ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Health-ISAC®
SHARING SINCE 2010
Collaborating for Resilience in Health

Health-ISAC Current and Emerging Healthcare Cyber Threat Landscape

October 7, 2026

Presenters

Taylor Porter and Phil Englert

About the host/moderator

Peter H. Dziedzic, MS
Engineer
Assistant Professor
Neurology and Neurocritical Care
Johns Hopkins University, School of Medicine

ACCE Education Committee member

ACCE gratefully acknowledges the sponsorship of this webinar by

Logistics

❖All attendees have their microphones muted during the presentation.

❖Questions to the panelists must be submitted via the "Q&A" feature in Zoom at any time. They will be addressed at the Q&A portion.

❖If there is any urgent issue, please use the "chat" feature to communicate with the host/moderator.

About the Speaker

Taylor Porter
Medical Device Security Analyst

Health-ISAC
Collaborating for Resilience in Health

Taylor Porter is a Medical Device Analyst at Health-ISAC. Taylor acts as the Health-ISAC liaison for the Medical Device Security Council.

Through the Health-ISAC community, Taylor connects medical device manufacturers and healthcare delivery organizations in a unique forum to collaborate on security issues and share information. She has spearheaded the distribution of medical device advisories released to member healthcare delivery organizations to increase awareness of potential vulnerabilities impacting devices.

About the Speaker

Phil Englert
VP Medical Device Security

Health-ISAC
Collaborating for Resilience in Health

As VP of Medical Device Security for Health-ISAC, I work with Medical Device Manufacturers (MDMs) to help improve privacy and security while coordinating with Health Delivery Organizations (HDOs) to ensure practical implementations are achievable.

An experienced leader in strategy and tactics development for a $450m biomedical services organization supporting over 130 Acute Care facilities across 22 states with deep knowledge of clinical settings and extensive knowledge of medical technologies.

Regulatory and standards efforts include HSCC, MITA, NTIA, CISA, AAMI, MDIC, Underwriters Laboratories, and MITRE.
Chief Product Officer at MedSec
Global Leader for Medical Device Security at Deloitte
Vice President of Operations at MDISS
National Director, Technology Operations at Catholic Health Initiatives

Session description

In 2024, healthcare systems worldwide faced significant cybersecurity challenges. The Health-ISAC Current and Emerging Healthcare Cyber Threat Landscape for 2025 reveals that cyberattacks targeting the healthcare sector are expected to escalate further. Health-ISAC is proud to partner with ACCE to collect an inclusive view of the threat landscape. Key findings include a surge in ransomware attacks, with increasingly sophisticated techniques employed by threat actors. Notably, the rise of the Internet of Medical Things (IoMT) devices has introduced new vulnerabilities, making medical devices a prime target for cyber threats.

Healthcare Technology Management staff play a crucial role in safeguarding IoMT devices and ensuring the resilience of healthcare organizations globally. This discussion highlights threats to patient safety and data privacy facing your organization. Awareness is the first step toward building a more resilient environment. Walk away with actionable insights you can use tomorrow.

Current and Emerging Threats in the Health Sector 2025-2026

What is an ISAC?

- ISAC is short for “Information Sharing and Analysis Center”
- ISACs empower **sharing and collaboration** in critical infrastructure communities to prevent, detect and respond to cybersecurity and physical security events
- ISACs collect, analyze, and disseminate actionable **threat information** to their members and provide them with **tools** to mitigate risks and enhance resiliency

About Health-ISAC

- Community of 15,000+ Global Security Analysts, built on **trust** and **anonymity**
- Members must be in the health sector and interested in providing value to the overall Health-ISAC eco-system by listening, sharing, and/or contributing
- Benefits

Community

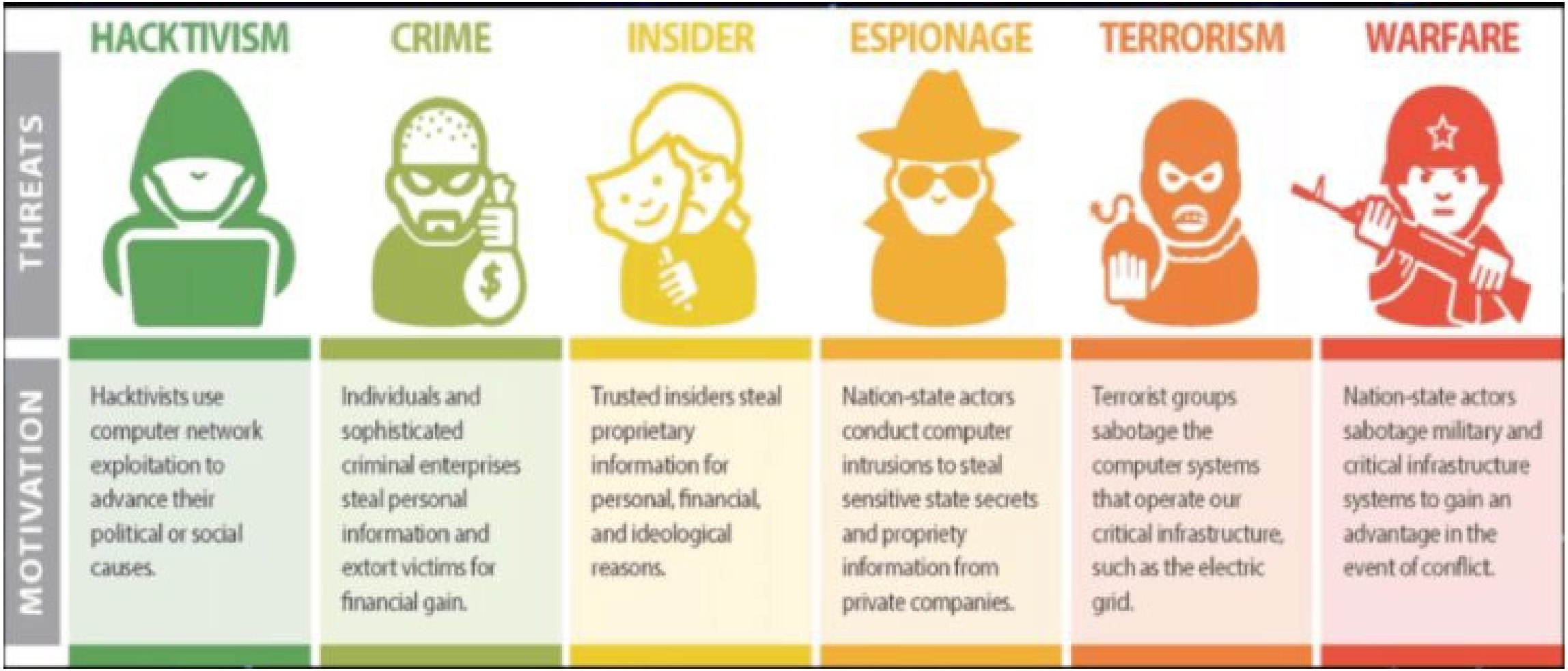
Events and Education

Threat Intelligence

Community Services

Cybersecurity Automation

The Cyber Threat Spectrum

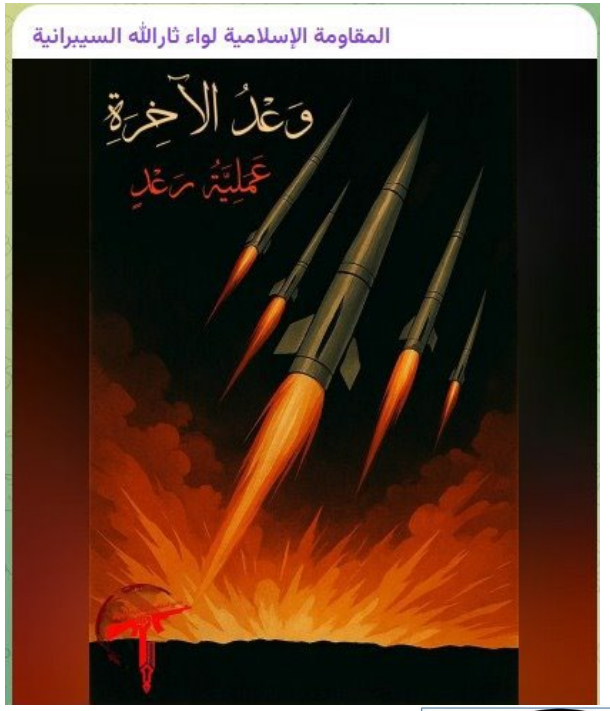


Agenda

- Current Threat Landscape
- Notable Tactics
- Business Resilience
- Annual Threat Survey Results

Current Threat Landscape

Middle East Conflict



- Threat actors targeting health sector organizations:
  - Distributed Denial of Service (DDoS) attacks
  - Data wiping attacks
  - Leaking internal CCTV camera feeds

- Nation state threat actors targeting Programmable Logic Controllers (PLCs) in Operational Technology (OT) environments.

