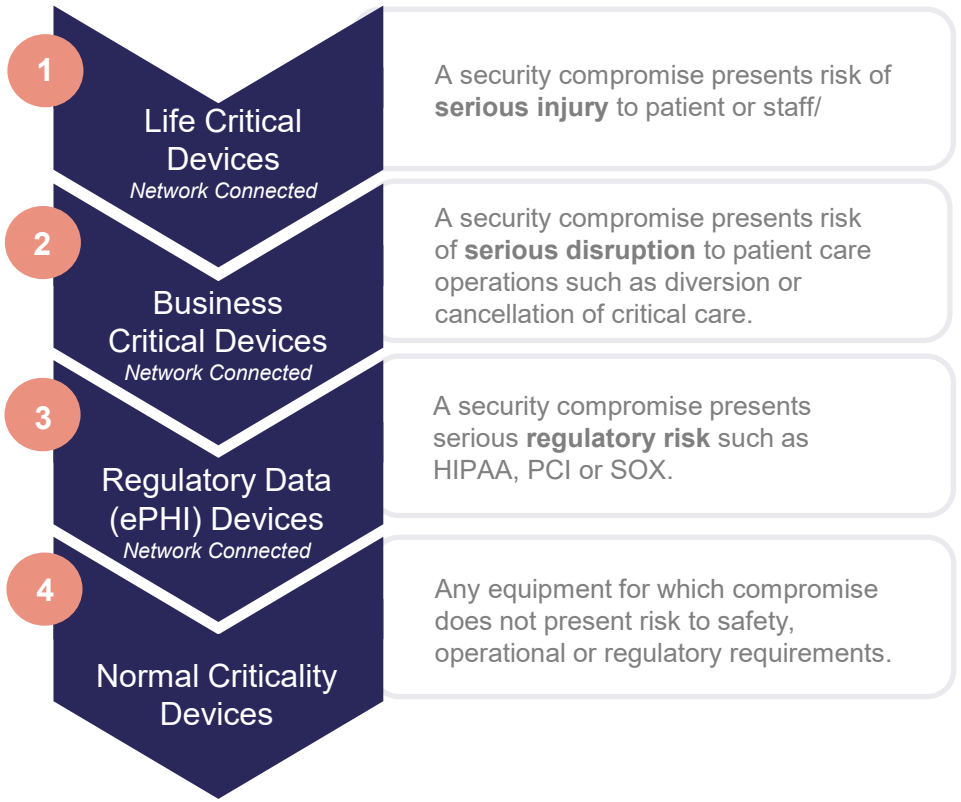
| Device Category | Manufacturer | Document ID | Document Release Date |
|---|---|---|---|
| 18360 Recorders, Electronic Storage, Data, Electrocardiography | GE Healthcare | DOC2002784 | JUN-2017 |
| **Device Model** | **Software Revision** | | **Software Release Date** |
| MAC 5500 | 9A, 9A.1, 9B, 9B.1, 9C, 9D | | 9/23/2013 (9D) |

| | Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form. | Yes, No, N/A, or See Note | Note # |
|---|---|---|---|
| **10** | **MALWARE DETECTION/PROTECTION (MLDP)** | | |
| | The ability of the **device** to effectively prevent, detect and remove malicious software (**malware**). | | |
| 10-1 | Does the **device** support the use of **anti-malware** software (or other **anti-malware** mechanism)? | No | — |
| | 10-1.1 Can the **user** independently re-configure **anti-malware** settings? | N/A | — |
| | 10-1.2 Does notification of **malware** detection occur in the **device user** interface? | N/A | — |
| | 10-1.3 Can only manufacturer-authorized persons repair systems when **malware** has been detected? | N/A | — |
| 10-2 | Can the device owner install or update **anti-virus software**? | No | |
| 10-3 | Can the device owner/**operator** (technically/physically) update virus definitions on manufacturer-installed **anti-virus software**? | No | — |
| MLDP notes: | | | |
| **11** | **NODE AUTHENTICATION (NAUT)** | | |
| | The ability of the **device** to authenticate communication partners/nodes. | | |
| 11-1 | Does the **device** provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information? | No | — |

