Perspectives in Healthcare Security

An industry report that examines attitudes, concerns, and impacts on medical device security as well as cybersecurity across large and midsize healthcare delivery organizations.

Sponsored by:

CyberMDX
A FORESCOUT COMPANY

PHILIPS

GAME CHANGERS

Ipsos

Table of Contents

Updated by Ipsos on September 9, 2021

Background

In the cybersecurity space, healthcare is one of the **most targeted industries**. A recent report from HHS cited a total of 82 ransomware incidents so far this year worldwide with 60% of them impacting the United States health sector. Whether the hack is committed by notorious gangs such as REvil or Conti or lesser known hackers, hospitals now account for **30% of all large data breaches** and at an estimated cost of **$21 billion in 2020 alone.**

This study, conducted by global market research leader Ipsos, surveyed 130 hospital executives in Information Technology (IT) and Information Security (IS) roles, as well BioMed technicians and engineers. The respondents, who averaged 15 years of experience in their fields, provided insight into the current state of medical device security within hospitals as well as highlighted the challenges their organizations face.

Key Findings

Ransomware is attacking the bottom line

48% of hospital executives reported either a forced or proactive shutdown in the last 6 months as a result of external attacks or queries.

Midsize hospitals feeling more pain

Of respondents that experienced a shutdown due to external factors, large hospitals reported an average shutdown time of 6.2 hours at a cost of $21,500 per hour while midsize hospitals averaged nearly 10 hours at more than double the cost or $45,700 per hour.

Cybersecurity investment not a high priority

Despite continuing cyber-attacks against healthcare and roughly half of respondents experiencing an externally motivated shutdown in the last 6 months, more than 60% of hospital IT teams have “other" spending priorities and less than 11% say cybersecurity is a high priority spend.

Dangerous Vulnerabilities Still Not Dealt With

When asked about common vulnerabilities such as BlueKeep, WannaCry and NotPetya, the majority of respondents said their hospitals were unprotected. 48% of respondents admitted their hospitals were not protected against the Bluekeep vulnerability, and that number increased 64% for WannaCry and 75% for NotPetya.

Lack of automation creates gaps in security

65% of IT teams in hospitals rely on manual methods for inventory calculations with 7% still in full manual mode. In addition, 17% of respondents from midsize hospitals and 15% from large hospitals admitted they have no way to determine the number of active or inactive devices within their networks.

Is there a staffing disconnect?

While 2/3 of IT teams believe they are adequately staffed for cybersecurity, nearly half of Biomed teams believe more staff is needed. Conversely, the industry has been experiencing a cybersecurity talent shortage and 100+ day lag to fill jobs.

Cyber insurance and compliance are popular options

58% of IT teams consider compliance “almost always” and rate it a high impact on their jobs. Similarly, 58% also said they had cyber insurance.

Methodological Overview

Understanding differences in IT/IS concerns and practices across environments and roles

Methodology

20-minute

Double Blinded

Online Survey

Sampling

N=100 IT/IS and N=30 BioMed respondents

n=100

Information Security respondents

n=30

BioMed technicians/ BioMed engineers

Respondent Profile

Years working in current field (mean) **15 years**

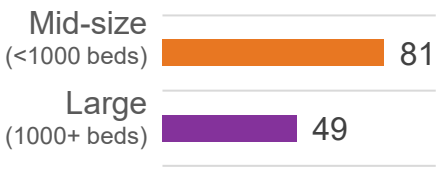
Role

Information technology (IT)	Information security (IS)	Biomedical engineer	Biomedical technician
43%	34%	17%	6%

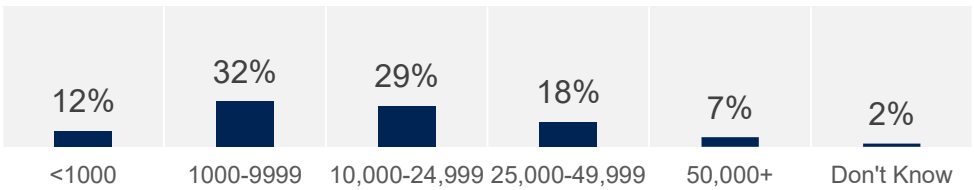
Level of influence on purchasing decisions