Significant Takedowns

- **RaccoonO365**
  - The Raccoon O365 phishing-as-a-service kit stole credentials and login tokens, becoming a fast-growing tool targeting thousands of organizations globally.
  - A collaboration between Microsoft's DCU and Health-ISAC successfully took down Raccoon O365, seizing 338 websites used in the criminal operation.

- **Tycoon 2FA**
  - Health-ISAC provided critical data confirming that over 100 members were successfully phished, illustrating the massive scale of the threat to healthcare.
  - Health-ISAC identified how the attacks caused tangible harm to healthcare operations, including the disruption of patient care and the diversion of essential medical resources.

Ransomware Groups Attacking Healthcare

Health-ISAC tracked 455 ransomware events in the health sector during 2025. The following profiles correspond to the five most active ransomware gangs observed with the highest number of victims.

Ransomware Gangs	***Number of Health Sector Entities Attacked***
Qilin	77
INC Ransom	50
SAFEPAY	23
Sinobi	21
World Leaks	18

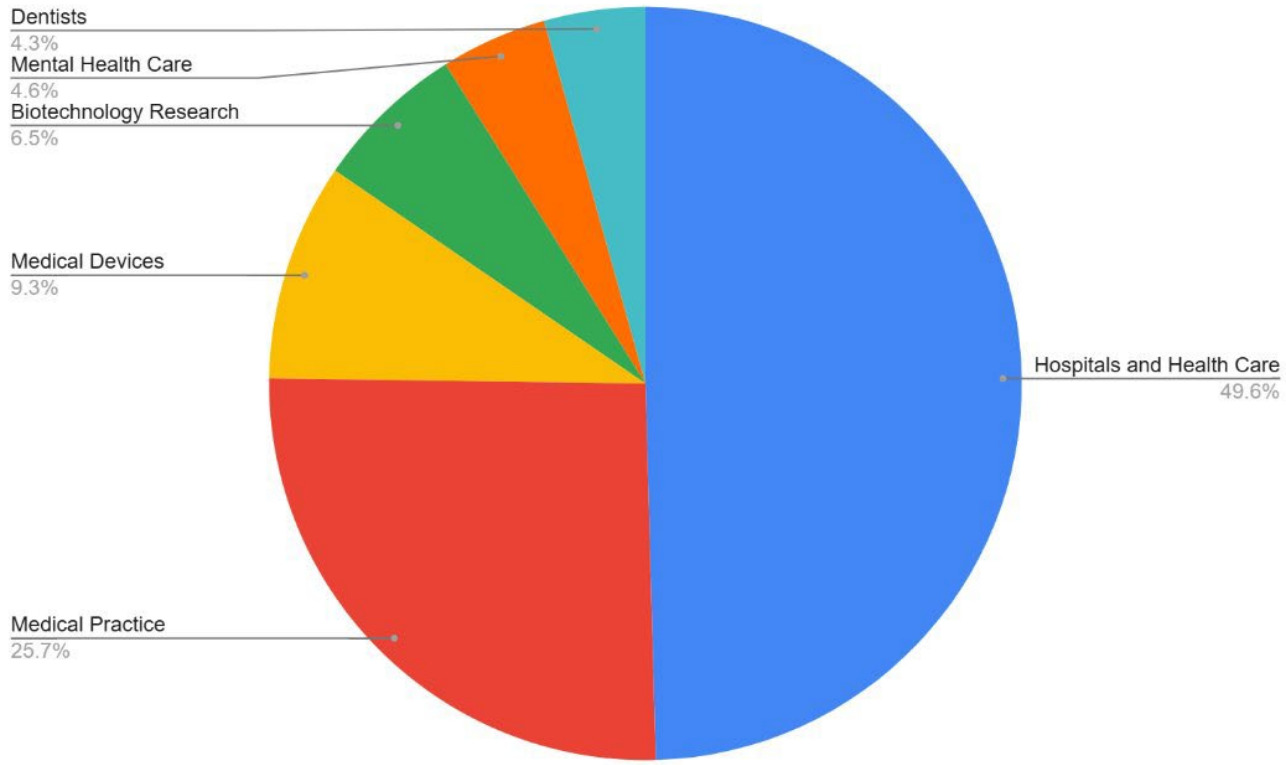
Ransomware Trends: Emerging and Receding Groups

This table represents which groups showed an increase or decrease in health sector victims going from 2024 to 2025:

Actor	2024 Victims	2025 Victims	2024 vs 2025 Difference	Percent Change (2024 to 2025)	Trend
SAFEPAY	3	23	20	666.67%	increasing
Qilin	23	77	54	234.78%	increasing
INC Ransom	39	50	11	28.21%	increasing
Rhysida	12	15	3	25.00%	increasing
Medusa	15	17	2	13.33%	increasing
Kill Security	14	11	-3	-21.43%	decreasing
RansomHub	36	18	-18	-50.00%	decreasing
Everest	19	9	-10	-52.63%	decreasing
BianLian	29	7	-22	-75.86%	decreasing
LockBit 3.0	39	0	-39	-100.00%	decreasing

Ransomware Trends: Victimology

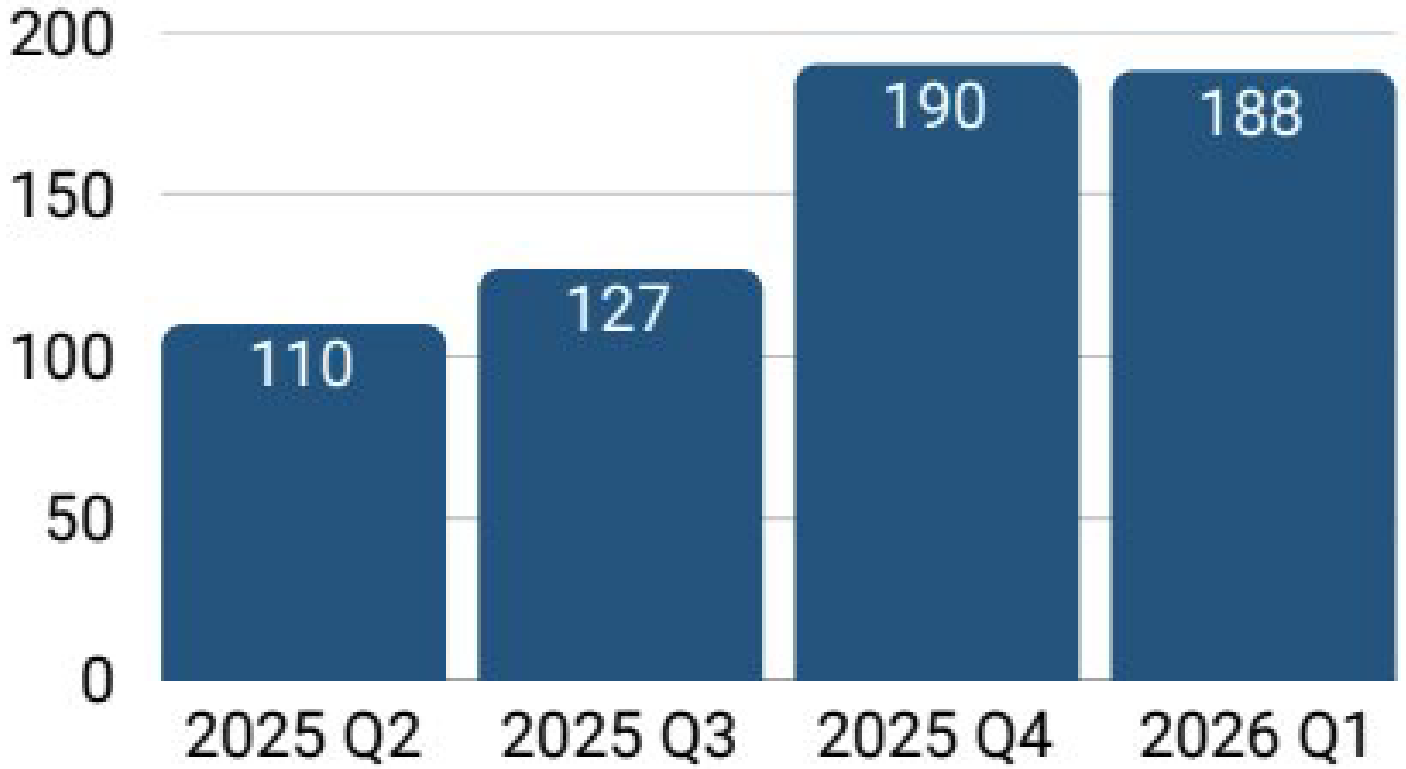
This chart shows the distribution of health subsectors in the Health-ISAC ransomware incident database.