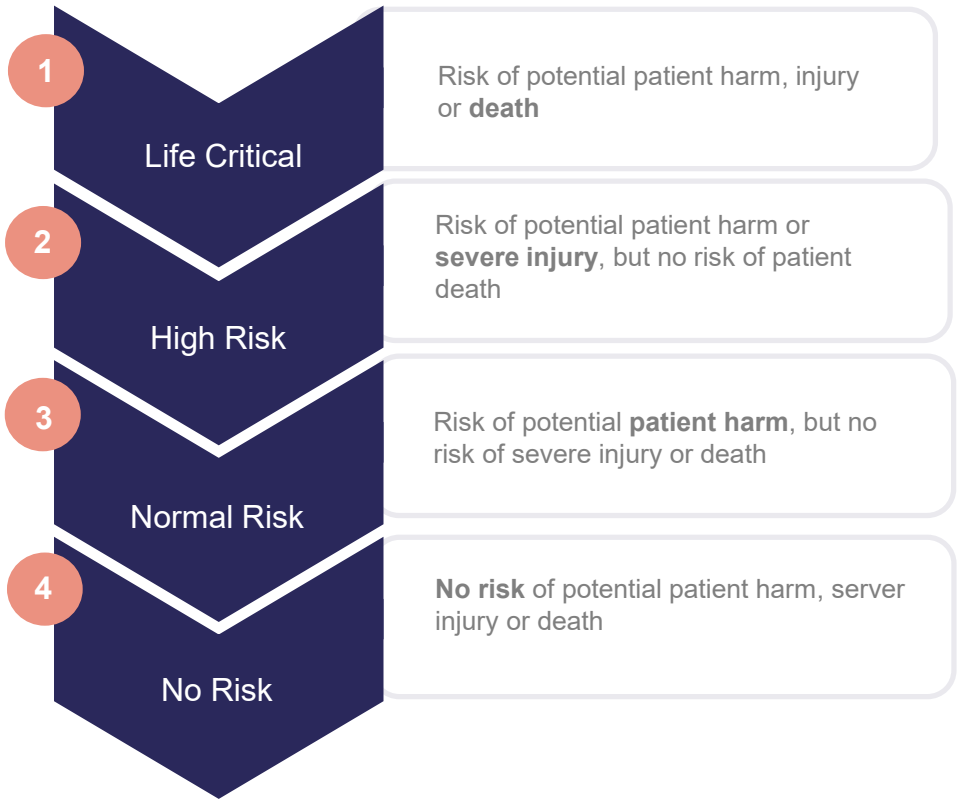
sodexo HEALTHCARE

# 2 Prioritization of Devices and Risks

## Business Criticality

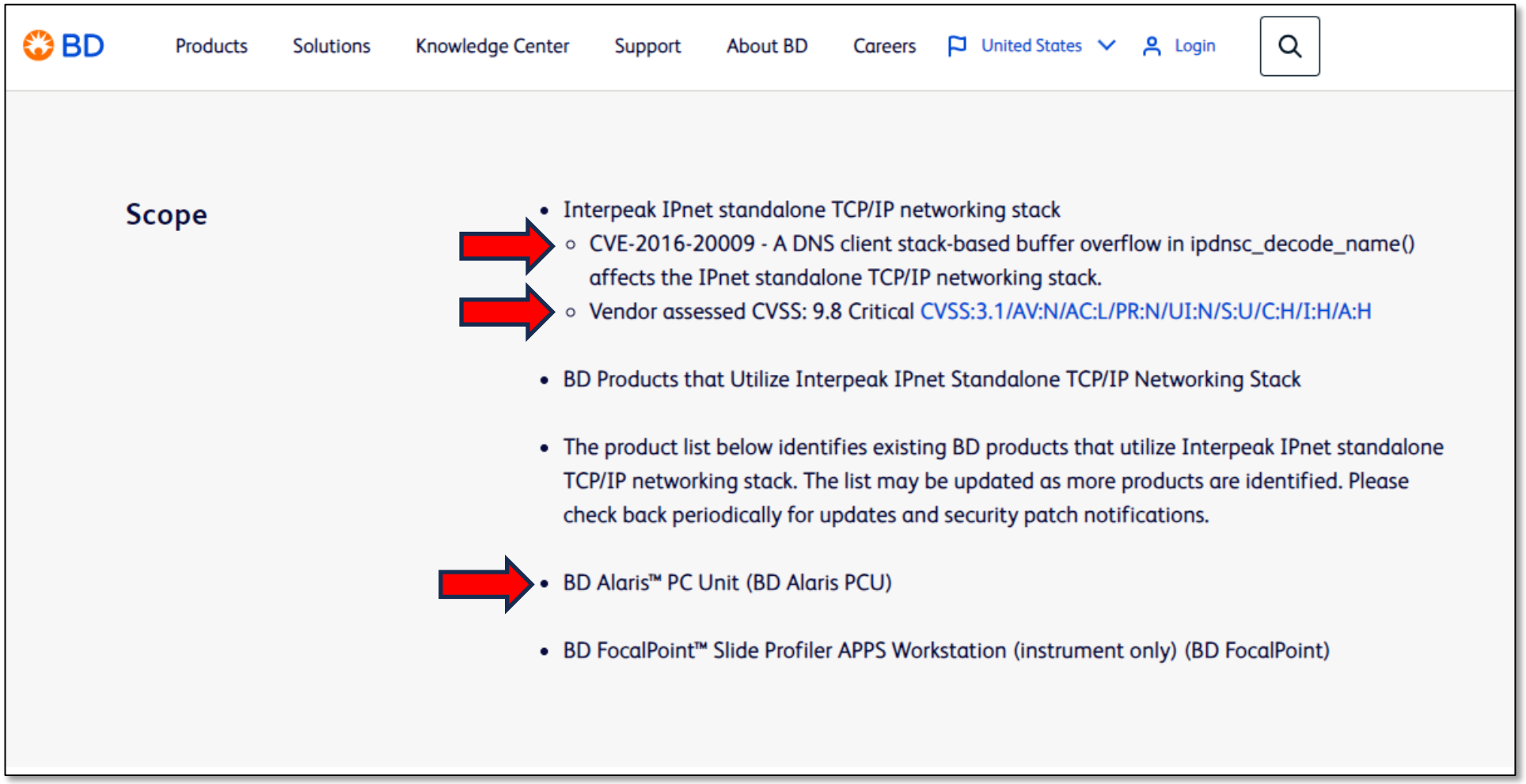



## Patient Safety




sodexo HEALTHCARE

# 2 Prioritization of Devices and Risks



BD Products Solutions Knowledge Center Support About BD Careers United States Login