	IoT and/or Medical Device Security	Compliance & Governance	Overall IT and/or Cyber Security
I am the **primary decision maker** for purchasing this product or choosing services and providers/vendors	62%	42%	57%
I am **one but not the primary decision marker** for purchasing this product or choosing services and providers/vendors	29%	42%	35%
I **provide input**, but am not a decision maker for purchasing this product or choosing services and providers/vendors	5%	12%	6%
I use items and services from this category or work with providers/vendors but **have no influence** in purchasing decisions	2%	2%	1%
Not applicable	1%	1%	1%

Hospital system size



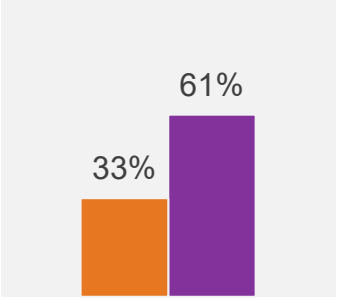
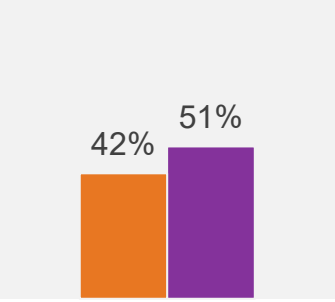
of medical devices in hospital



S1,S2,S5, S6, S8, Q207

Previous Shutdown Experience

Large hospitals appear more likely to have experienced internally or externally initiated shutdowns

	Previous shutdown scenarios	Device shutdown time *(hours)*	Device shutdown financial impact *(cost per hour, thousands)*
Shutdown of devices by external attacks		9.8 6.2	$45.7 $21.5
Shutdown of devices due to accidental internally-initiated action (e.g. phishing)		5.8 5.7	$4.8 $16.7

Midsize Large

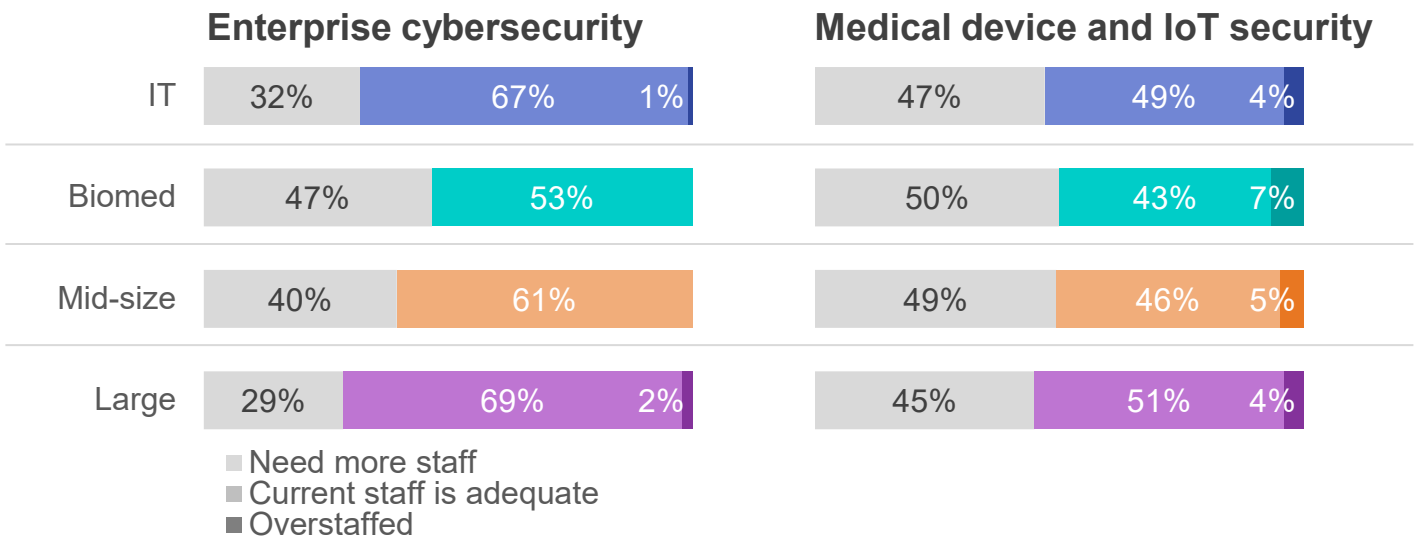
Base: Respondents who have experienced unplanned shutdowns (n=Varies)
Q240. Which of the following device shutdown scenarios has your hospital encountered in the last 6 months? 250. How long has a typical device shutdown lasted? 255. How much does a device shutdown cost your hospital per hour?