Hospitals and Health Care	49.6%
Medical Practice	25.7%
Medical Devices	9.3%
Biotechnology Research	6.5%
Mental Health Care	4.6%
Dentists	4.3%

Ransomware Growth Against Health Sector

- Q1 2026 has nearly the same number of attacks as the Q4 2025.
- 30 more than 2025 Q1



Nation-State Threats

- **DPRK IT Fraud:** North Korean operatives are infiltrating the global health sector by posing as remote IT workers to fund weapons programs, disrupting talent acquisition and security.
- **Israel-Iran Conflict:** The 2025 war triggered hacktivist attacks against Israeli healthcare infrastructure, including DDoS attacks and one-way ransomware attacks that prioritize data destruction.
- **Hybrid Warfare Tactics:** Health-ISAC research highlights a rise in nation-states utilizing "gray zone" tactics, specifically leveraging cybercriminal proxies to attack geopolitical rivals while maintaining plausible deniability.

Mythos Strategic Concerns

- **Unprecedented Capabilities:** Autonomous discovery and exploitation of zero-day vulnerabilities.
- **Security Risk:** High risk of misuse, similar to dual-use penetration tools.
- **Global Proliferation:** Expected to be replicated by Chinese firms within 6–12 months.
- **Broad Distribution:** Likely to spread widely via unregulated or open-source releases by late 2026.

Medical Device Security

- **CMS8000 Patient Monitor:** CISA and the FDA warned that Contec CMS8000 monitors contain severe insecure design flaws, including hard-coded IP addresses and remote access risks.

- **Legacy System Risks:** The 2025 expiration of Windows 10 support has exacerbated the legacy device crisis, requiring healthcare providers to implement compensating controls.

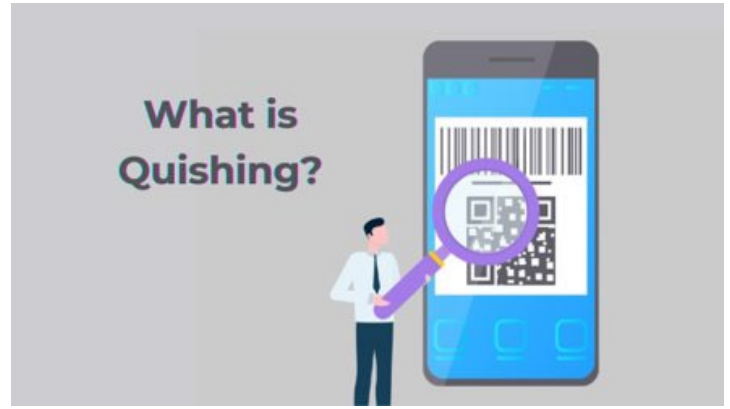
- **Imaging Infrastructure Exposure:** Health-ISAC continued to observed PACS/DICOM exposures in 2025.

- **AI in Medical Devices:** 200+ medical devices with AI features approved by the FDA.

Notable Tactics and Techniques

Social Engineering Evolution

- **ClickFix and FileFix**: Malicious sites trick users into executing malicious code by mimicking system errors
- **QR Code Risks:** Quishing exploits trusted healthcare QR codes to direct mobile users to malicious sites
- **Cleo Victim Bundling:** Ransomware victim bundling on DLS sites caused additional third party risk concerns to emerge



Malicious Activity Observed by Members

The member shared indicators of compromise have been analyzed to produce the Top 5 malicious activities observed by members.

Top 5 Observables:

1. **XWorm:** This commodity remote access trojan can harvest sensitive data, exfiltrate files, and hijack social media accounts from infected systems.
2. **NetSupportRAT:** This malware masquerades as a legitimate remote management tool to provide threat actors with stealthy, unauthorized access to a victim's personal data.
3. **njRAT:** Operating since 2013, this .NET-based trojan allows even inexperienced criminals to remotely control computers, capture webcam feeds, and steal credentials.
4. **SocGholish:** First observed in 2017, this malware loader typically gains initial access through drive-by compromises by masquerading as legitimate software updates.
5. **AsyncRAT:** Designed for Windows systems, this trojan establishes connections with external command and control servers to steal user credentials and deploy additional malicious software.

Malicious TTPs Observed by Members

The member shared indicators of compromise have been analyzed to produce the Top 5 MITRE ATT&CK Techniques observed by members.

Top 5 Techniques:

1. **T1059.001 -** Command and Scripting Interpreter: PowerShell
2. **T1189 -** Drive-by Compromise
3. **T1204.004 -** User Execution – Malicious Copy & Paste
4. **T1566.002 -** Spearphishing Link
5. **T1219 -** Remote Access Tools

Notable Vulnerabilities

- **Microsoft SharePoint ToolShell (CVE-2025-53770)**
  - Critical RCE vulnerability (CVSS 9.8) disclosed July 19, 2025, for on-premises Microsoft SharePoint Servers.
  - Allows unauthenticated attackers to execute arbitrary code and exfiltrate sensitive data.
- **Cisco ASA 5500-X Series (CVE-2025-53770)**
  - Critical vulnerabilities in Cisco ASA 5500-X and FTD devices reported on September 29, 2025, with active exploitation.
  - Exploitation possible by remote, unauthenticated attackers with low privileges to execute code or access restricted endpoints.

High Frequency Targeted Alerts

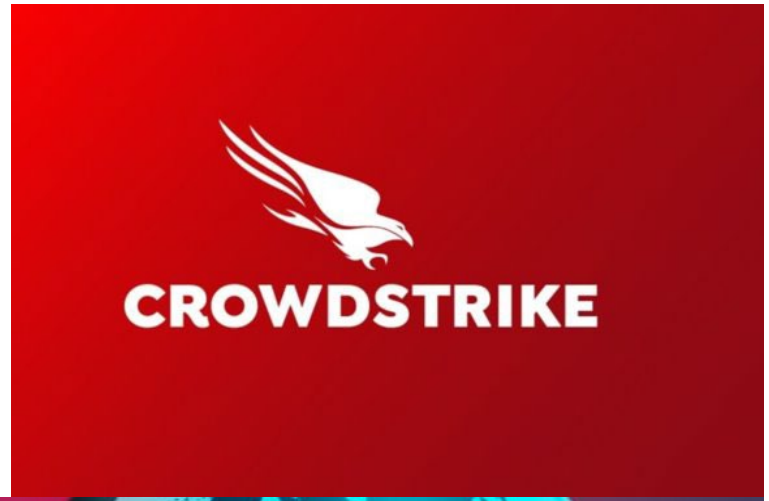
The following are the top five most frequently sent targeted alerts in 2025:

1. **Dangling DNS:** Health-ISAC issued 407 targeted alerts to organizations with obsolete, unused DNS records that pose significant cybersecurity risks if not removed.
2. **Citrix NetScaler (CVE-2025-7775, CVE-2025-7776, CVE-2025-8424):** 98 alerts warned of critical vulnerabilities in Citrix NetScaler appliances.
3. **BeyondTrust (CVE-2024-12686, CVE-2024-12356):** 77 alerts were sent after December 2024 exploitation exposed sensitive customer data in BeyondTrust Remote Support
4. **CEO Doxxing:** 54 alerts notified organizations with executives listed on a publicly available CEO doxxing website that aggregated personal and professional data
5. **Remote Desktop Protocol (RDP):** 41 alerts addressed the critical risk of internet-exposed RDP ports .