**Scope**

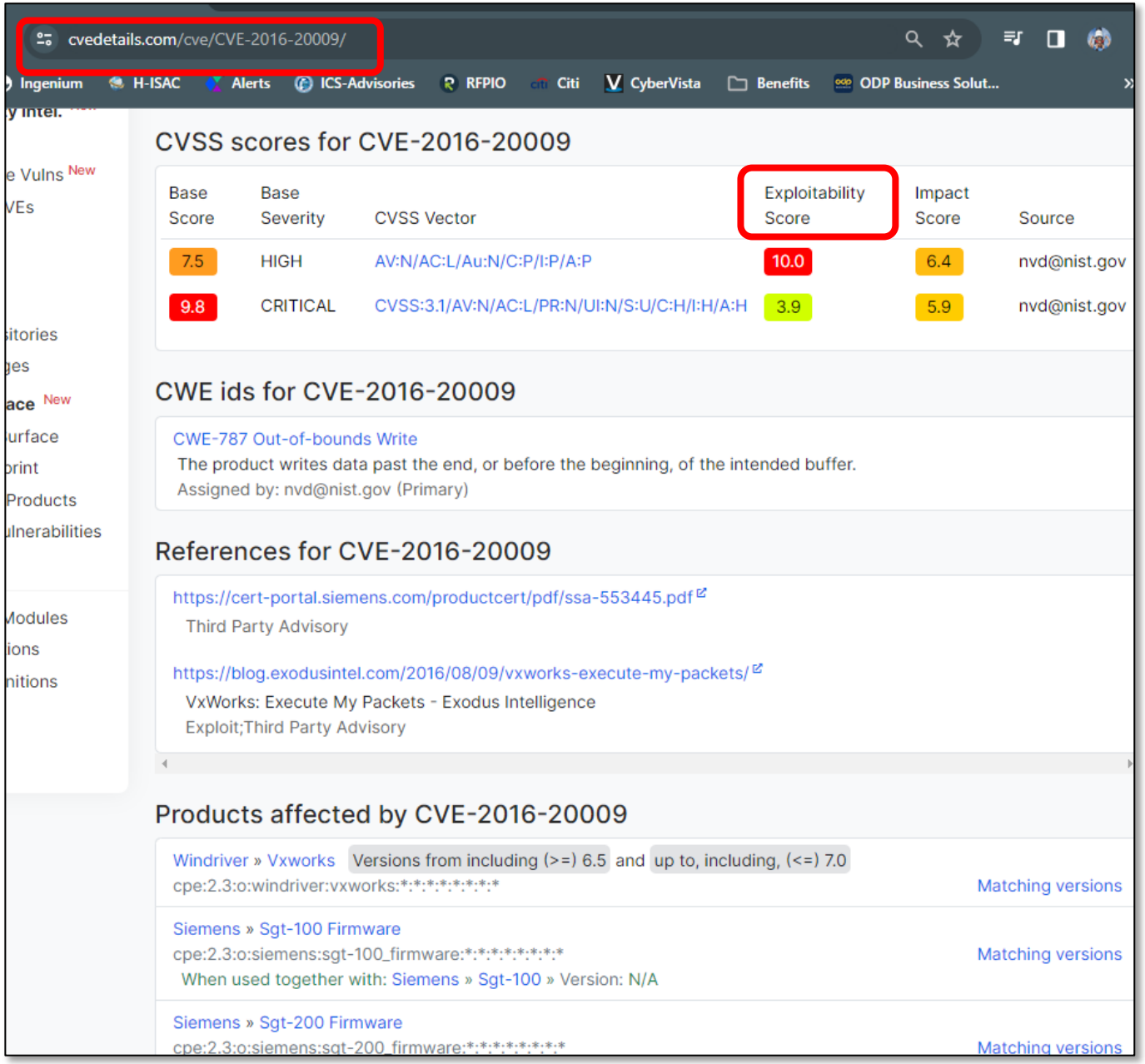
- Interpeak IPnet standalone TCP/IP networking stack
  - CVE-2016-20009 - A DNS client stack-based buffer overflow in ipdnsc_decode_name() affects the IPnet standalone TCP/IP networking stack.
  - Vendor assessed CVSS: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- BD Products that Utilize Interpeak IPnet Standalone TCP/IP Networking Stack
- The product list below identifies existing BD products that utilize Interpeak IPnet standalone TCP/IP networking stack. The list may be updated as more products are identified. Please check back periodically for updates and security patch notifications.
- BD Alaris™ PC Unit (BD Alaris PCU)
- BD FocalPoint™ Slide Profiler APPS Workstation (instrument only) (BD FocalPoint)

sodexo HEALTHCARE

2

# Prioritization of Devices and Risks

- www.cvedetails.com



# 2 Prioritization of Devices and Risks

## Common Vulnerability Scoring System

CVSS v3.0 Ratings

| | |
|---|---|
| Critical | 9.0-10.0 |
| High | 7.0-8.9 |
| Medium | 4.0-6.9 |
| Low | 0.1-3.9 |
| None | 0.0 |

## Exploit Prediction Scoring System

EPSS v2 Probabilities

| | |
|---|---|
| Critical | 75-100% |
| High | 50-74% |
| Medium | 20-49% |
| Low | 0.1-19% |
| None | 0.0% |

sodexo HEALTHCARE

3

# Operating System Patching

## OS Patching Windows devices

- What devices can have patches auto update?
- What devices can have patches pushed remotely?

| | | | |
|---|---|---|---|
| 5 | **CYBER SECURITY PRODUCT UPGRADES (CSUP)**<br>The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade **device**'s security patches. | | |
| 5-1 | Can relevant OS and **device** security patches be applied to the **device** as they become available? | Yes | 1 |
| | 5-1.1 Can security patches or other software be installed remotely? | Yes | 2 |

| | |
|---|---|
| Device Operating System (OS) | Windows 7 Professional 32 or 64 bit |
| Can the OS be automatically patched? | ☑ Yes ☐ No |
| ***Note that systems that do not support automated patching via the VHA MD Update Server or via vendor channels impose a significantly higher risk to the VA network.* | |
| If patching is not automated, what is the patching process and/or limitations? | Please see GeneXpert Security Guidelines |