Cybersecurity Staffing

Almost half of all respondent types find their medical device & IoT security staffing inadequate

# of staff members *(mean)*	IT	Biomed	Mid-size	Large
Enterprise cybersecurity	12.1	17.5	13.4	13.2
Medical device and IoT security	11.5	15.9	12.7	12.2

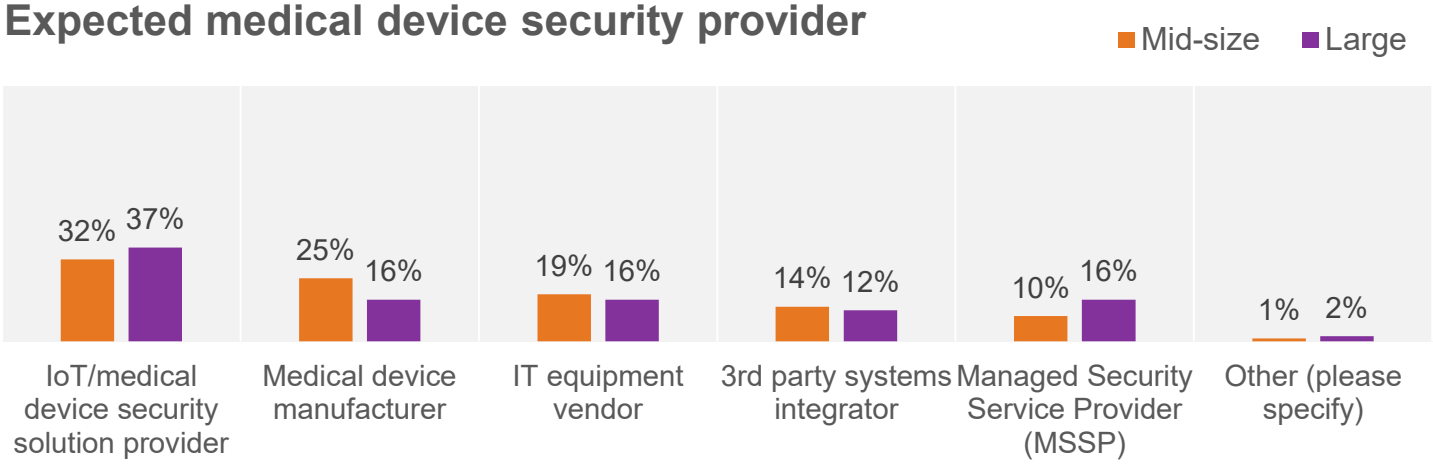
Staffing adequacy



Base: All Respondents, IT (n=100), Biomed (n=30), Mid-size (n=81), Large (n=49)
Q335. How many staff members are focused on the following cybersecurity vectors: Q340. Is the current staffing level adequate to maintain strong security for the following cybersecurity vectors:

Cybersecurity Policy and Concern Dashboard

Expected medical device security provider



Inventory knowledge

	Midsize	Large
I know the exact number of devices	24%	23%
I don't know the number, but we have a dashboard that can tell us the exact number	59%	63%
We don't have a way to determine that number	17%	14%