Business Resilience

Crowdstrike Outage

- The CrowdStrike incident exposed substantial supply chain risks in healthcare critical infrastructure, impacting operational stability.
- Research shows 750 US hospitals experienced disruptions, with over 20% affecting patient care and direct losses totaling $1.94 billion.
- Shows the importance of identifying single points of failure in digital supply chains.



Business Resilience in 2026

- Health sector threats in 2026 include supply chain issues, financial strains, and governance risks related to AI and emerging technologies.
- Rapid AI and digital health tech deployment introduces risks like algorithmic bias, misdiagnoses, and unreliable AI-driven equipment.
- Improper AI governance and validation pose significant patient safety and liability concerns.
- Health leaders must strategically adapt and plan resilience efforts to manage evolving technology risks in healthcare workflows.

Recommendations & Free Resources

Health-ISAC – www.health-isac.org

- Annual Threat Report - https://health-isac.org/health-isac-2025-health-sector-cyber-threat-landscape/
- Health-ISAC Community Services Free Offerings - https://h-isac.org/community-services-2?_sft_category=free-tools
- Information on DDoS, including mitigation strategies - https://h-isac.org/distributed-denial-of-service-ddos-attacks/
- AHA & Health-ISAC / Preparing for the Next “SolarWinds” Event - https://h-isac.org/preparing-for-the-next-solarwinds-event-2/

Health Sector Cybersecurity Coordination Center (HC3) - https://www.hhs.gov/about/agencies/asa/ocio/hc3

HHS 405(d) Aligning Health Care Industry Security Approaches - https://405d.hhs.gov/

HHS Office of the Assistant Secretary for Preparedness and Response (ASPR) - aspr.hhs.gov

Annual Threat Survey

Survey Findings

Survey Purpose: The purpose of the survey is to gather confidential insight on the most significant security and cyber threats affecting the health sector in 2025 and those anticipated in 2026 from across the health sector community.