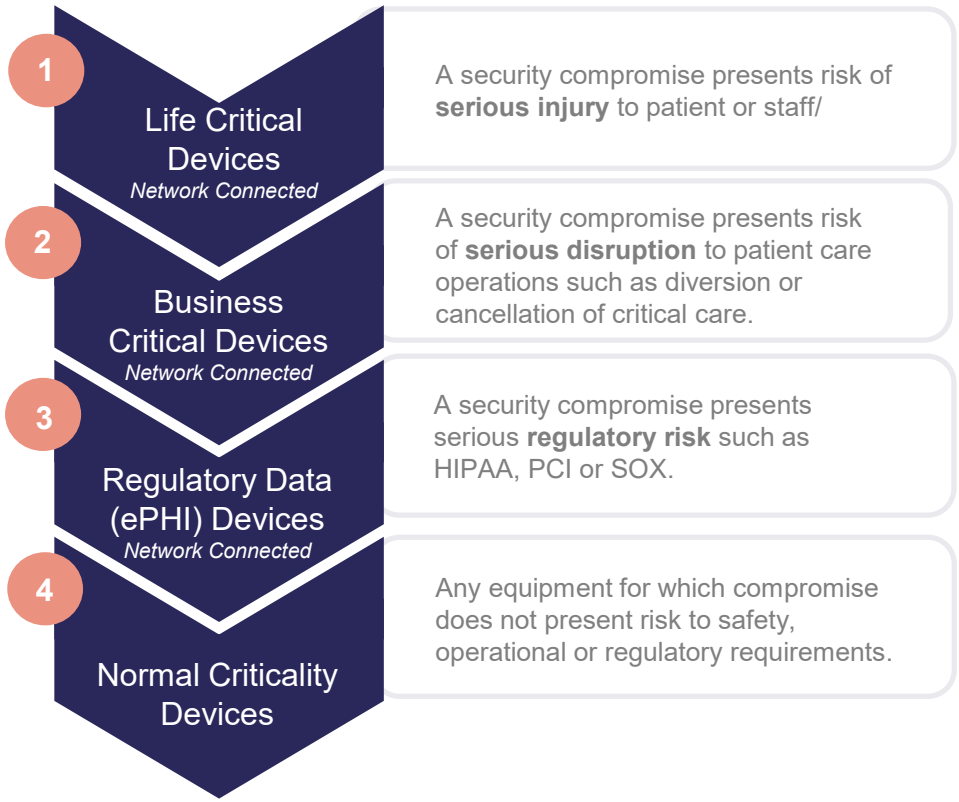
sodexo HEALTHCARE

# 3 Prioritization of Devices for Patching

## Include Patching in Other Services

- Does your existing contract include patching?
- Can patching be added to time and material devices a vendor maintains?
- Can patching be added to in house PM's?

## Business Criticality




sodexo HEALTHCARE

# Summary

1

## Identify and Inventory Capabilities

- Document network data
- Explore cyber capabilities

2

## Prioritization of Devices and Risks

- Balance Business Criticality with Patient Risks
- Understand how to read and prioritize vulnerabilities