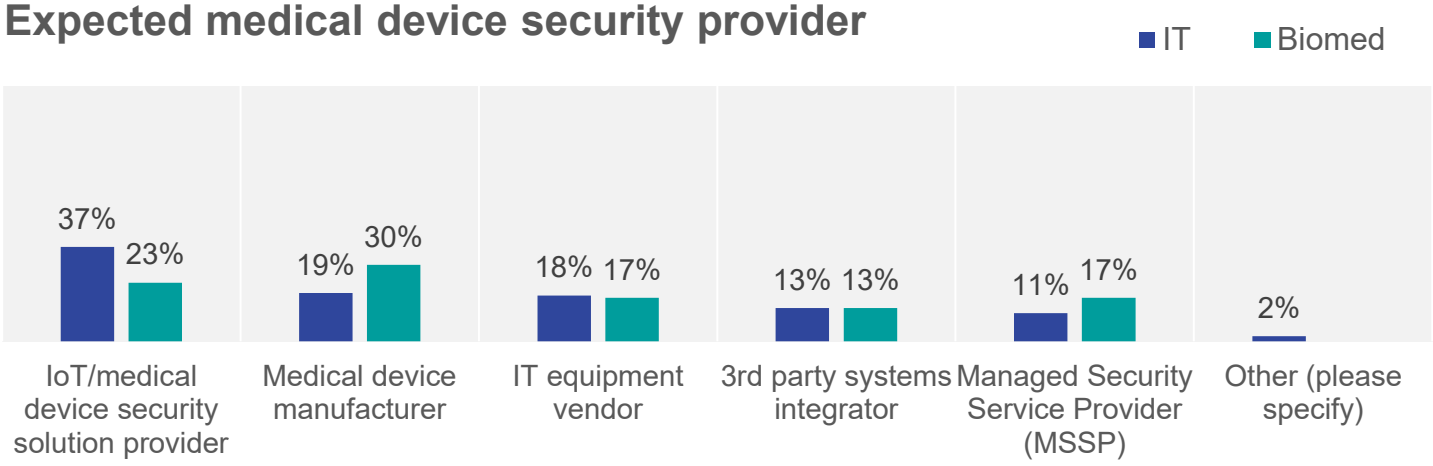
Inventory policy

	Midsize	Large
Automated software system with full visibility to all	12%	22%
Software system with limited visibility	21%	18%
Mix of some automation and manual inventory	56%	53%
Fully manual inventory	11%	4%
I don't know	-	2%

Base: All Respondents, Small/Medium (n=81), Large (n=49)
Q207A, Q207B
Q213. When it comes to securing medical devices in your hospital, which type of provider do you expect to protect your hospital?

Cybersecurity Policy and Concern Dashboard

Expected medical device security provider



Inventory knowledge

	IT	Biomed
I know the exact number of devices	27% B	10%
I don't know the number, but we have a dashboard that can tell us the exact number	59%	67%
We don't have a way to determine that number	14%	23%

Inventory policy

	IT	Biomed
Automated software system with full visibility to all	15%	20%
Software system with limited visibility	19%	23%
Mix of some automation and manual inventory	58%	43%
Fully manual inventory	7%	13%
I don't know	1%	-

Base: All Respondents, IT/IS (n=96), Biomed (n=26)
Q207A, Q207B
Q213. When it comes to securing medical devices in your hospital, which type of provider do you expect to protect your hospital?

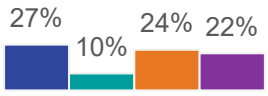
Knowledge Of In-network Devices

Most respondents' inventory is still partially manual

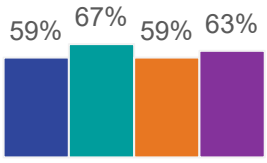
# of medical devices in hospital *(mean)*

	IT	Biomed	Mid-size	Large
<1000	13%	7%	17%	2%
1000-9999	27%	50%	40%	20%
10,000-24,999	29%	30%	27%	33%
25,000-49,999	20%	10%	11%	29%
50,000+	8%	3%	1%	16%
Don't Know	3%	-	4%	-

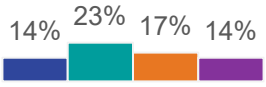
Knowledge of # of devices



I know the exact number

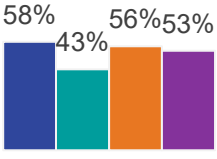


I don't know the number, but we have a dashboard that can tell us the exact number

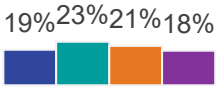


We don't have a way to determine that number

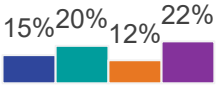
Inventory policy



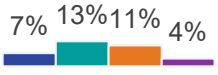
Mix of some automation and manual inventory



Software system with limited visibility



Automated software system with full visibility to all



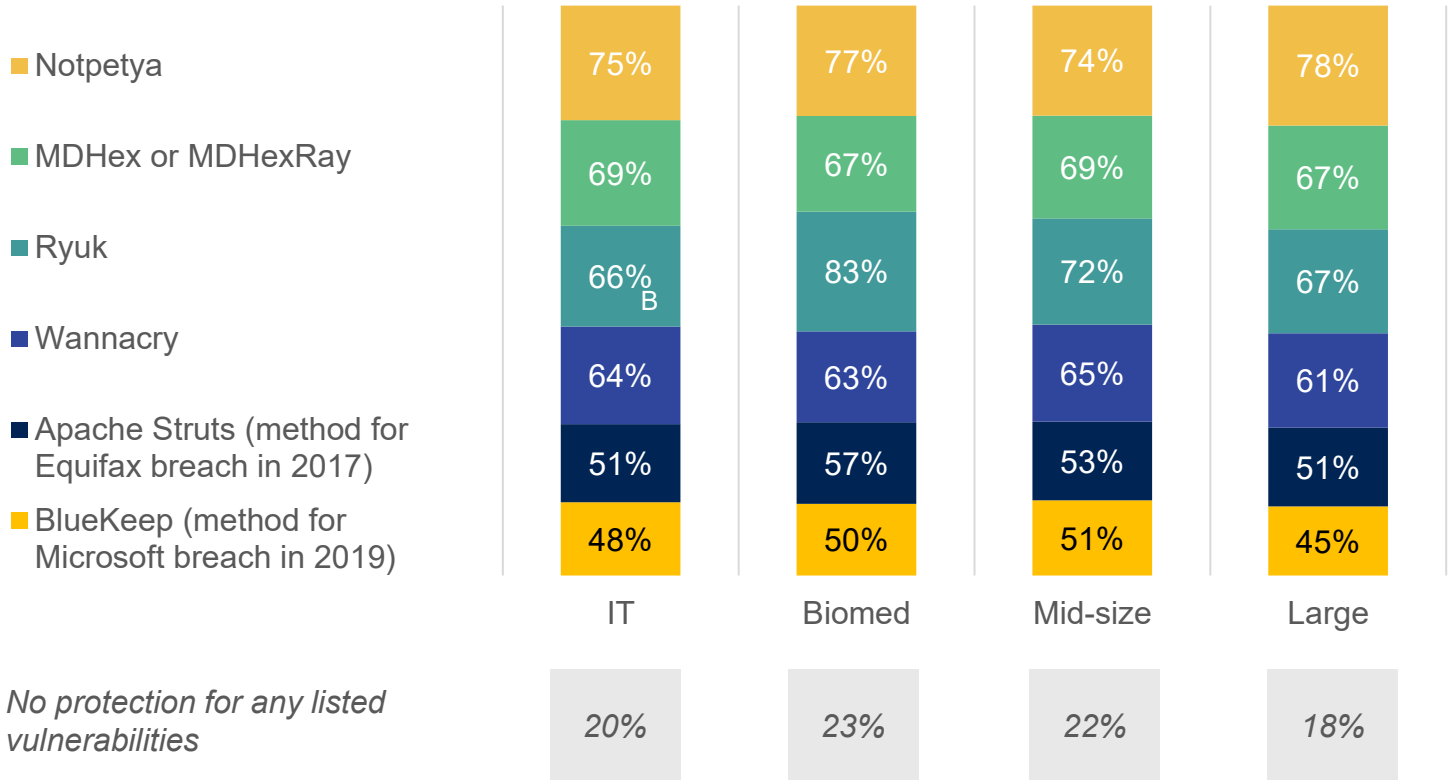
Fully manual inventory

Base: All Respondents, IT (n=100), Biomed (n=30), Mid-size (n=81), Large (n=49)
Q207. Approximately how many medical devices are in your hospital system's network?
Q207A. Which best describes your knowledge of the number of IoT devices (both managed and unmanaged) in your hospital system's network? Q207B. How do you currently inventory medical, connected medical, IoT and IoMT devices?

Current Cybersecurity Characteristics

Bluekeep and Apache Struts are the most common protected vulnerabilities across the board

Current vulnerabilities: *NOT PROTECTED*



Base: All Respondents, IT (n=100), Biomed (n=30), Mid-size (n=81), Large (n=49)
Q225. Are the medical devices/IoT in your hospital protected against the following vulnerabilities?

Cybersecurity Spending and ROI

2 out of 3 respondents do not track ROI for cybersecurity spending

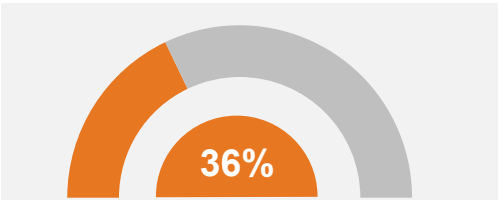
Annual IT Spend *(mean)*

Annual IT Budget	**$3.5M**	**$3.1M**
Don't know / Not willing to share	*70%*	*67%*

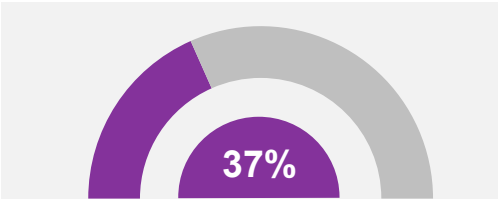
Annual medical device and IoT cybersecurity spend *(mean)*

Annual Spend	**$293K**	**$329K**
Don't know / Not willing to share	*77%*	*69%*

ROI for cybersecurity spending *(% Yes)*

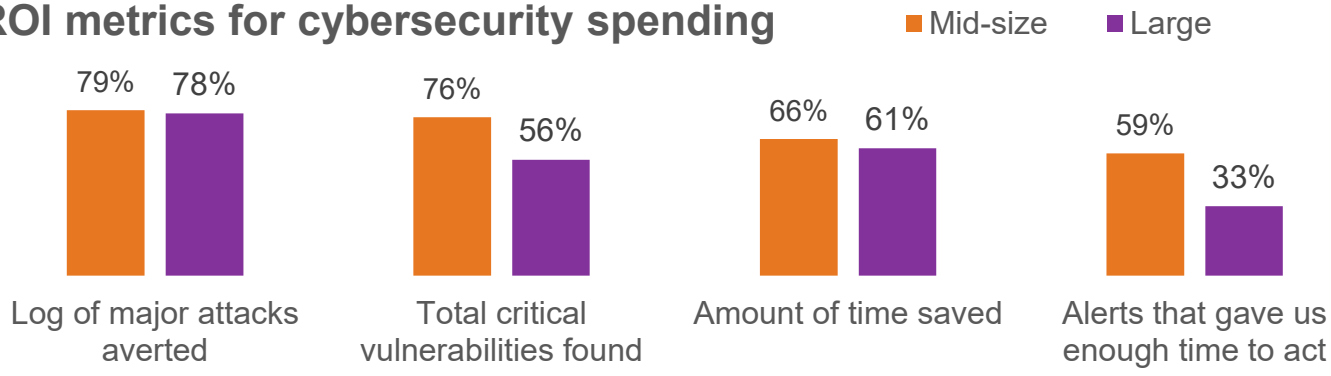


Mid-size



Large

ROI metrics for cybersecurity spending

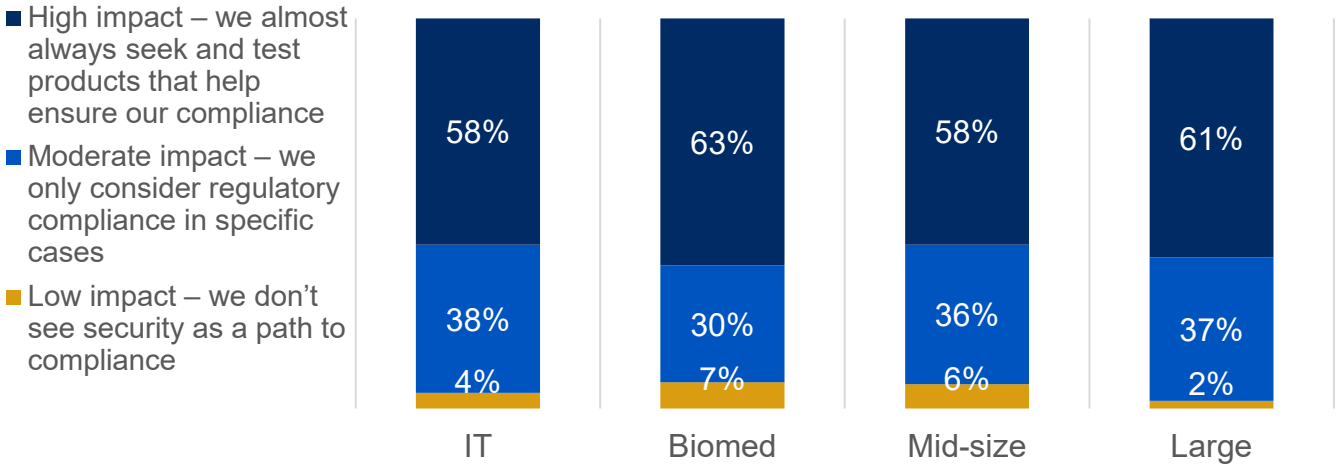


Base: All Respondents, Mid-size (n=81), Large (n=49)
Q405A. What is your hospital's annual IT budget? Q410A. What is your hospital's annual medical device and IoT cybersecurity budget? Q520. Does your hospital or hospital system formally measure ROI (return on investment) for cybersecurity software and services spending?
Base: Respondents measuring ROI, Mid-size (n=29*), Large (n=18*)
Q520A. Which metrics are critical for your hospital or hospital system to formally measure ROI (return on investment) for cybersecurity software and services spending?

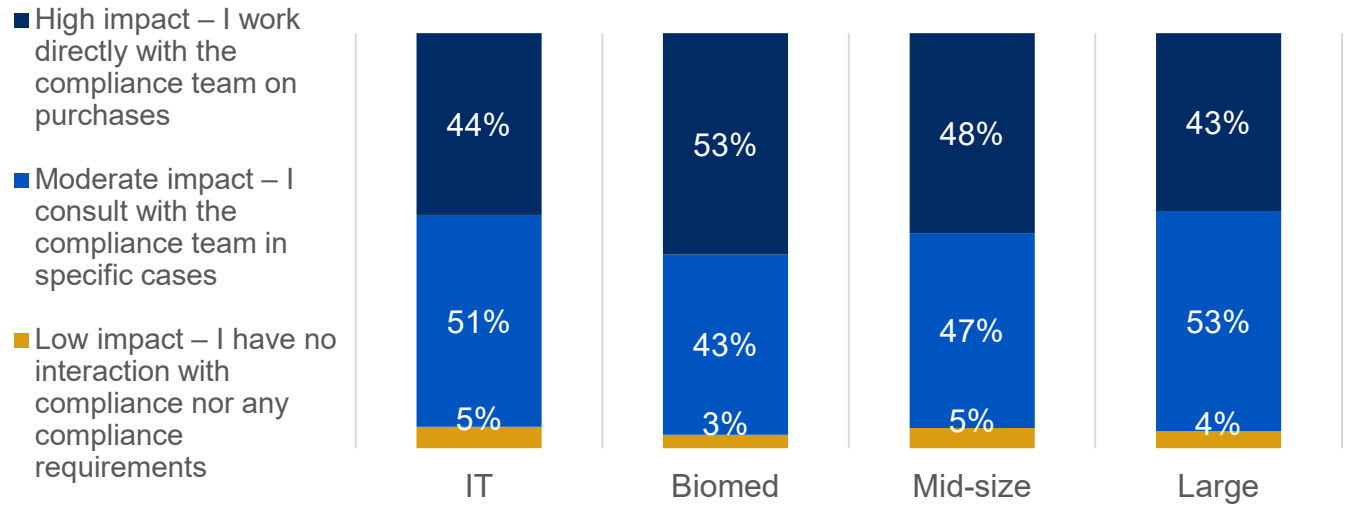
Compliance Impact

Compliance has moderate-high impact on respondents' roles; Impact appears even larger for cybersecurity purchasing

Impact of compliance on cybersecurity purchasing



Impact of compliance on job/role

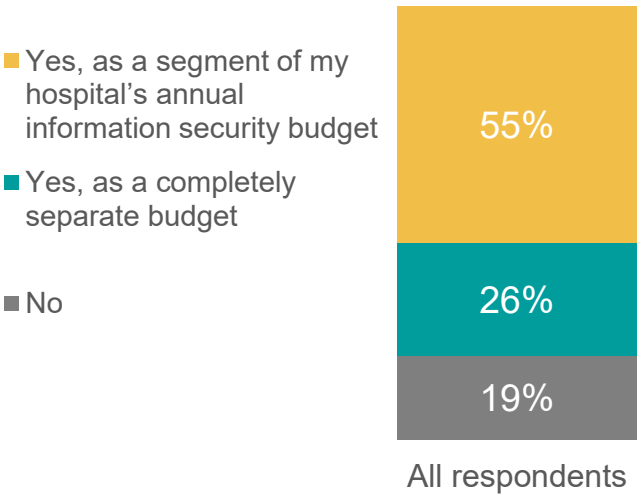


Base: All Respondents, IT (n=100), Biomed (n=30), Mid-size (n=81), Large (n=49)
Q280. To what extent is regulatory compliance (e.g. HIPAA) impacting your hospital's cybersecurity purchasing? Q285. To what extent is regulatory compliance (e.g. HIPAA) impacting your job/role?

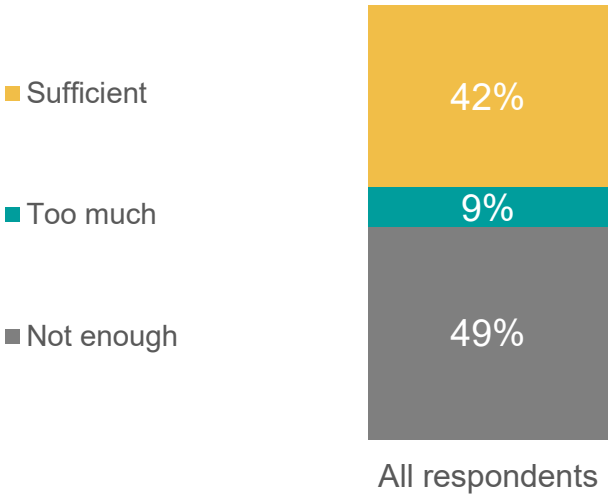
Compliance budget

Almost half of all respondents find their annual compliance budget insufficient

Specific budget for compliance



Adequacy of compliance budget



Hospital annual cybersecurity compliance budget

All respondents

$617 thousand

75% *Don't know / Not willing to share*

Base: All Respondents (n=130)
Q420. Does your hospital or hospital system have a specific budget for medical device and IoT cybersecurity compliance?
Q435. My hospital's annual cybersecurity compliance budget is:
Base : Respondents with specific compliance budgets (n=105)
Q430. What is your hospital's annual cybersecurity compliance budget?

Sponsored by:

CyberMDX
A FORESCOUT COMPANY

PHILIPS

GAME CHANGERS

Ipsos