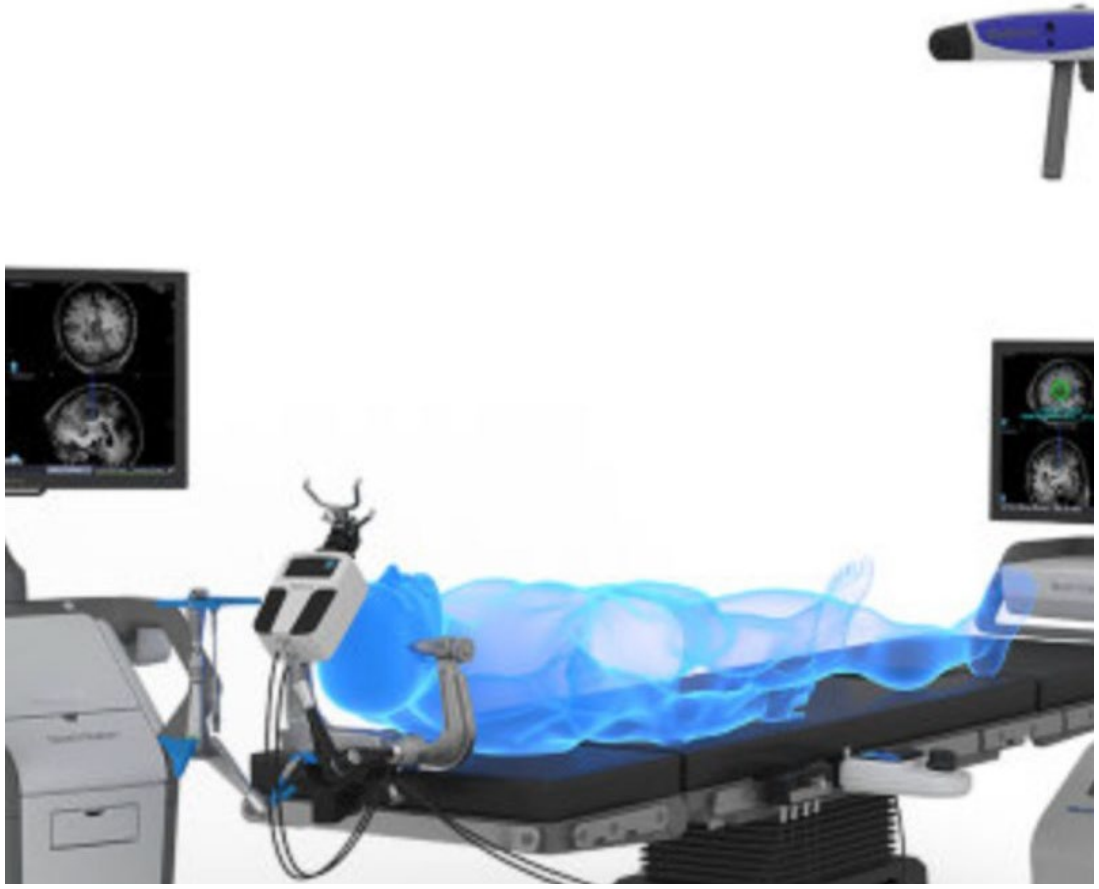
Survey Dates: 9/25 – 12/07/2025

Participant organizations: Health-ISAC, HSCC, AAMI, ACCE,

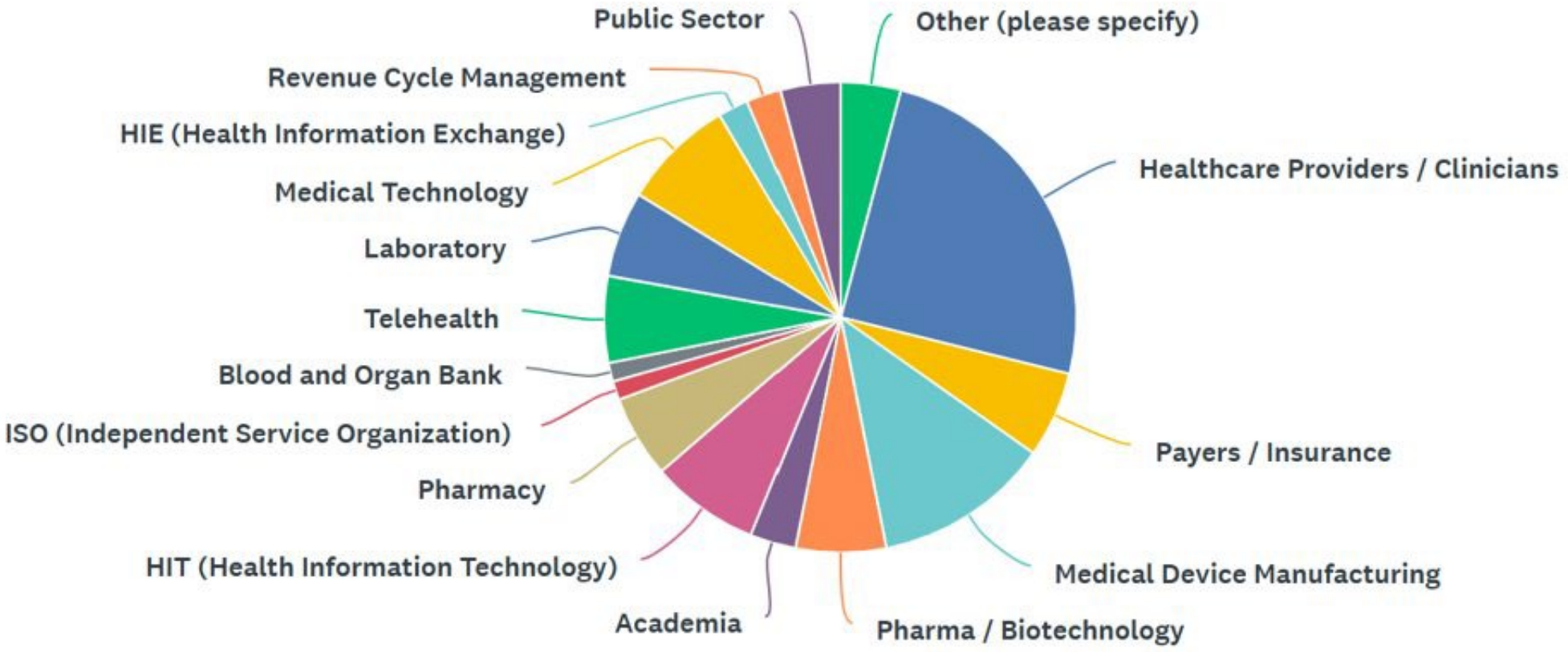
Respondents: 244

Completed Surveys: 201

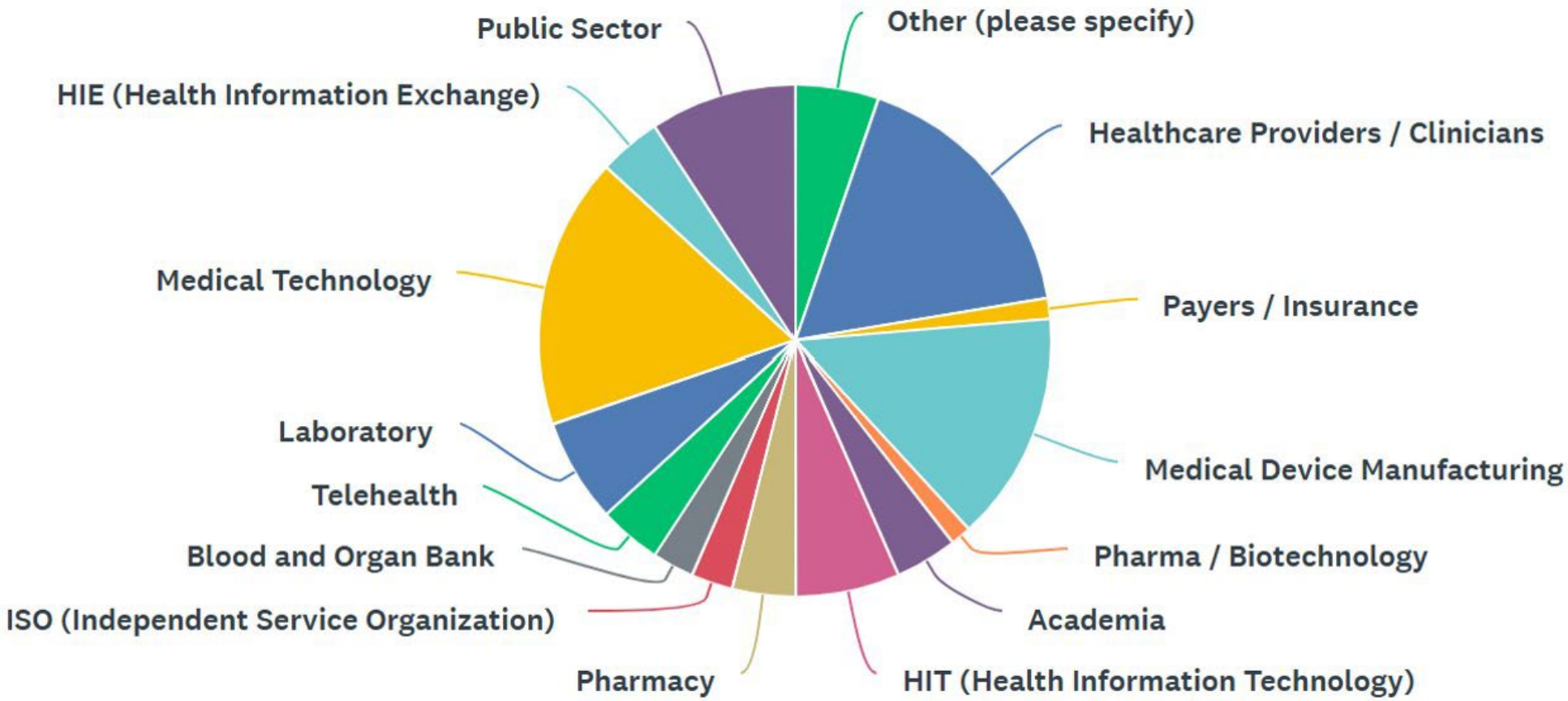
Flow: Show All Respondents then AAMI respondents separately



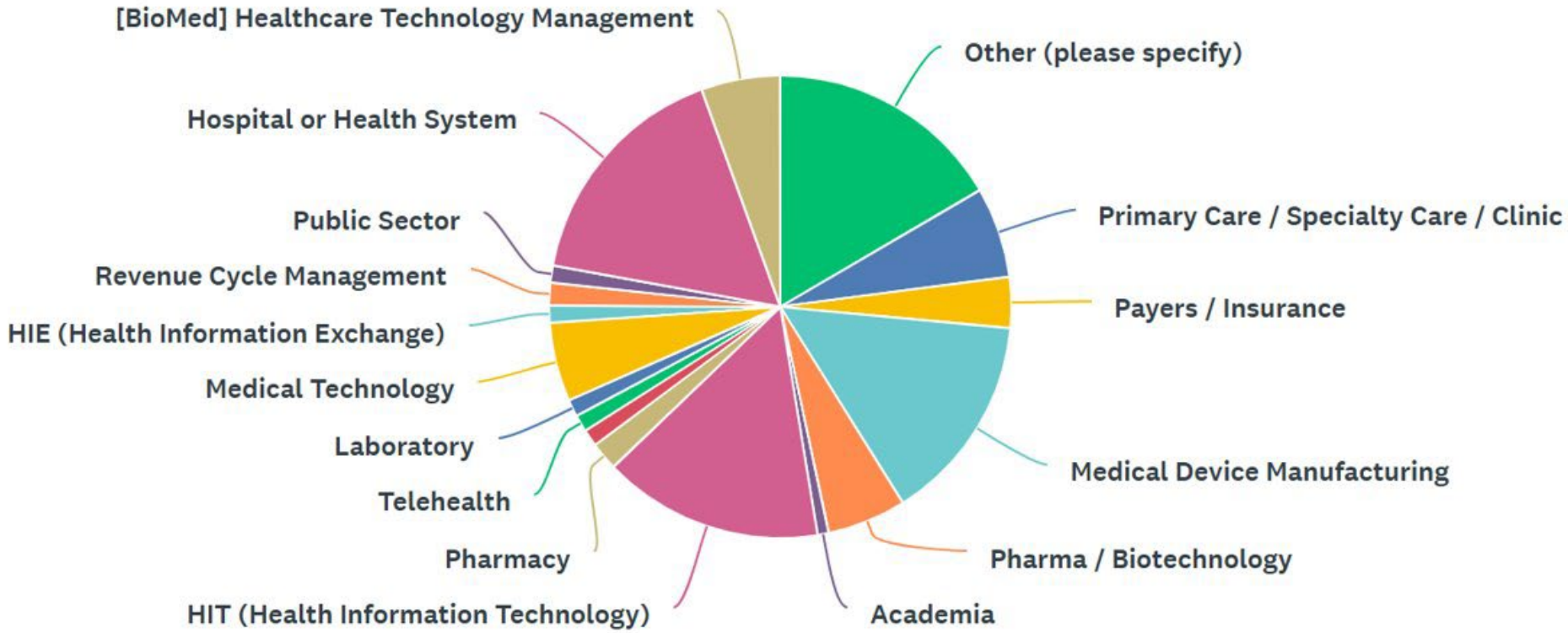
In what business lines does your company operate? (all respondents)