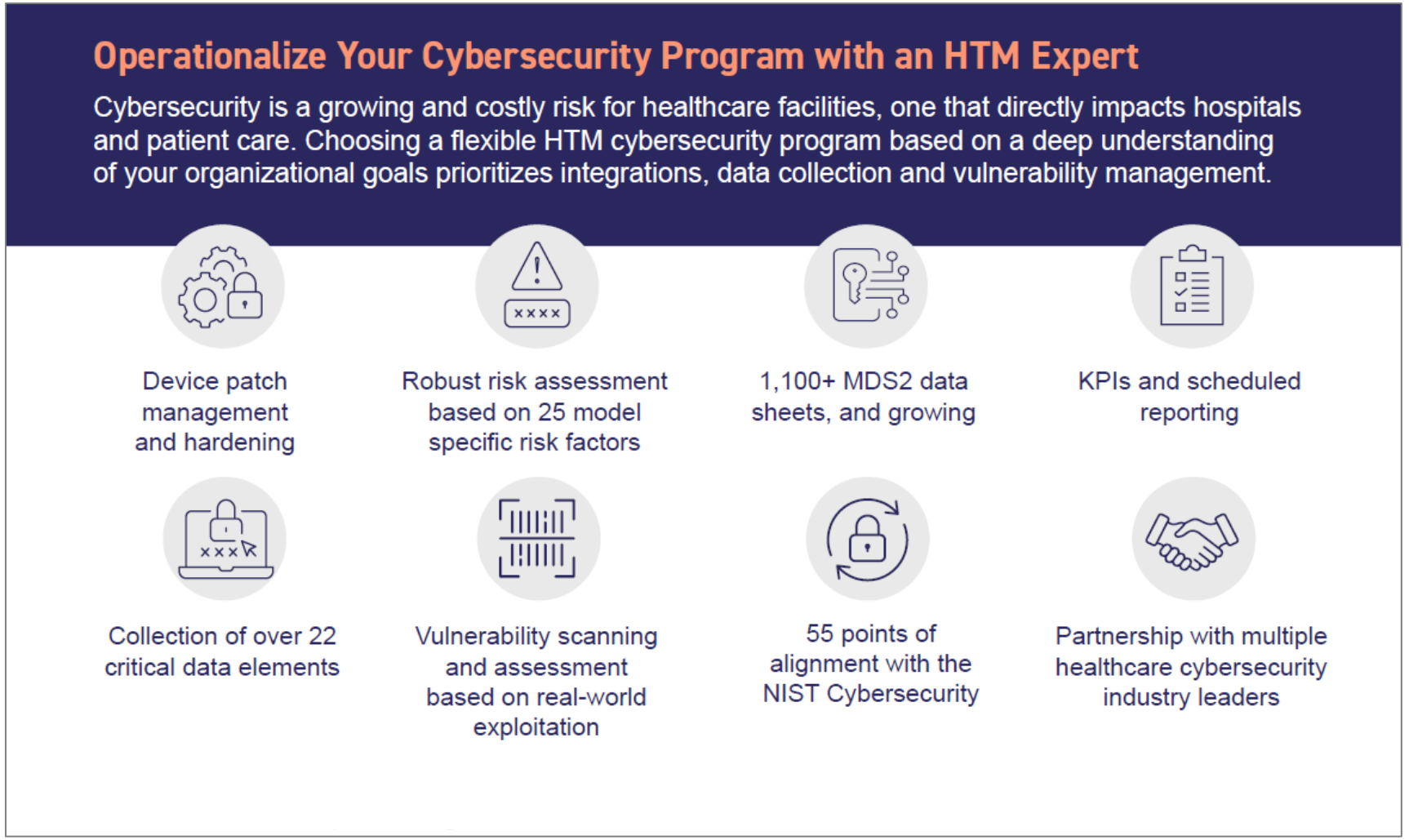
3

## Operating System Patching

- Automate patching when safe and able
- Optimize patching efforts with clear guidance
- Include patching in existing services

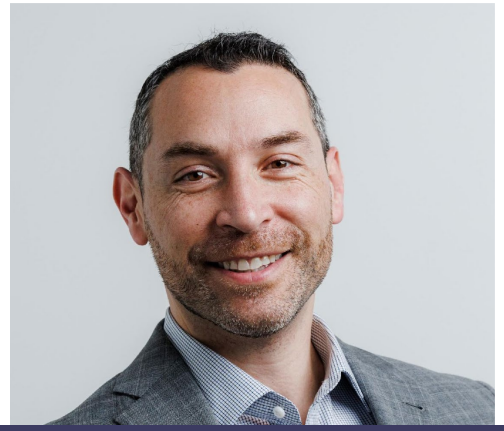
sodexo HEALTHCARE

# Sodexo HTM Cybersecurity Overview




sodexo HEALTHCARE

# Questions?



**Ryan Gonzalez**
Director, HTM Cybersecurity
Sodexo Healthcare

ryan.gonzalez@sodexo.com

Please scan QR code
to submit a survey
for this session.

**Thank You!**