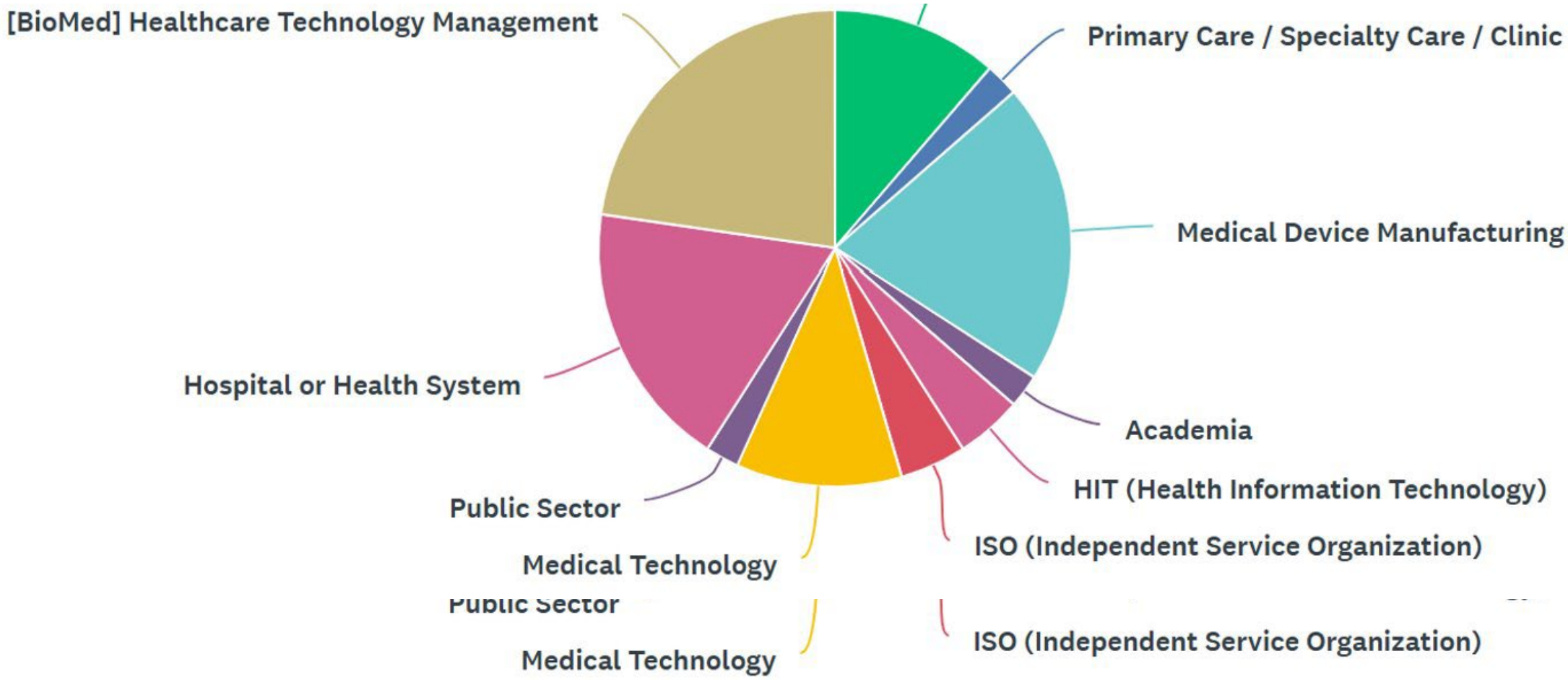
In what business lines does your company operate? (AAMI respondents)



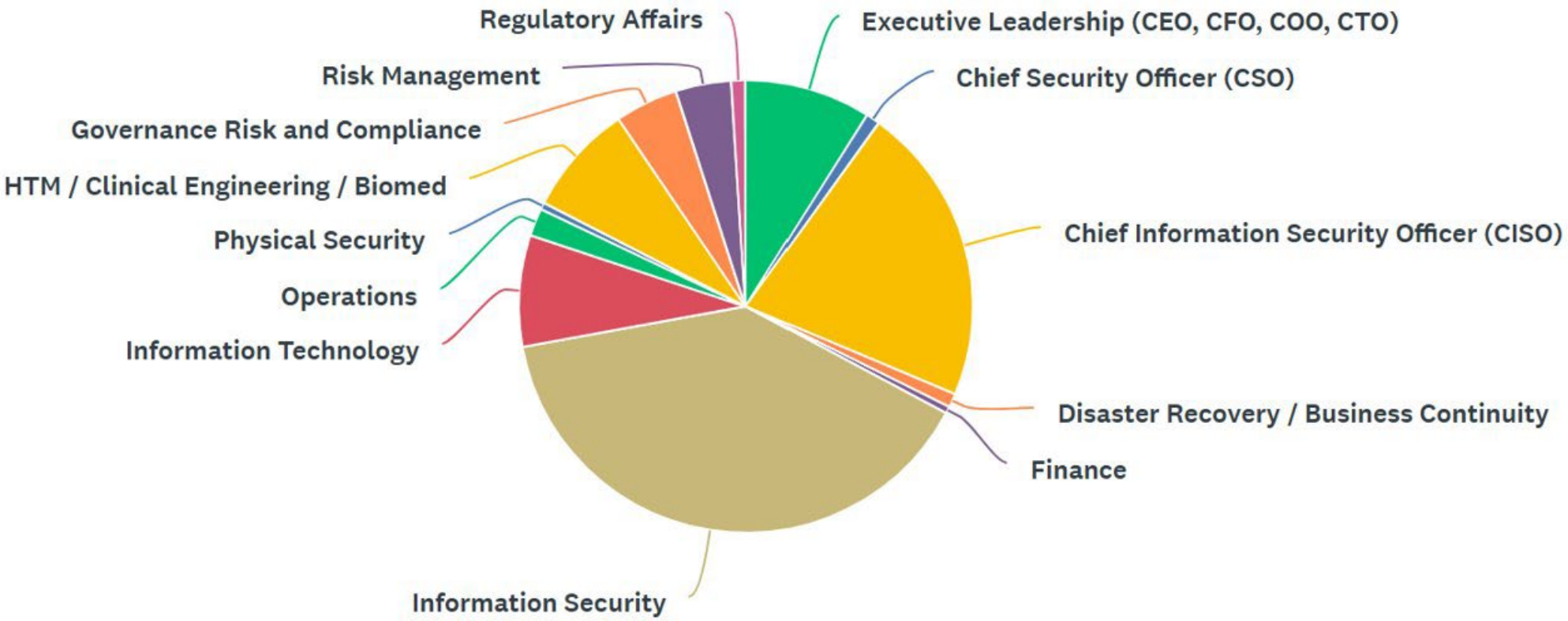
In your position, what business unit do you primarily work in? (All)



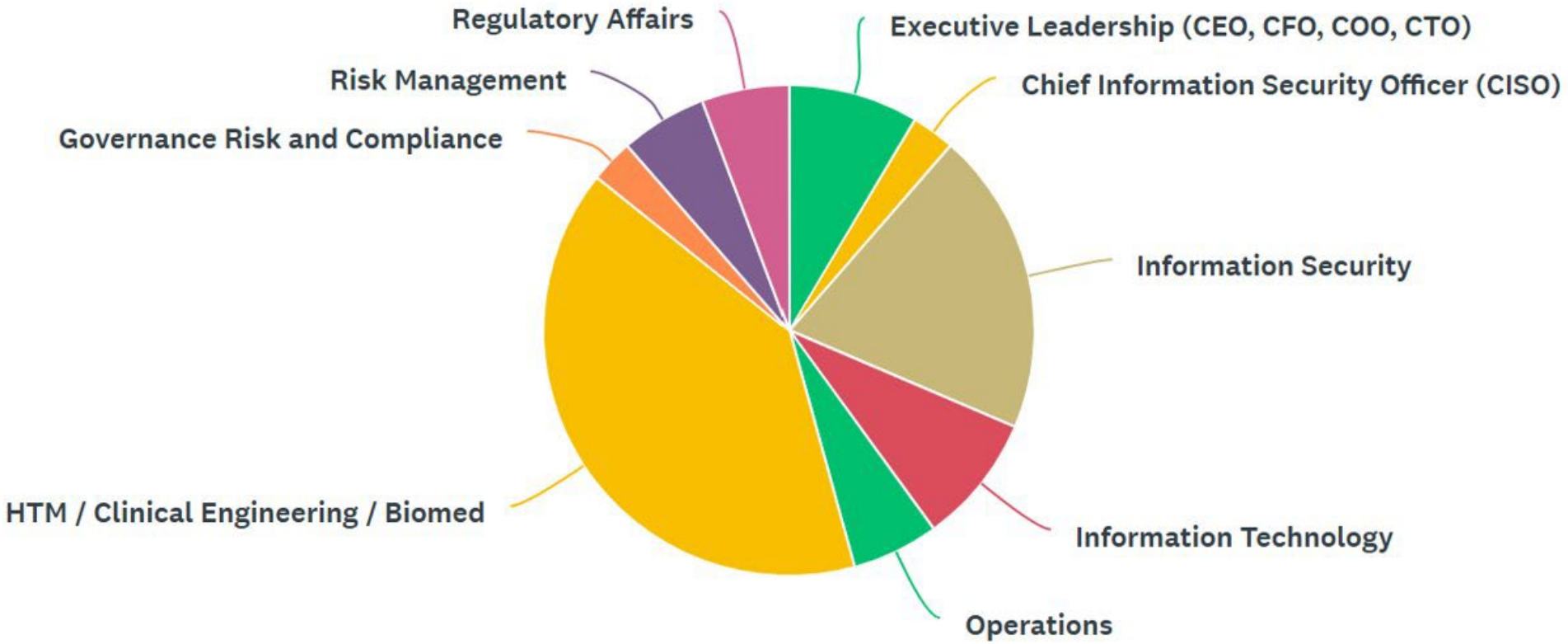
In your position, what business unit do you primarily work in? (AAMI)



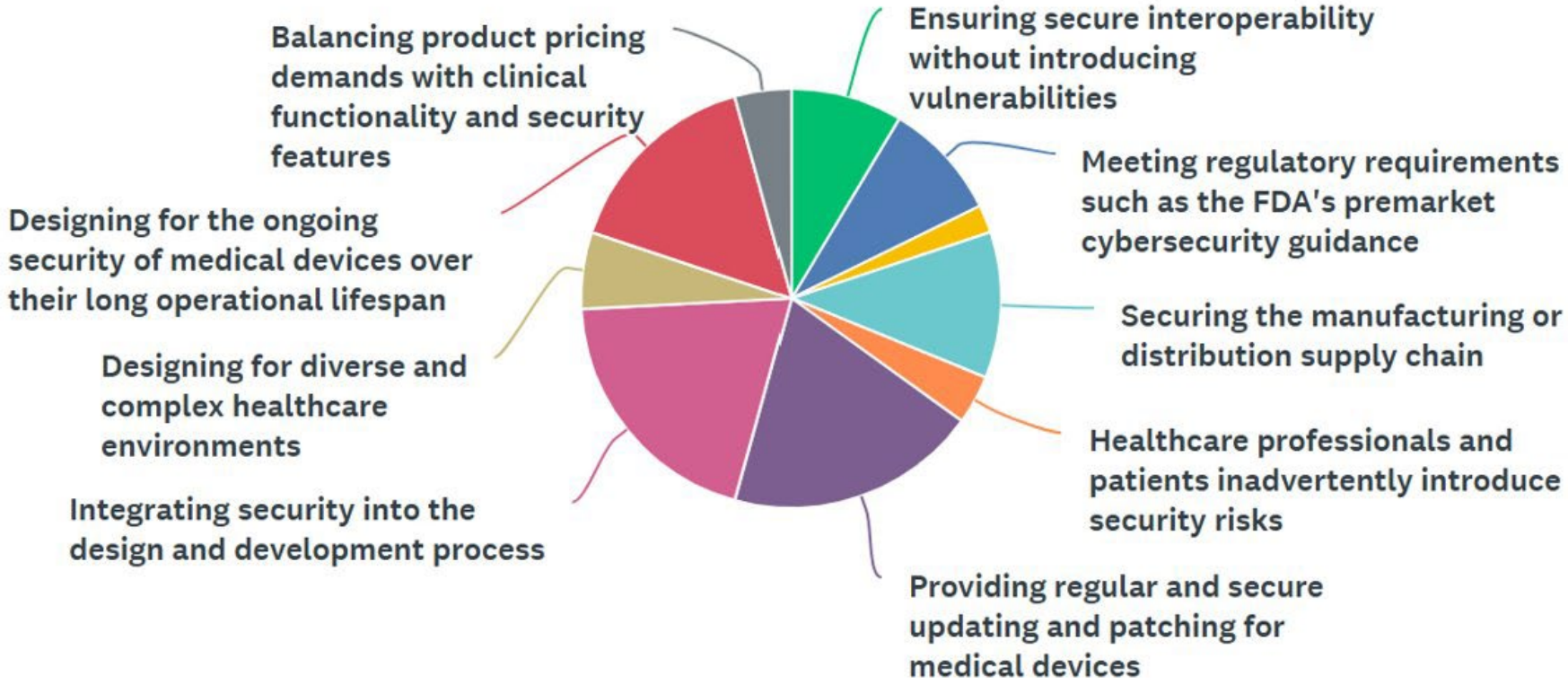
What is your role in your business unit? (All)



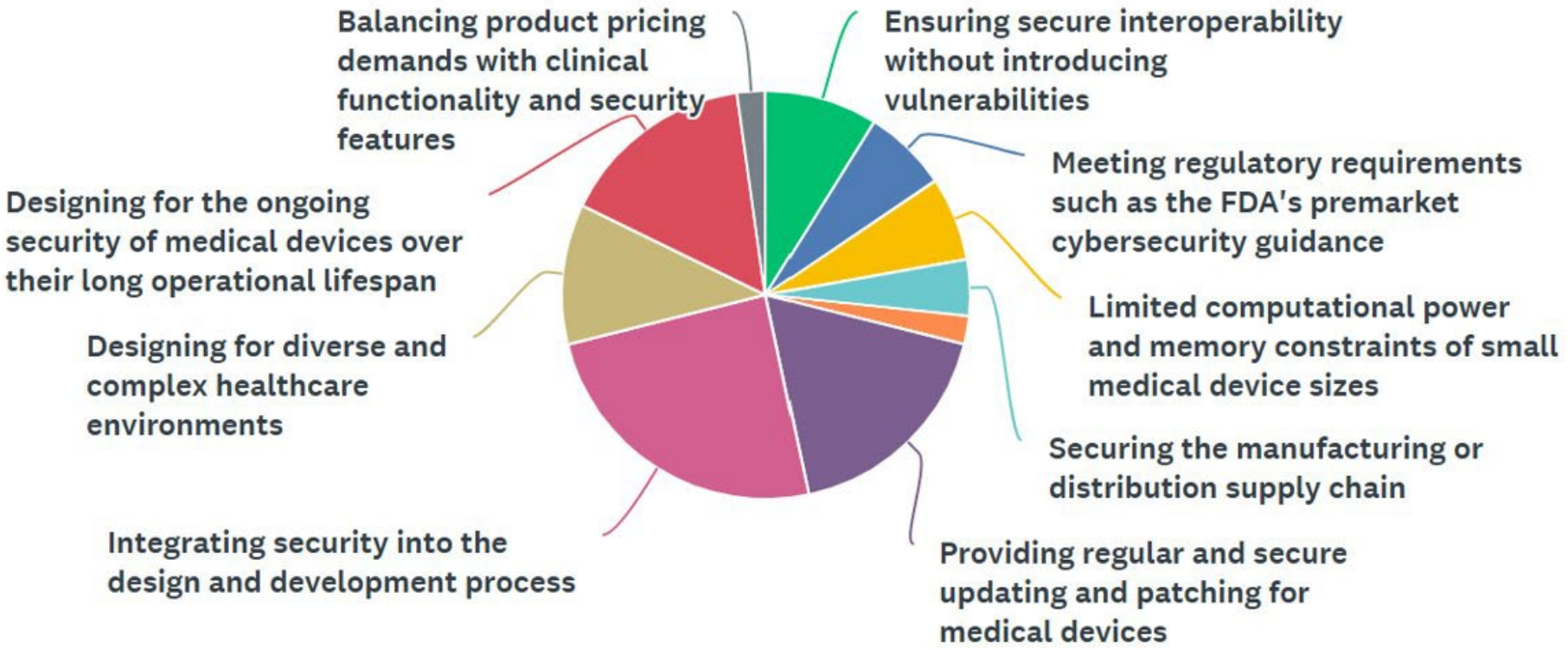
What is your role in your business unit? (AAMI)



What are the top 3 most significant challenges in developing secure medical devices? (MDM respondents)



What are the top 3 most significant challenges in developing secure medical devices? (AAMI)



Top 3 most significant challenges in developing secure medical devices

AAMI

73% - Integrating security into the design and development process

53% - Providing regular and secure updating and patching for medical devices

47% - Designing for the ongoing security of medical devices over their long operational lifespan

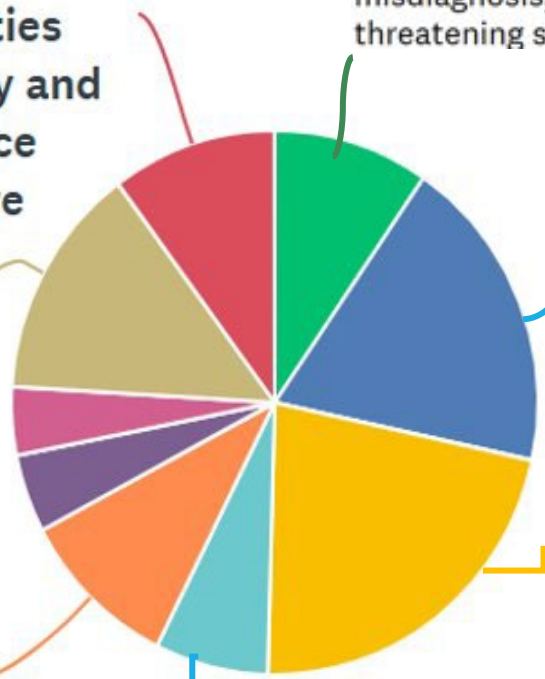
All Respondents

60% - Integrating security into the design and development process

58% - Providing regular and secure updating and patching for medical devices

47% - Designing for the ongoing security of medical devices over their long operational lifespan

What are the top 3 most significant impacts on Healthcare Delivery Organizations? (All)



Compromised medical device functionality leading to misdiagnosis, incorrect treatment, patient harm, or even life-threatening situations

Supply chain vulnerabilities impacting the availability and integrity of medical device components and software updates

Unauthorized access, theft, or exposure of patients' personal health information (PHI), resulting in privacy violations and legal consequences

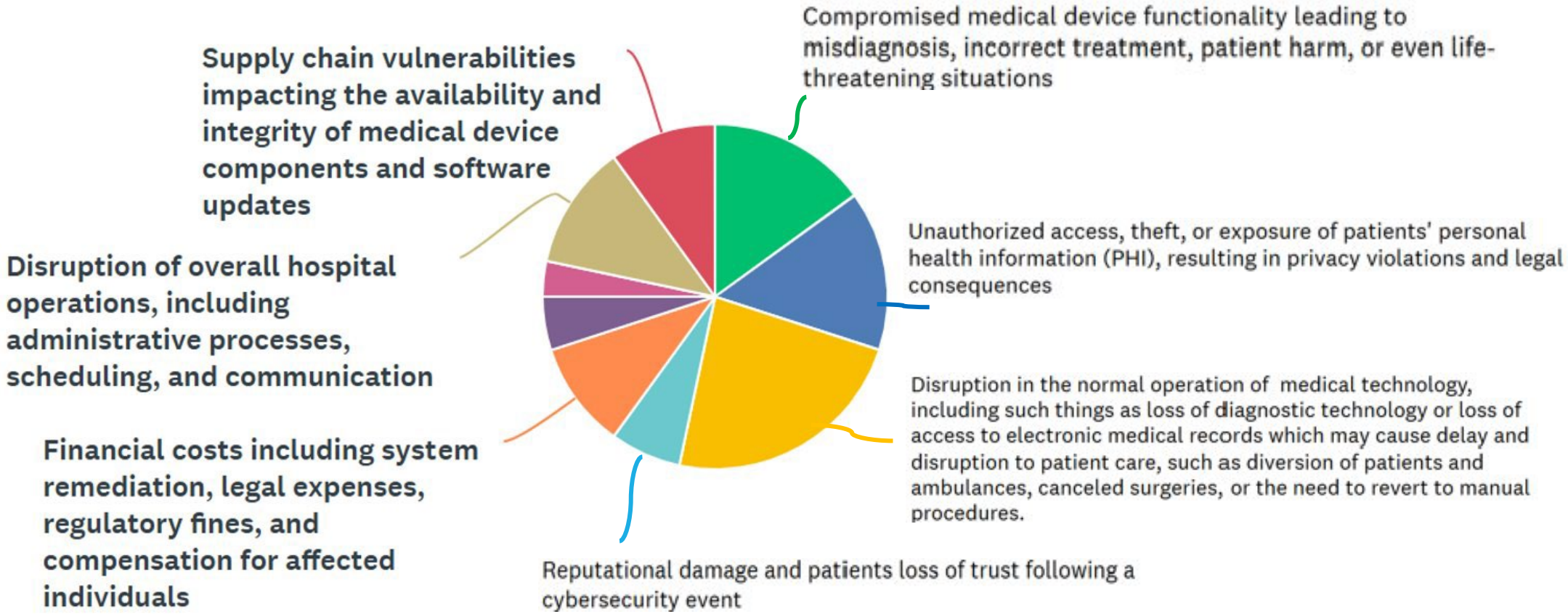
Disruption of overall hospital operations, including administrative processes, scheduling, and communication

Disruption in the normal operation of medical technology, including such things as loss of diagnostic technology or loss of access to electronic medical records which may cause delay and disruption to patient care, such as diversion of patients and ambulances, canceled surgeries, or the need to revert to manual procedures.

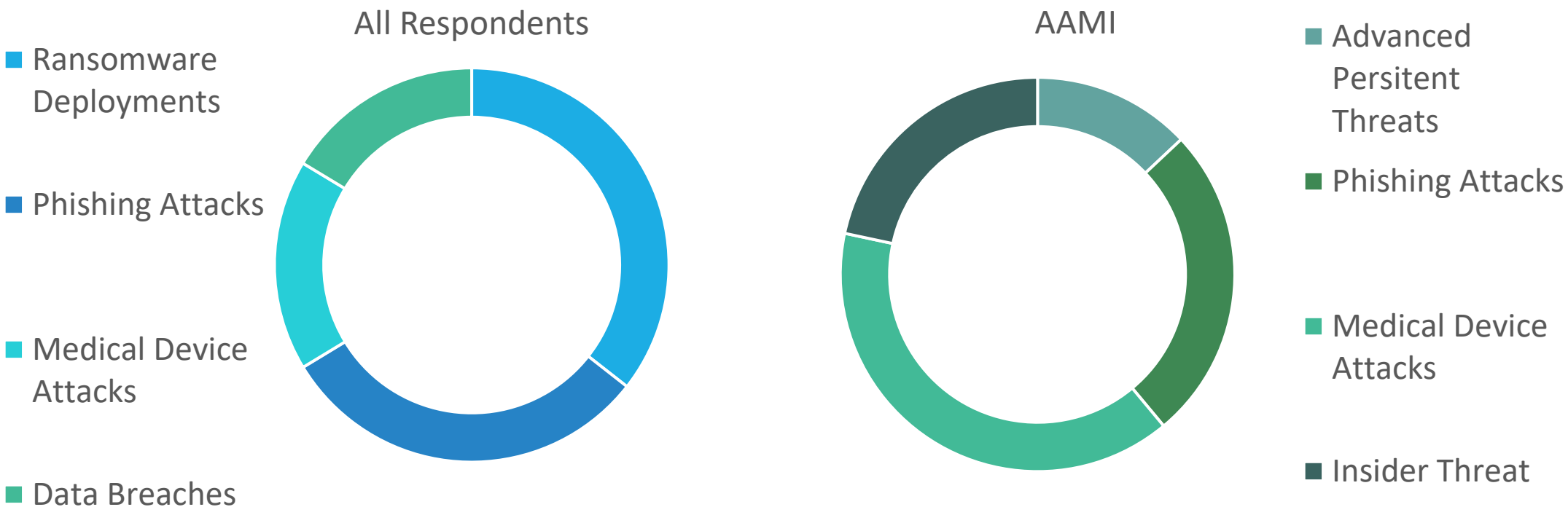
Financial costs including system remediation, legal expenses, regulatory fines, and compensation for affected individuals

Reputational damage and patients loss of trust following a cybersecurity event

What are the top 3 most significant impacts on Healthcare Delivery Organizations? (AAMI)



Greatest cybersecurity threat concerns in 2025?



Take Aways

1. Excellent alignment of HTM and broader Healthcare community view.
2. Secure design and patchability are top medical device challenges
3. Disruption of med-tech operations and data exposure are considered significant impacts
4. Phishing & Medical Device attacks are seen as greatest threats

What HTM can do

1. Cybersecurity is maintenance operations & an HTM function.
2. Patching and updates are preventative maintenance
3. Cybersecurity operations is a team sport – get in the game.
4. Cybersecurity impacts patient care delivery
    1. Plan B – How does clinical operations continue without medical devices?
    2. Restoration - Consider how to recover clinical functionality
    3. Exercise it - TTX, include clinical, IT, HTM
        1. KISS – the CT is ransomed, now what?

Questions?

Please type your questions
in the Q&A window

Thank You

Taylor Porter
tporter@h-isac.org

Phil Englert
penglert@h-isac.org

Health-ISAC
Collaborating for Resilience in Health

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING