Cynerio Ponemon INSTITUTE

The Insecurity of Connected Devices in Healthcare 2022

A report Presented by Cynerio and Ponemon Institute

An industry report that examines the current impacts of cyberattacks on healthcare facilities and network-connected IoT and medical devices.

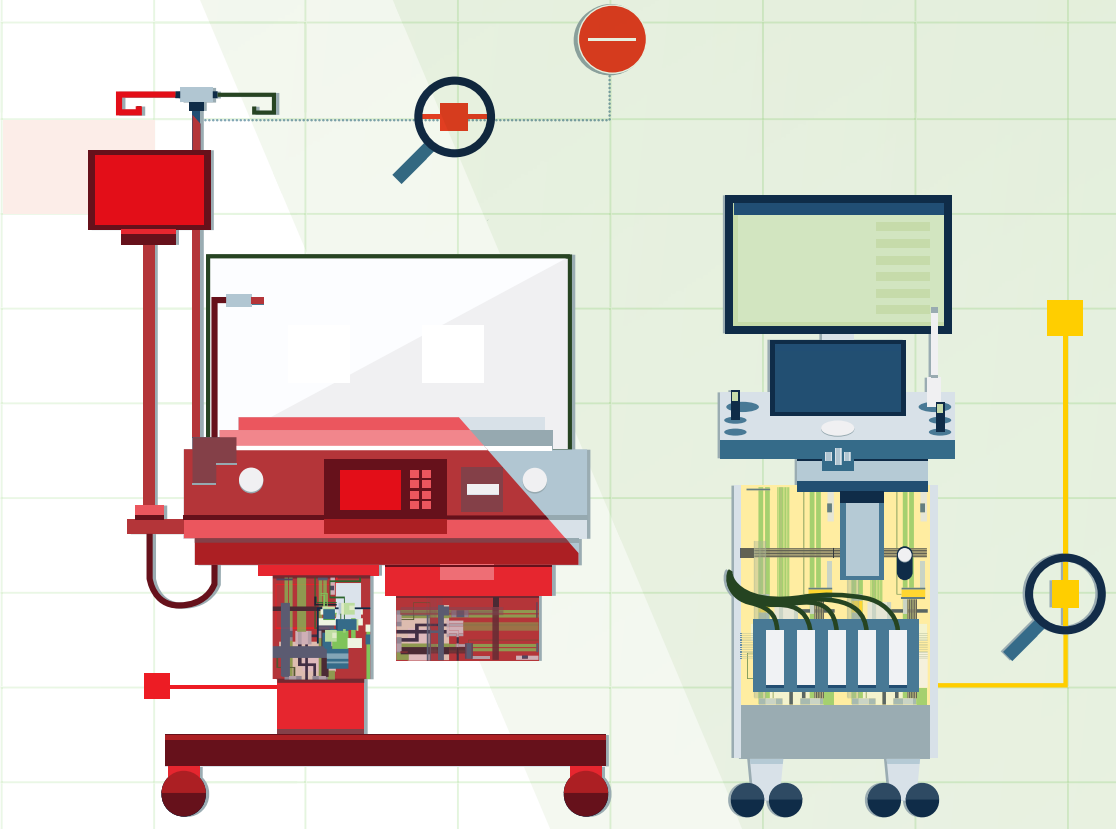
Table of Contents

Background

Healthcare facilities have been increasingly targeted by cyberattacks at alarming rates. Fueled by lagging security practices and failures measured in fatalities rather than fiscal loss, nation-states, ransomware gangs and other groups have identified an industry that presents low levels of cyber protection paired with multiple revenue channels. In nearly any other industry such results would be akin to an act of war, but everyday interactions with mortality have contributed to a more conservative approach to addressing the threats introduced by unprotected technology, namely IoT and IoMT devices. This report will make it clear that IoT and IoMT have been, and will likely continue to be, primary targets for cybercriminals.

This report highlights a wide range of data that until now was based on anecdotes and cautionary tales rather than larger trends and academic investigation. The volume of those data points has become large enough to warrant this more formal research, which has uncovered multiple trends that far exceed the worst case scenarios considered by healthcare industry leaders.

The information in this report was collected jointly by the Ponemon Institute and Cynerio and is based on data provided by 517 healthcare experts in leadership positions at hospitals and healthcare systems throughout the United States. With hospitals struggling to stem the tide of seemingly non-stop cyberattacks it is clear that original research, insight and guidance is needed now more than ever. It is also clear that the gap between cyberattacks and their more dangerous cyber-physical brethren has been bridged. From alarming mortality rate increases to higher than expected ransomware payments, this research is intended to clarify the risks faced by those we trust most in vulnerable times - healthcare facilities and the heroes that operate within them.



Executive Summary

Cyberattacks Are Frequent with Notable Impact on Patient Care

The fallout of cyberattacks on healthcare is often measured fiscally, but this study uncovers a darker truth. **56% of respondents say their organizations experienced one or more cyberattacks in the past 24 months involving IoMT/IoT devices**, with an average of 12.5 attacks over the same timeframe. 45% of these respondents report adverse impacts on patient care from these attacks, and 53% percent of those (24% in total) report adverse impacts resulting in increased mortality rates.

Ransomware Is a Vicious, Profitable Cycle Fueled by Frequent Hospital Payments

Ransomware attacks are crippling to all aspects of a hospital and often present a situation with only bad options. Hospitals are increasingly seeing ransom payments as a viable option for quick recovery with 47% of those experiencing an attack resulting in a ransom being paid. **32% of the ransoms paid fall in the range of $250k - $500k.** Those that did not pay the ransom most frequently attributed their actions to an effective backup strategy (53%) and company policy (49%).

Repeat Attacks Are Commonplace and Inevitable

The anecdotal nature of cyberattack examples paints a picture of one-time attacks with poor outcomes. The truth is that attackers routinely perform long-term operations that uncover numerous avenues for repeated attacks. Of the previously noted 56% of respondents who experienced at least one cyber attack in the last 24 months, 82% of those experienced an average of 4 or more attacks in that timeframe. **Ransomware attacks experienced roughly equivalent rates, with 43% of respondents having experienced an attack** and 76% of those experiencing an average of three or more.

Cyberattacks Including Data Breaches Almost Always Involve IoT / IoMT Devices

Reselling patient data is still valuable, as demonstrated by the **43% of respondents who suffered at least one data breach in the prior 24 months.** Of those, 65% suffered an average of 5 or more data breaches in that timeframe with IoT / IoMT devices being involved 88% of the time. Respondents were asked to estimate the total cost of the one largest data breach involving an IoMT/IoT device including direct cash outlays, direct expenditures, indirect labor costs, overhead costs and lost business opportunities. The average total cost of the largest data breach was estimated at $13 million for the organizations represented in this research.

Lacking Ownership and Accountability Delay IoT / IoMT Security

One reason for lagging security practices is clear - there is no widely accepted ownership. When asked who is primarily responsible for ensuring the security of these risky devices, **not one role received more than 18% of responses.** Even the top responses varied widely from CIO/CTO (18%) to Operations Leadership (14%), CISO/CSO (14%) and Network Leadership (11%). In an industry where leadership and guidance is often well defined, the lacking agreement on responsibility for IoT/IoMT devices requires significant improvements.

Perceived Risk in IoT / IoMT Devices Is High, but Proactive Security Actions Are Not

When asked to rate the level of security risk created by IoMT/IoT devices on a 1-10 scale (1 = low risk to 10 = high risk), 71% of respondents rated the risk as high or very high (7 or higher) but **only 21% of respondents self-report a mature stage of proactive security actions.** In about half of cases (46%) the most basic activity of scanning for devices is in-place, but ⅔ of these respondents (67%) don't track the resulting inventory.

On Average Hospitals Report Spending 3.4% of IT Budget ($5 Million Annually) to Secure Devices

Budget owners often struggle with allocating resources to secure their environments. This will be an ongoing challenge in the IoT/IoMT space for years to come, but initial practices are clarifying. The typical **IT spend for respondents averages $145 million** in the fiscal year and an average of 17% of that spend is focused on IT security. Of that security spend, an average of 20% was reported to go towards IoT/IoMT device security - an average of $5 million in the fiscal year. These numbers will likely vary widely, but provide an initial baseline for others to work from.

Healthcare Faces Widespread Attack Types

Staffing shortages lead not only to empty seats, but also to large gaps in knowledge. Attackers have taken advantage of the IoT / IoMT security knowledge gap by unleashing a wide array of attacks on healthcare environments. Respondents believe that a combined lack of knowledge and wide array of attacks are leading to a complicated threat landscape. Among the top threats to IoT and other connected devices that **respondents expressed the most concern about were lack of visibility into IoT networks (45%),** phishing (45%), zero-day attacks (41%), and ransomware attacks (39%).

Introduction

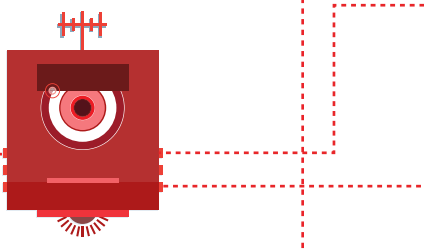
IoT Cybersecurity Practices: Frequent Attacks and Lacking Accountability Notably Impacts Patient Care

56%

Respondents who have experienced at least one cyberattack in the last 24 months involving an IoT / IoMT device

43%

Respondents who have experienced an average of at least one ransomware attack



The vector of IoT/IoMT devices as an entryway for cyberattacks was first documented by the Ponemon Institute in their 2021 Impact of Ransomware on Healthcare During COVID-19 and Beyond report, which revealed that 21% of ransomware attacks are rooted in Medical and IoT devices. What was not fully understood at the time was the collateral damage caused by those attacks, the actions that needed to be taken to protect those devices, and gaps where significant progress could be made. Ponemon's work with Cynerio in this report attempts to resolve many of those questions, often with disappointing, frustrating and occasionally even terrifying results.

While reading through this report, the prevalence of activities and results with the same odds as flipping a coin will become clear. About half (45%) of cyberattacks resulted in adverse impact on patients. About half (53%) of those with adverse impacts

45%

Believe attacks involving IoT / IoMT devices had an adverse impact on patient care

53%

Respondents with adverse impact on patient care who believe there were increased mortality rates due to a cyberattack

24%

Calculated rate of cyberattacks on healthcare that increase mortality rates

on patient care report increased mortality rates after a cyberattack (24% overall). About half (56%) have experienced one or more cyberattacks in the last 24 months. About half (54%) report senior management not requiring assurances that IoT and IoMT risk is being properly addressed. Almost half (43%) have experienced at least one ransomware attack in the last 24 months.

Patients cannot continue to receive treatment in environments with a "heads we win/tails we lose" security mentality at the leadership level, particularly when new technologies and emerging practices are available to reduce risk well below the "about half" failure rates that are currently experienced. The Cynerio and Ponemon teams hope readers find this study informative, beneficial and ultimately constructive despite the dismal data it presents.

Methodology + Respondent Details

Ponemon Institute was founded in 2002 by Dr. Larry Ponemon and Susan Jayson. The Institute is dedicated to independent research and education that advances the responsible use of information and privacy management practices within business and government. The Ponemon Institute mission is to conduct high quality, empirical studies on critical issues affecting the security of information assets and the IT infrastructure. In 2021 Ponemon Institute published unique insight to the threats faced in healthcare environments due to ransomware attacks in The Impact of Ransomware on Healthcare During COVID-19 and Beyond.

Cynerio was founded in 2018 by Leon Lerman and Daniel Brodie with the goal of securing every IoT and IoMT device in healthcare environments. The resulting technical innovations have led to multiple reports and disclosures that have contributed to security improvements in healthcare environments worldwide. Among these were The State of IoMT Device Security 2022 report which provided a significant amount of insight related to the risks, challenges and activities needed to better secure connected devices in healthcare environments.

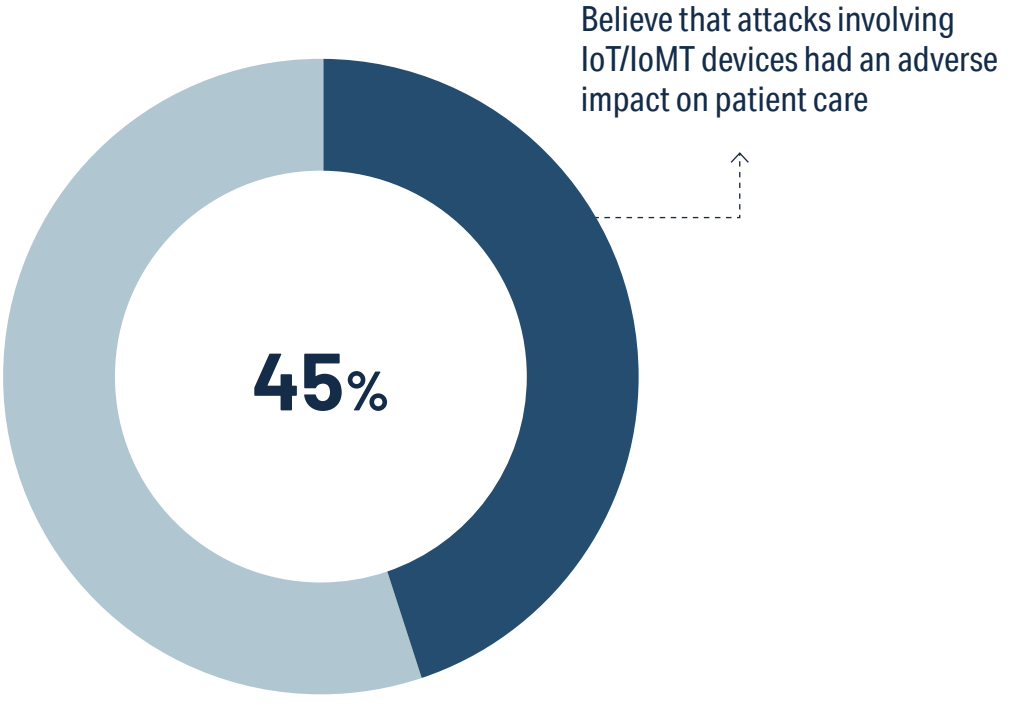
Institute Collaboration

The Cynerio and Ponemon Institute collaboration on this report was driven by necessity over all other factors. Individual healthcare leaders have invaluable data related to the types, methods, and results of cyberattacks on their facilities, as well as insight on the activities being performed in an attempt to prevent future attacks. Unfortunately, collecting and acting on that data is a challenging task made more difficult by the shame, embarrassment and litigation that often arises after being compromised. On behalf of the entire healthcare industry we would like to thank the 517 respondents healthcare leaders who provided brutally honest answers to often difficult questions. Their transparency will help improve IoT and IoMT cybersecurity practices worldwide.

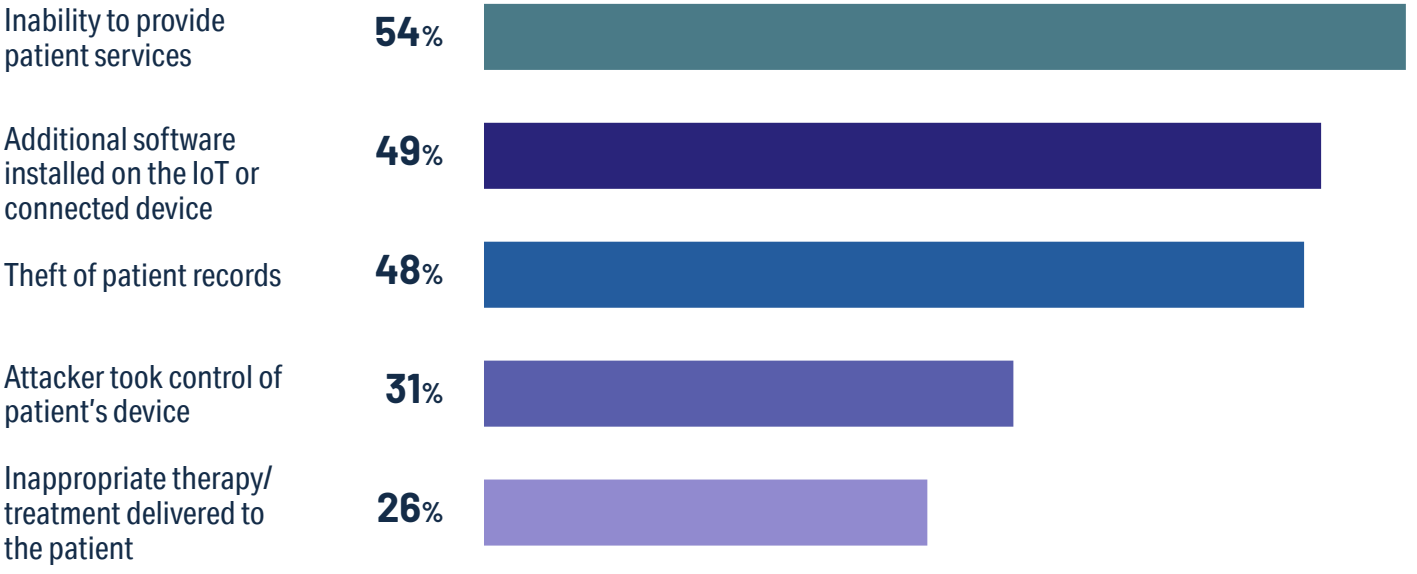
Impact of Cyberattacks on Patient Care

How Did Cybercriminals Disrupt Patient Care?

The effects of adverse events are wide ranging, like the attacks themselves. HIPAA regulations have led to an environment where data breaches are disproportionately reported, leading to a skewed public perception of the risks healthcare providers face. In the background, facilities are confronting attacks that have shifted from bits and bytes to cyber-physical threats. When attacks result in adverse patient care (45%), patients face risks including high rates of impacted service (54%) and inappropriate therapy or treatment deliveries (26%). For every reported set of vulnerabilities related to hospital robots or infusion pumps, there are likely thousands more that are unknown and far more dangerous.

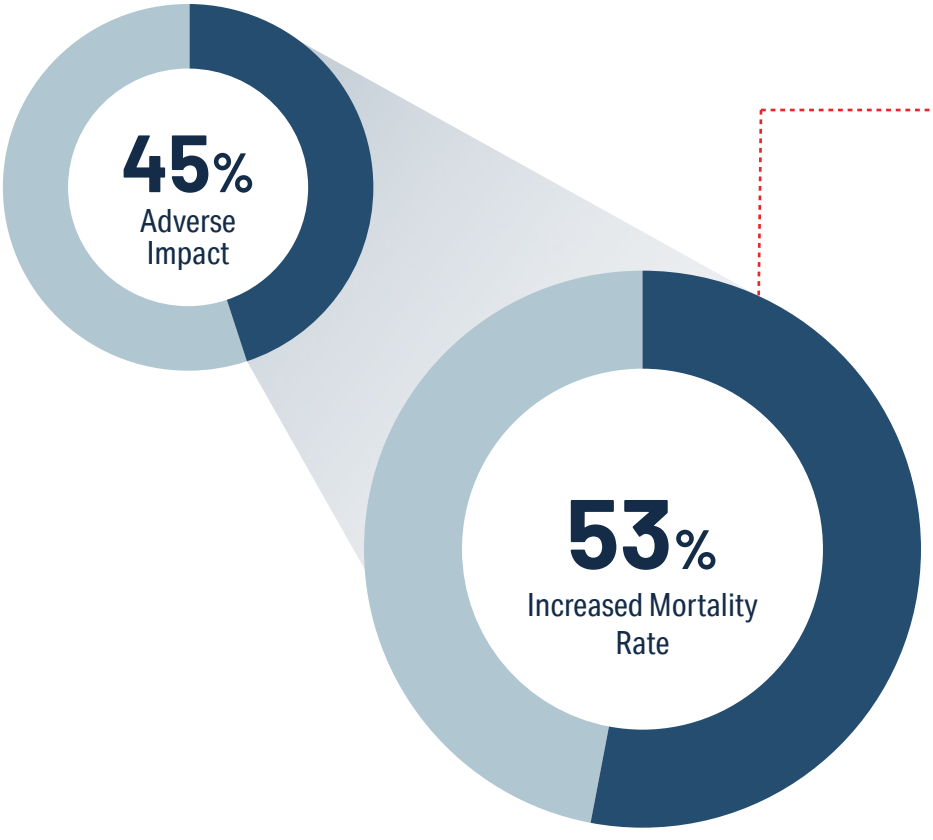


Effect of adverse events



The Overly Adverse Impact of Cyberattacks on Patient Care

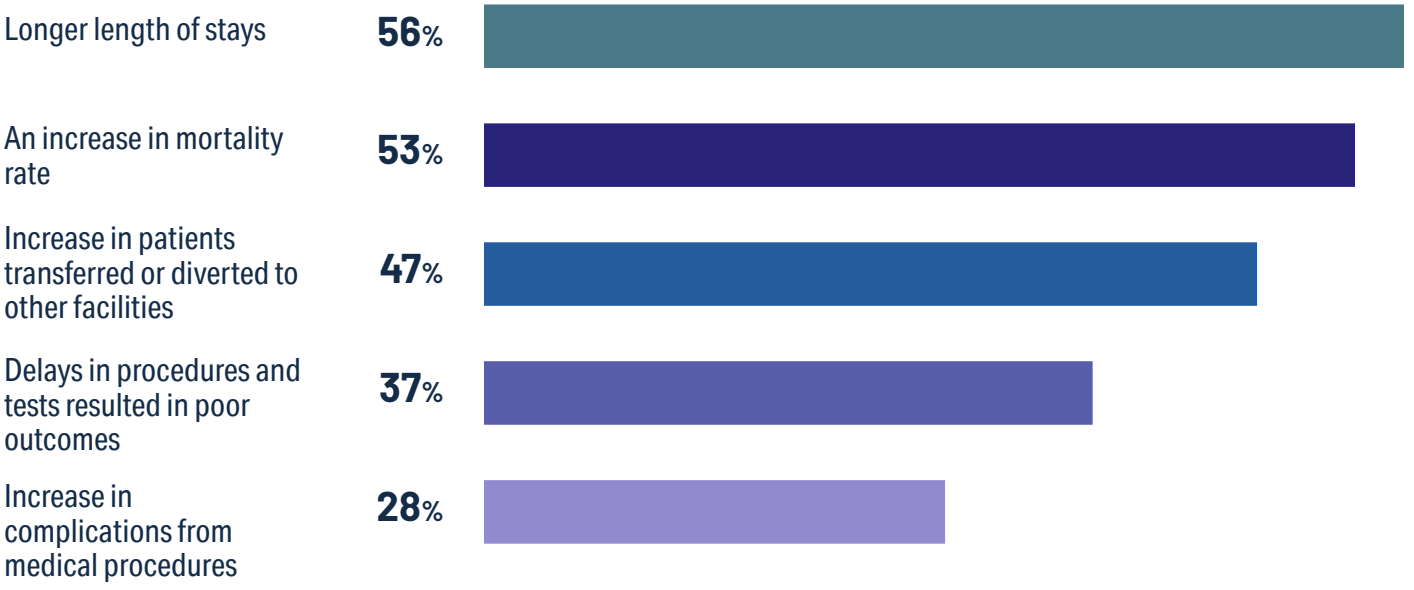
In most industries the true impact of cyberattacks is seen in financial ledgers. In healthcare the impacts are more dire, measured by increased mortality rates, health complications and a lower quality of life. There have been warnings and anecdotal examples of the impacts on patient care, but this evidence makes it clear - regardless of an attacker's motives, the collateral damage frequently involves increased mortality, more cumbersome procedures, longer stays and delayed service. The question is no longer if patients are going to die due to cyberattacks, it is how many already have and when will the industry improve protections to limit more in the future.



24%

Calculated rate of attacks that resulted in increased mortality rates due to the results of a cyberattack.

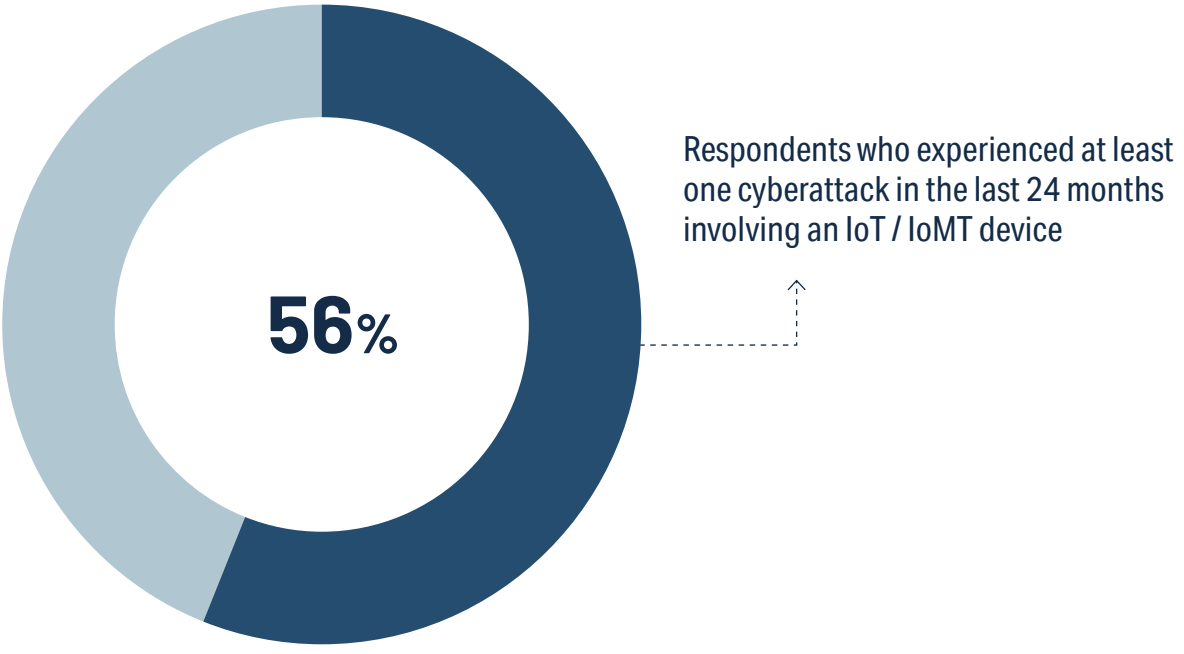
Adverse impact of a cyberattack on patient care



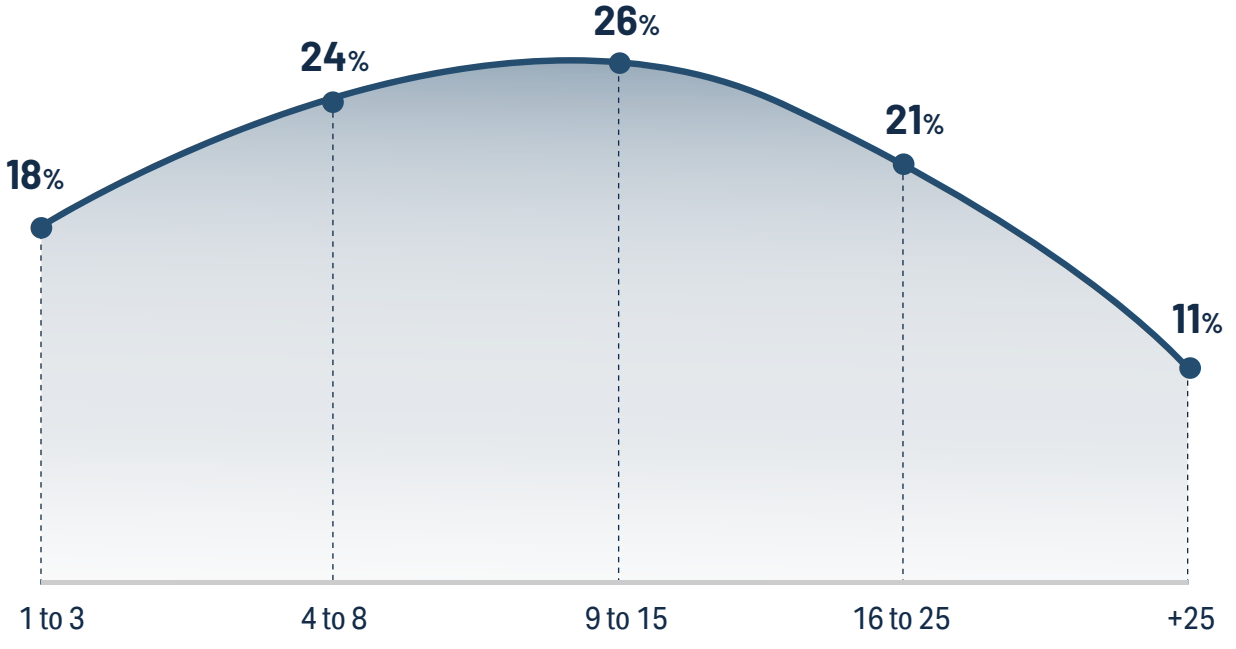
Volume and Frequency of Attacks

The Astonishing Breadth of Attacks on Healthcare

The true depth and breadth of attacks on healthcare providers has long gone undocumented. Beyond the HHS "Wall of Shame" (and its valid criticisms) there is an incredible lack of data available on the raw volume of activity that puts patients and facilities at risk. Reports detailing the $20.8 billion in annual losses faced by hospitals and exposure of 45 million patient records are known but rarely drive direct action. Respondents to this survey have provided clarity to the widespread attacks that have hit over half (56%) of their facilities in the last two years with a significantly higher than expected number of repeat attacks.



Average number of cyberattacks in last 24 months involving an IoT / IoMT device



Ransomware Payments Drive a Vicious Attack Cycle

As first reported in the September 2021 Ponemon report, ransomware attacks have been the revenue generator of choice during the COVID pandemic. This updated research shows the tremendous activity that hospitals must defend themselves against. With 76% of respondents having experienced three or more ransomware attacks on average, the reality is that incidents are not one-off cautionary tales like those at Scripps or UVM Health, but instead common occurrences with strong financial motives. Payment is often the quickest path to recovery, and was the elected option for nearly half of respondents, with the most frequent ransom amount being in the $250,000 - $500,000 range.

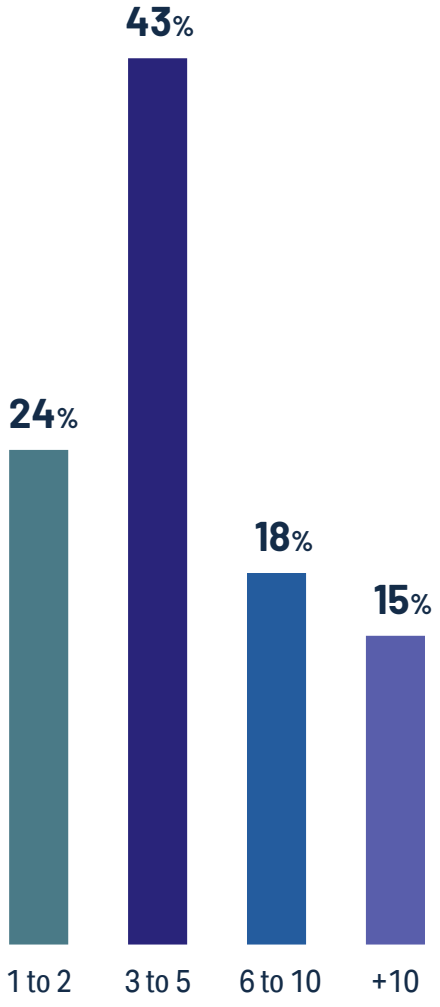
43%

of respondents have experienced at least one ransomware attack.

47%

of respondents experiencing a ransomware attack (34%) paid the demanded ransom.

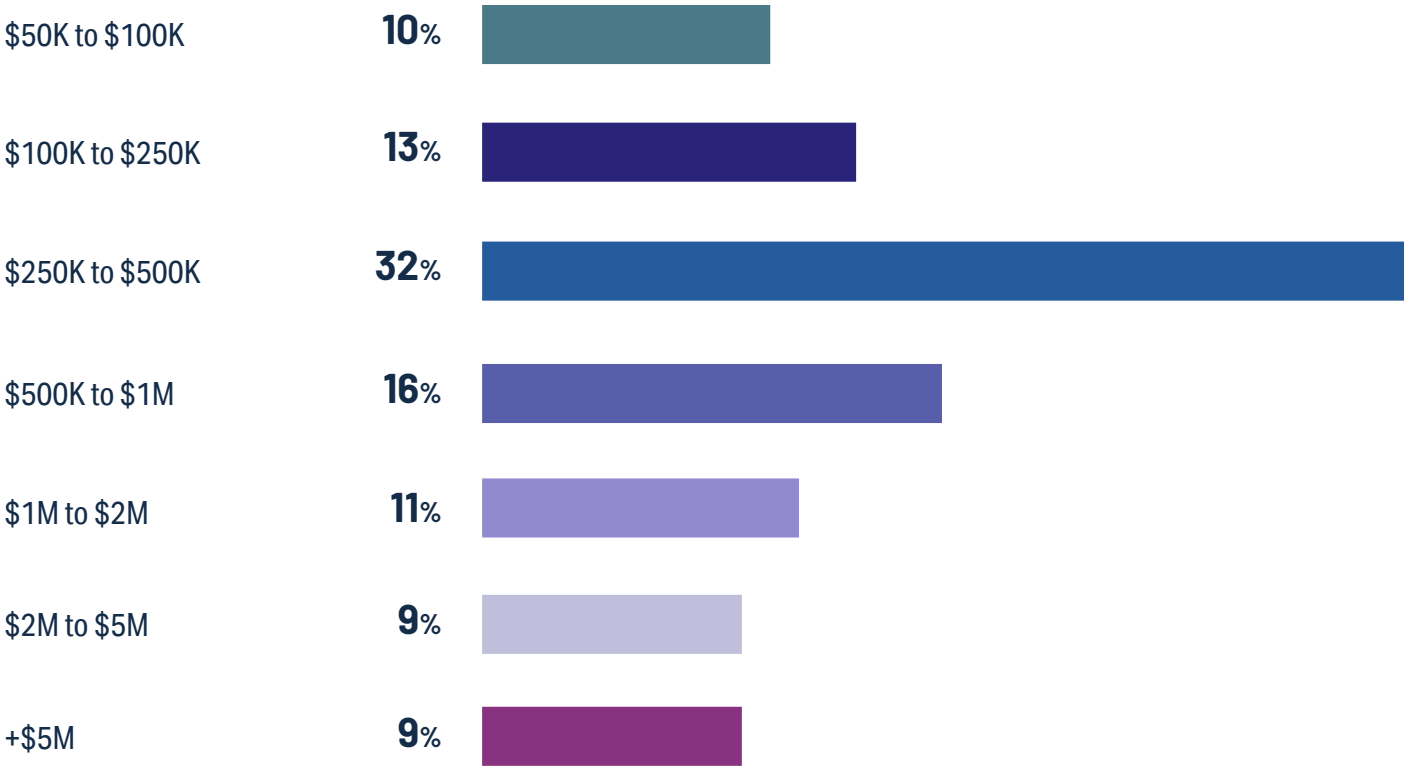
Number of ransomware incidents experienced

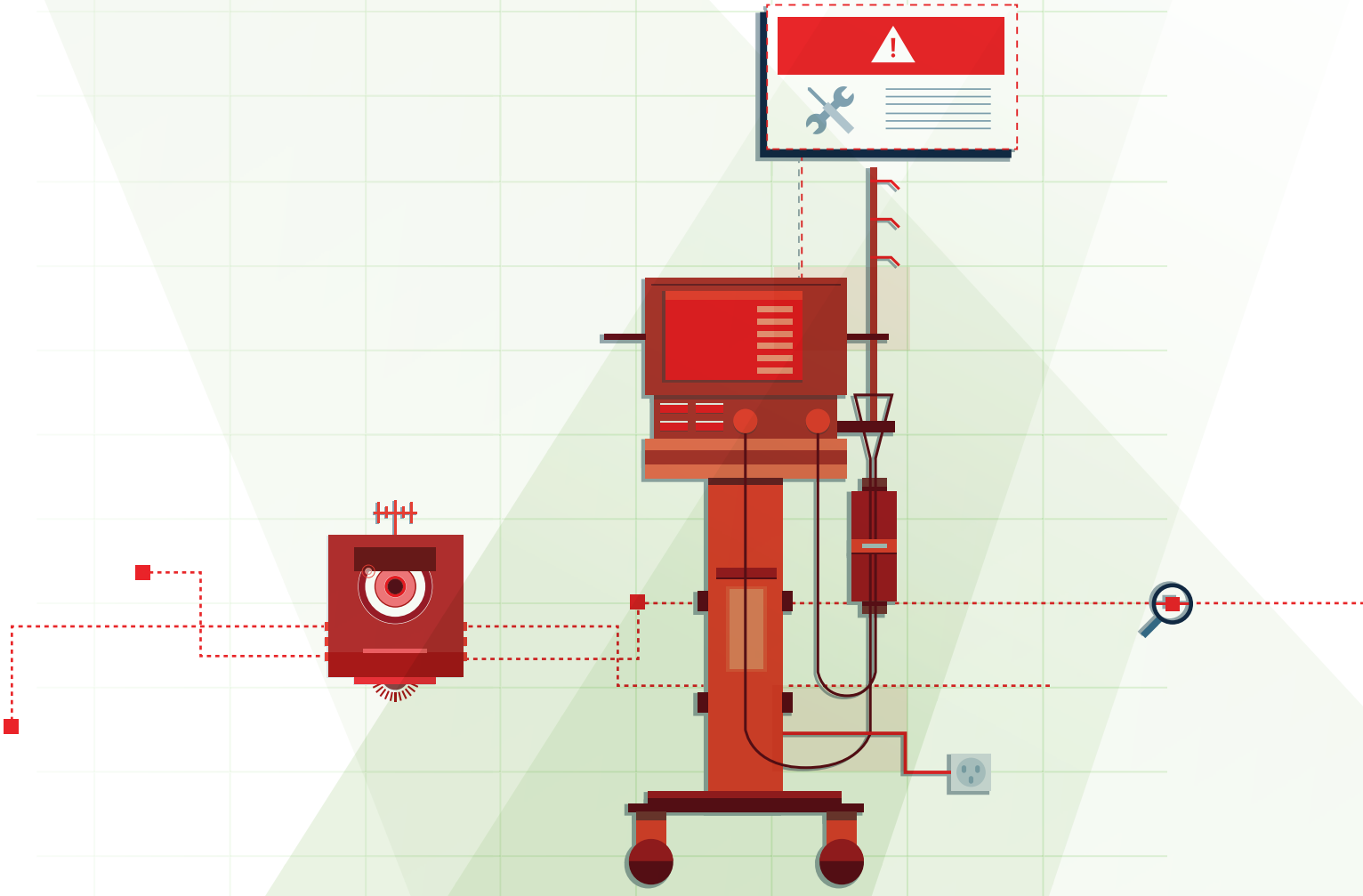


$250k – $500k:

Most common ransom paid (32%)

Total bitcoin or other currency demanded for ransom

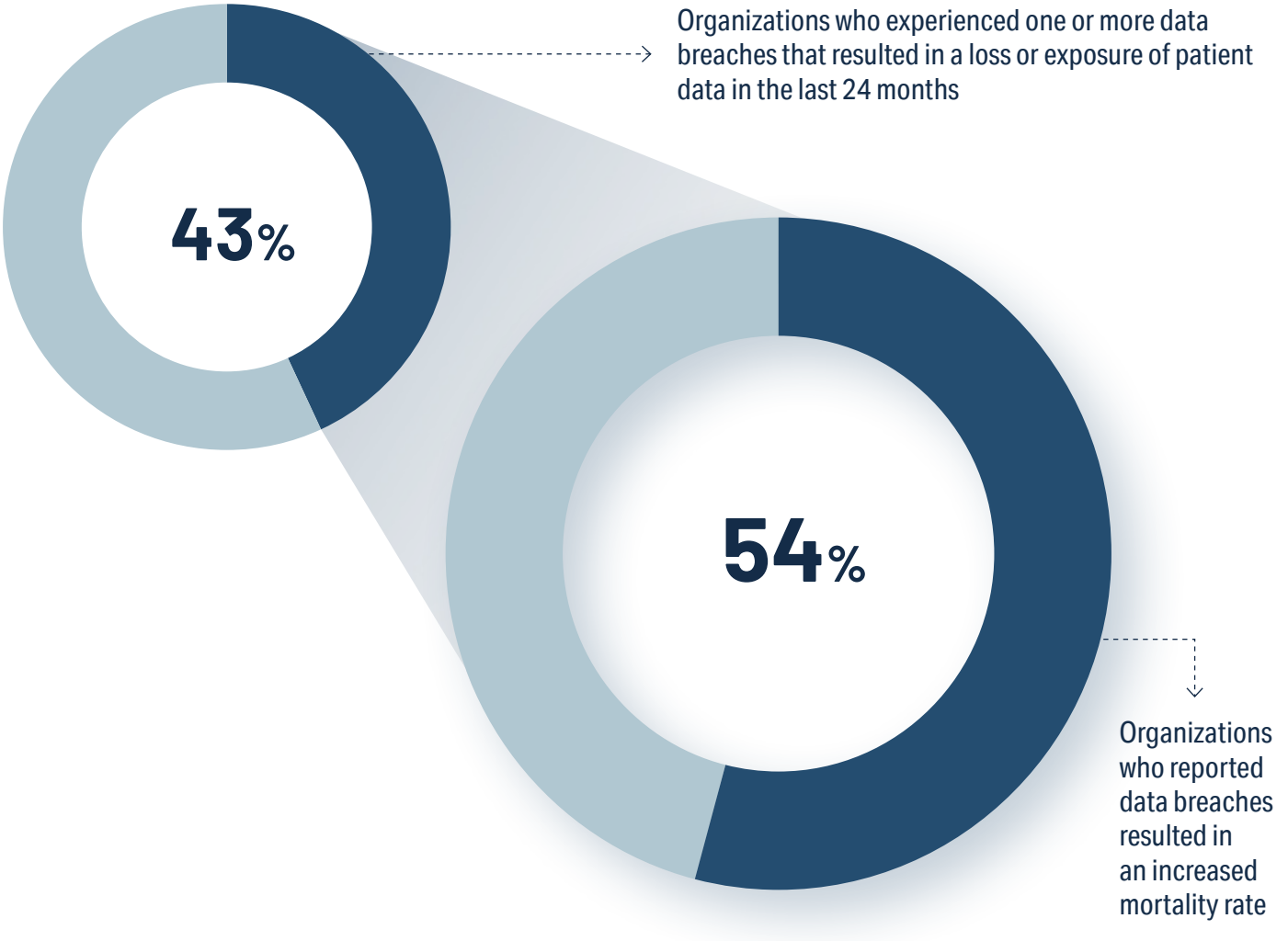




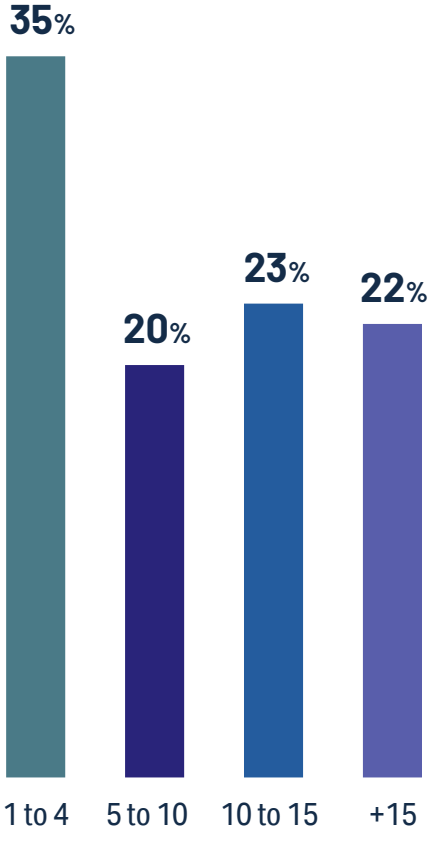
Attack Impacts Extend Well Beyond Data Breaches

Financial Fines Don't Provide Sufficient Motivation

The 2009 HITECH Act created a strict system of financial penalties for exposing patient records and provided the primary motivation for improving cybersecurity practices in most healthcare facilities. This study makes it clear that the deeper concern of patient care and protection should now be considered an equally important driver. Of the 43% of organizations that reported at least one data breach in the last 24 months. 88% report at least one IoT / IoMT device contributing to the breach.



Number of breaches experienced



88%

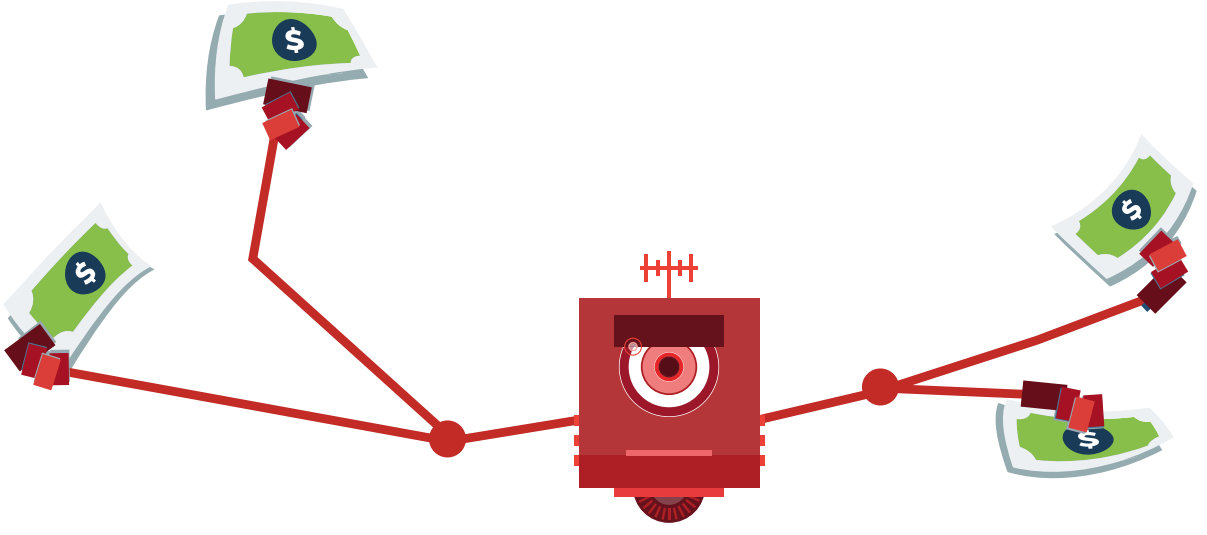
of these data breaches involved at least one IoT / IoMT device

$1M–$5M

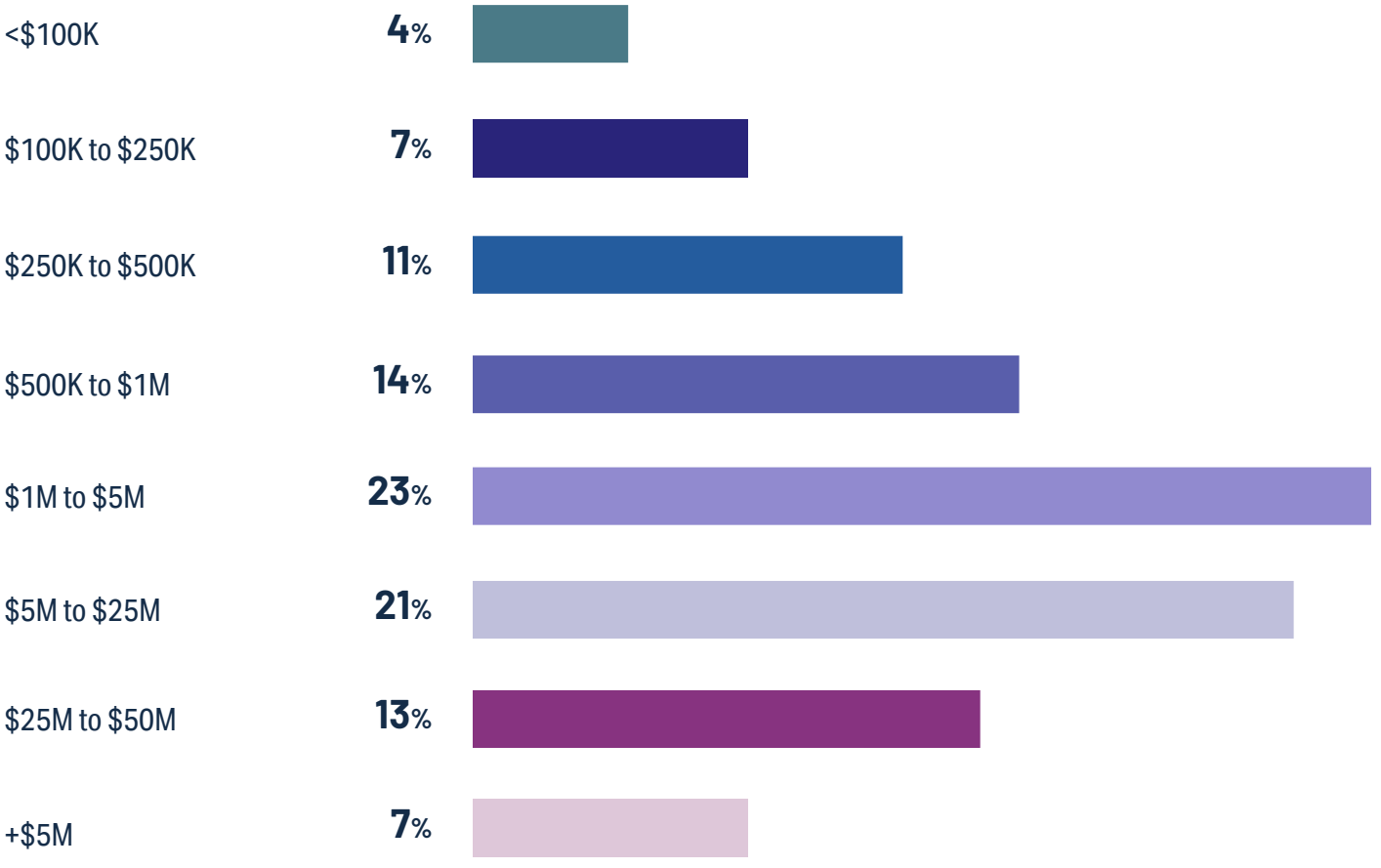
Most Common Total Cost of Largest Data Breach Experienced

$13M

Average total estimated cost of largest data breach



Total cost of the largest data breach involving IoMT or other connected devices



IoT/IoMT Devices Present Unique Security Challenges

The Gap between High Awareness and Disappointing Action on Healthcare IoT Security

Nearly every interview or survey involving healthcare professionals refers to cybersecurity being a top priority for their organization, with IoT/IoMT devices often being referenced. This survey is no different, with seven out of ten respondents (71%) believing that very high security risks are created by these otherwise overwhelmingly beneficial marvels of modern medicine.

While this recognition of risk is a step in the right direction, it is unfortunately more of a talking point than one of action. Over half (54%) of respondents did not report senior management requiring assurances of properly addressed IoT/IoMT device risk. Even more concerning, two thirds (67%) don't believe their devices are being patched in a timely manner - the most basic, widely-accepted and often required action for nearly any healthcare environment.

While recognition and discussion of these challenges is a positive leading indicator, the woeful inaction after the words have been spoken is as disappointing as it is discouraging.

The Known Risks

72% Report a high level of urgency in securing IoT/IoMT devices

71% Believe IoT/IoMT devices create a very high security risk

54% Report senior management does not require assurances that IoT/IoMT risk is being properly addressed

49% Organizations who do not measure the effectiveness of IoT/IoMT security practices

33% Report high or very high confidence in timely IoT/IoMT device patching

But Lacking Action

Unclear Ownership and Accountability Drive Inactivity

Neither Seeing Nor Securing

Despite demonstrations of remote attacks on medical devices as early as 2011, it wasn't until the recent increase in ransomware attacks rooted in these devices that organizations took the threats seriously. The result is a disproportionately small number of respondents viewing their device security initiatives in a state described as mature. Of the 46% who performed well known and accepted procedures such as scanning for devices, only 33% of these respondents keep an inventory of the devices that were discovered. In an industry where "you can't secure what you can't see" is quickly becoming considered as an outdated security strategy, it is disappointing that so few are even attempting to track what they see.

79%

Do not consider their IoT/IoMT cybersecurity activities to be mature

67%

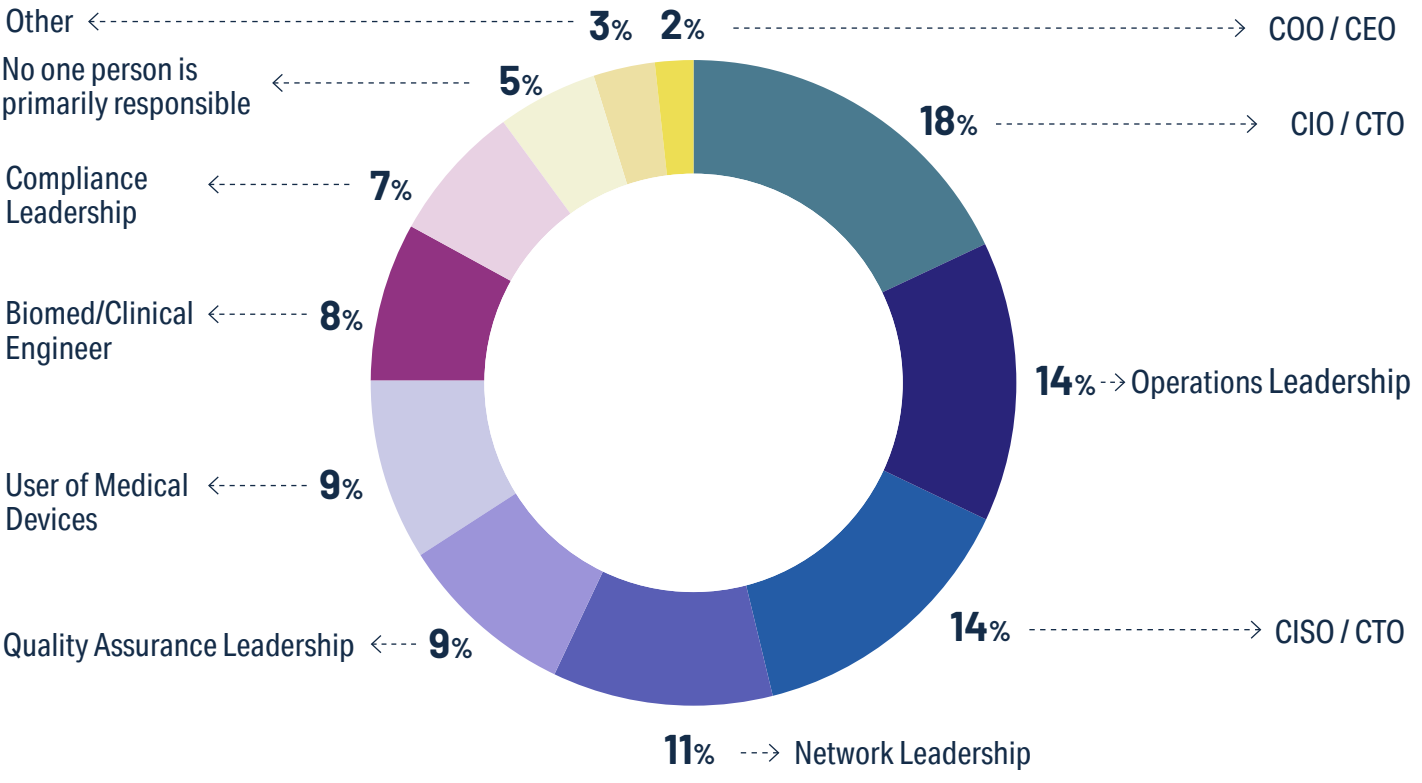
Rate of organizations that do not keep an inventory of the IoT/IoMT devices that they scan

Maturity of an organization's IoT/IoMT cybersecurity activities

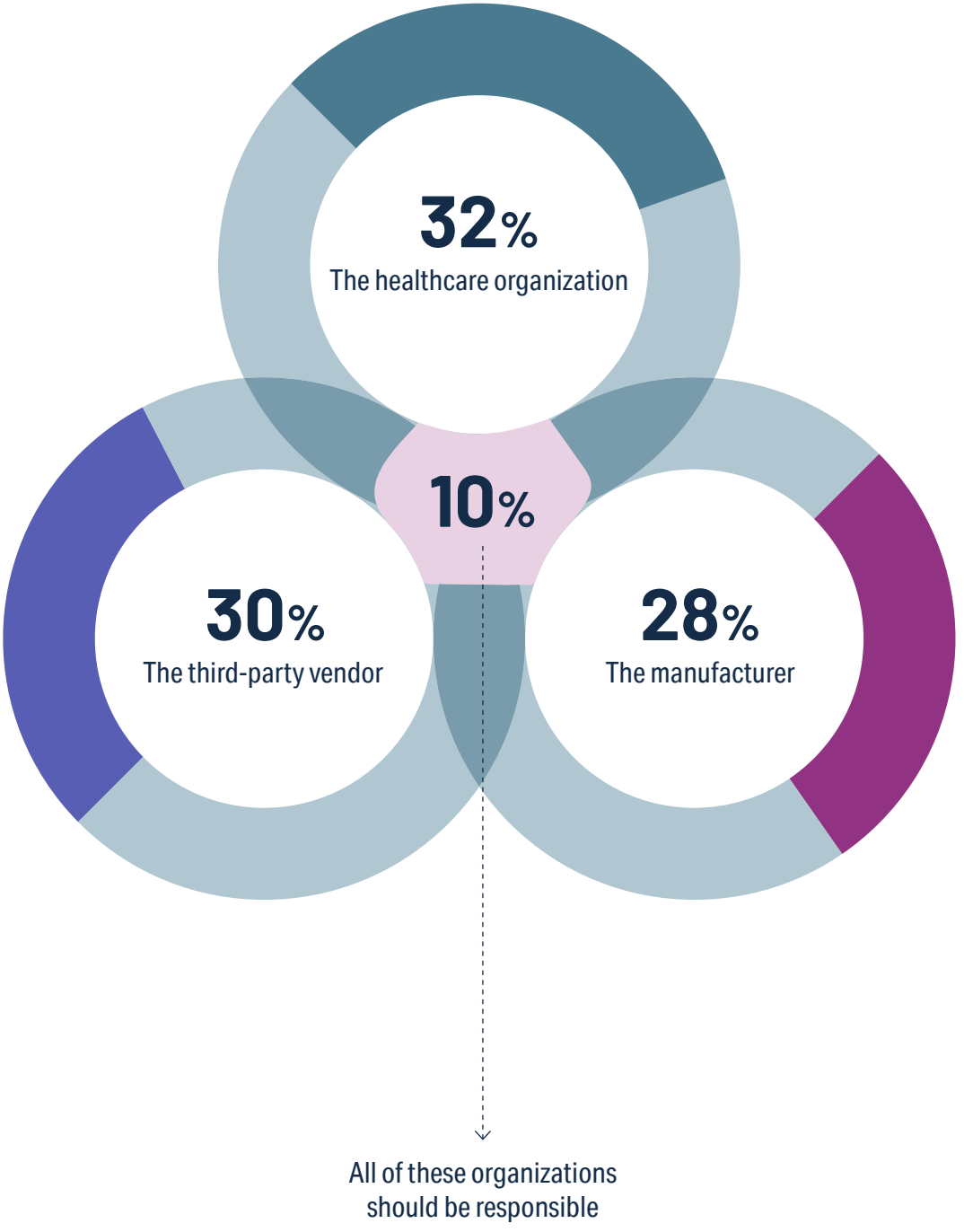
Waiting For Everyone Else to Secure Healthcare IoT First

In an industry where structure and responsibility is a key component of most departments, the lack of clear ownership stands out even more regarding IoT/IoMT security. Not only are there no clearly agreed upon stakeholders for protecting the thousands of connected devices in most environments, but the list hits numerous departments from BioMedical Engineers to CEOs and nearly everyone in between. Given that many of these devices are nearly a decade old, it is clear that better practices regarding ownership and responsibility need to be better defined and implemented.

Party most responsible for IoT/IoMT device security in your organization



Organization most responsible for IoT/IoMT device security



Security Investment Does Not Reflect Gravity of Risk

Securing The Bare Minimum

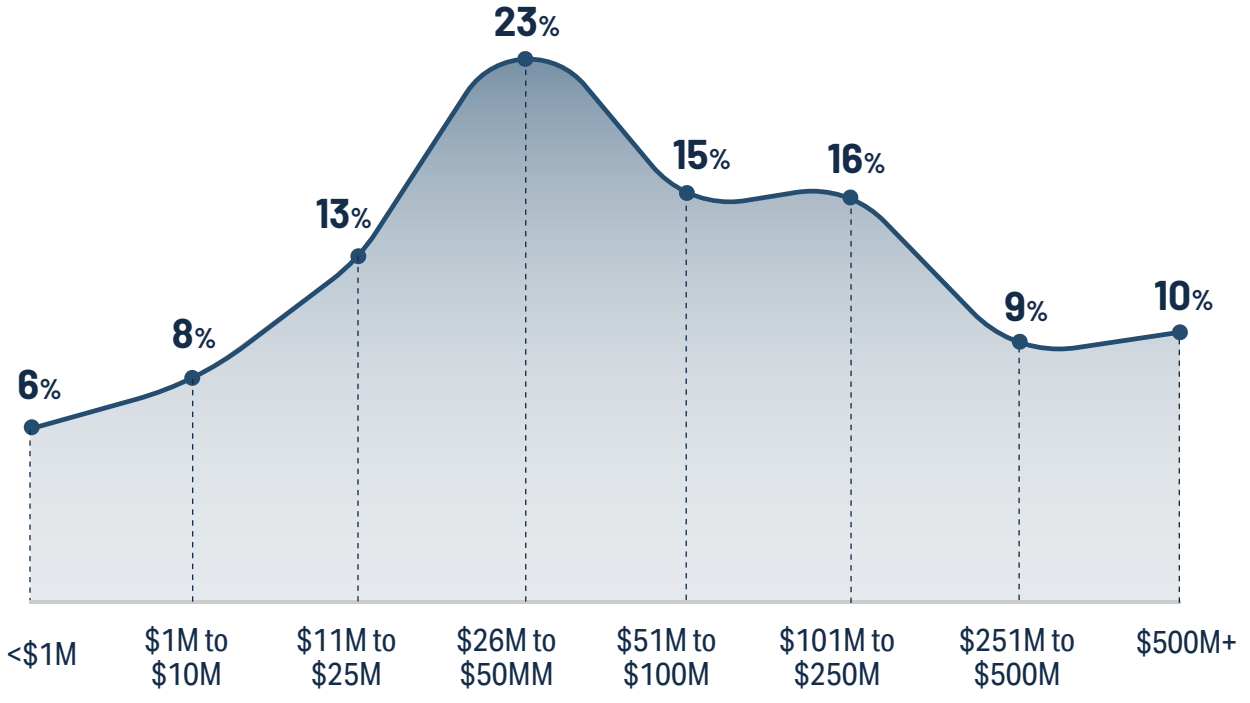
The challenges with finding resources is not new to healthcare. There is never enough budget, headcount or expertise to address the myriad challenges they face. Furthermore, the desire for spend to overwhelmingly favor patient care is understandable. After all, every dollar saved on IT or security spend is a dollar that can be used to treat a patient.

With that in mind, IT activities are often budgeted for depending on how they improve care in some measurable way. Spending on IoT/IoMT device security is no different- all respondents reported spending some amount on the activity, but that amount varied widely from under $100,000 to several reports of spending an astounding $10 million or more. Given the varying number of factors to consider in such spending, one data point stood clear - a typical respondent reported spending 3.4% of their overall IT budget on security IoT/IoMT devices. While this is clearly not sufficient, particularly when considering that these devices often make up half of the device volume in a hospital, it does give the low bar that providers should at least be hitting when investing in their IoT/IoMT security practices.

$26M – $50M

Typical IT budget of respondents

IT budget of respondents



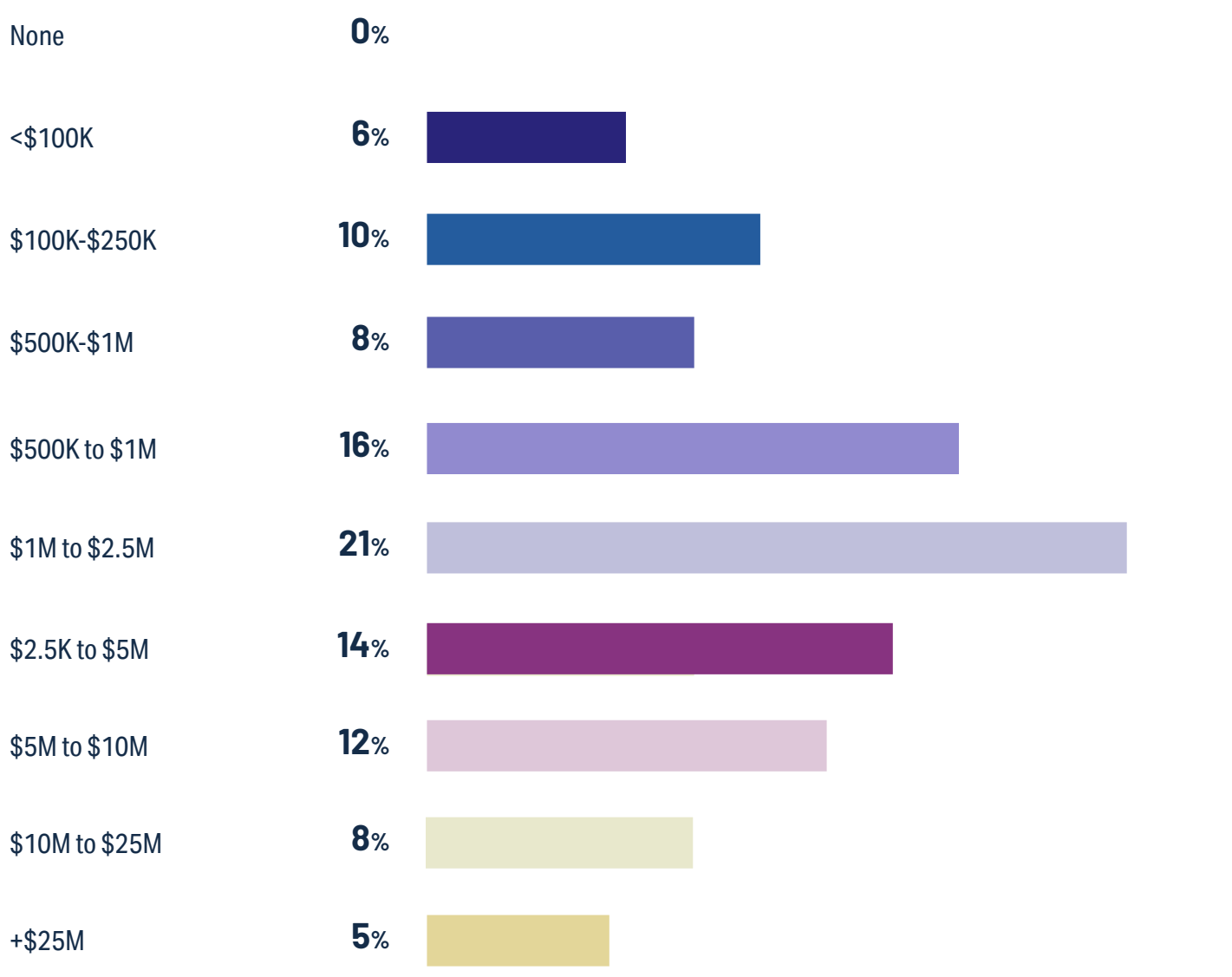
$5M

Reported spend focused on IoT/IoMT device security

3.4%

Reported amount of IT budget focused on IoT/ IoMT device security

Annual organizational spend on IoT/IoMT device security



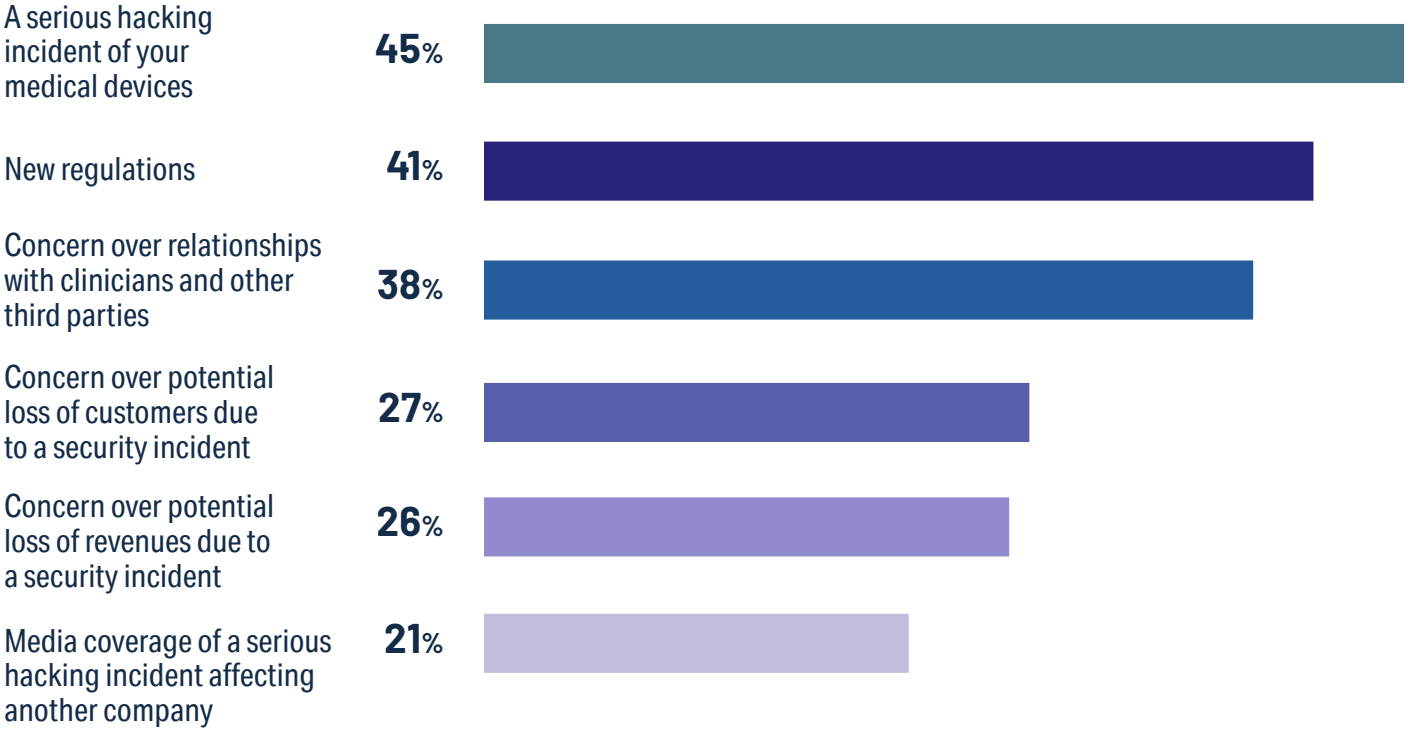
The IoT/ IoMT spending funnel

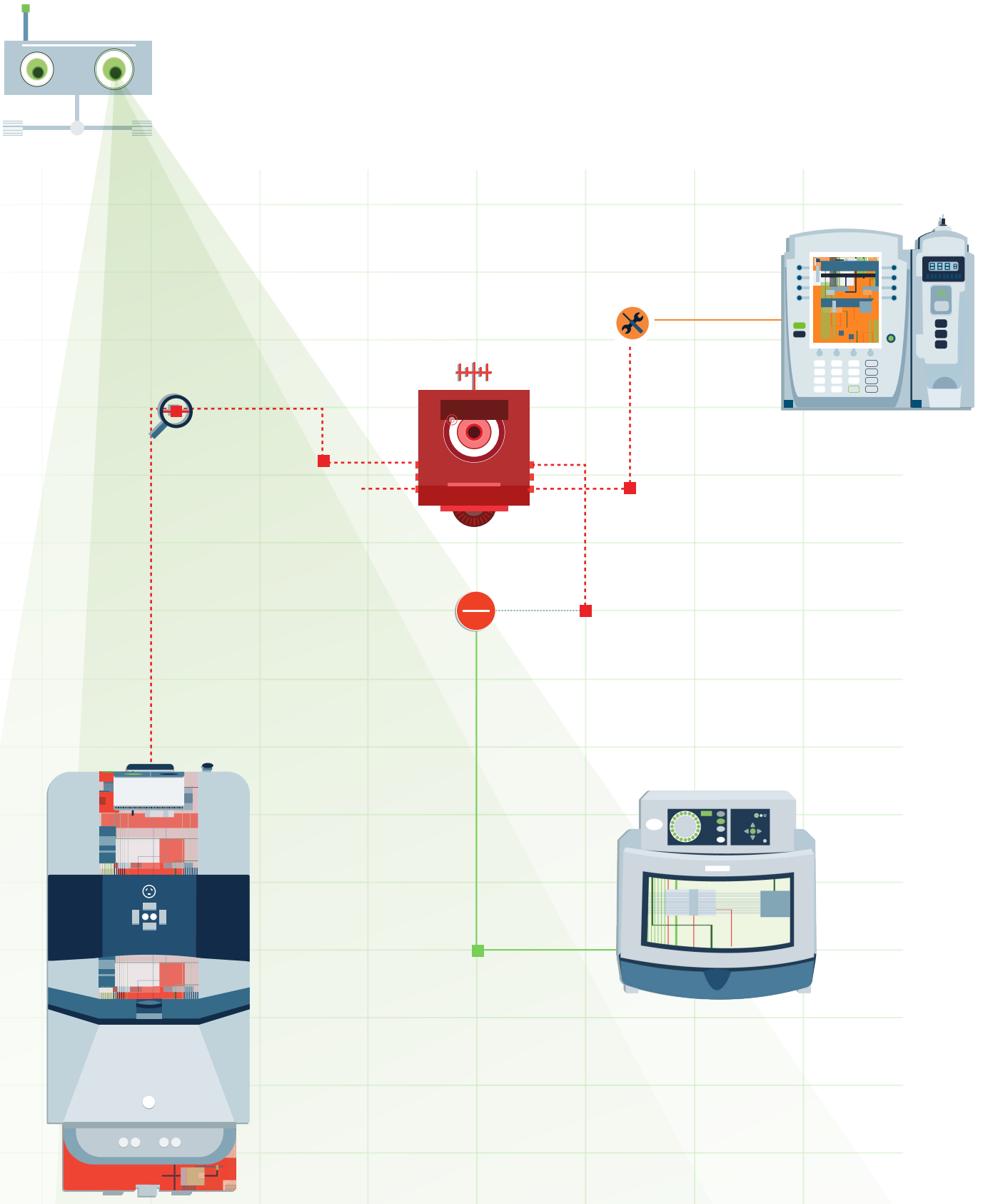
Average Fiscal Year IT Budget **$145M**

17% Amount of IT Budget Spent on Security **$25M**

20% Amount of Security Spent on IoT / IoMT **$5M**

Factors that would influence an organization to increase IoT/IoMT cybersecurity budget





The Healthcare IoT Security Crisis Point Has Already Arrived

What does the healthcare industry do with this information? Many had hoped that the recent rise in ransomware and other cyberattacks had impacts that were overwhelmingly financial. Anecdotal evidence of compromised care due to cyberattacks have occasionally made headlines, but they were infrequent enough to provide a false sense of security that often comes from a "safety in numbers" approach. The 500+ healthcare leaders that responded to this survey have painted a different picture. Widespread, repeated attacks. Desperation driving negotiations with cyber criminals. Confused ownership and responsibility. Losses measured in both lives and dollars.

As with all new threats, there is rarely one magic bullet that will prevent all damage, but there is emerging guidance that can be used to inform action. On average 3.4% of IT budgets are spent securing devices. Treat this as a floor for how resources should be allocated. 67% of respondents do not have high confidence in the patch management processes for IoT/IoMT devices, one of the most basic procedures required. New approaches must be investigated that scale all aspects of securing these devices - automated inventory, discovery of unmanaged devices, improved defense in depth at the device, network and environment levels, and a clear understanding of who owns responsibility, action and accountability for the widespread medical marvels of IoT/IoMT to ensure devices are not doing more harm than good.

Fortunately, cybercriminals are not the only parties with technical expertise and resources. To combat the lack of security expertise throughout healthcare, Managed Security Service Providers (MSSPs) are rapidly introducing new offerings. Grassroots movements like I Am The Cavalry are investigating and educating healthcare leaders,

politicians and private industry on the threats they face. Research organizations including Ponemon Institute are focusing increasing efforts on collecting and reporting on data that will help improve care for every patient at some point in their life.

Finally, technology companies like Cynerio are recruiting team members from industries with notably higher cybersecurity expertise (Investment Banking, Insurance, Military) and redirecting their efforts to protecting healthcare facilities and the patients they treat.

At the end of the day, increased attacks on healthcare environments are driven by opportunity and further fueled by relative inactivity. Media coverage routinely ignores attacks and instead points to oil pipelines when demonstrating what might go wrong. Regulators introduce legislation such as the PATCH act to great fanfare, but forgo the difficult details in providing training, focus and funding that will be necessary for notable improvements. Analysts focus on the digital impact of cyberattacks with woefully few desperately ringing the bell to warn of cyber-physical gaps being crossed. Unintended consequences like the HHS Wall of Shame provide fuel for attackers and discredit overstressed healthcare systems in the name of patient safety. Finally, cybersecurity vendors have designed systems intended to protect the revenues of investment banks and technology companies which they then wedge into healthcare environments with mediocre success at best.

Our teams hope this report helps inform discussion, impact change and ultimately protect patients. We fear it may not.

About Ponemon Institute

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations. Ponemon Institute upholds strict data confidentiality, privacy and ethical research standards, and does not collect any personally identifiable information from individuals (or company identifiable information in business research). Furthermore, strict quality standards ensure that subjects are not asked extraneous, irrelevant or improper questions. To learn more visit **https://www.ponemon.org/**

About Cynerio

Cynerio is the one-stop shop Healthcare IoT security platform. With solutions that cater to healthcare's every IoT need – from Enterprise IoT to OT and IoMT – we promote cross-organizational alignment and provide hospitals the control, foresight, and adaptability they require to stay cyber-secure in a constantly evolving threatscape. We empower healthcare organizations to stay compliant and proactively manage every connection on their own terms with real-time IoT attack detection and response and rapid risk reduction tools, so that they can focus on healthcare's top priority: delivering quality patient care. Learn more about Cynerio at **cynerio.com** or follow us on Twitter **@cynerio** and **LinkedIn**.

Cynerio Ponemon INSTITUTE

Appendix A: Ponemon Institute Methodology

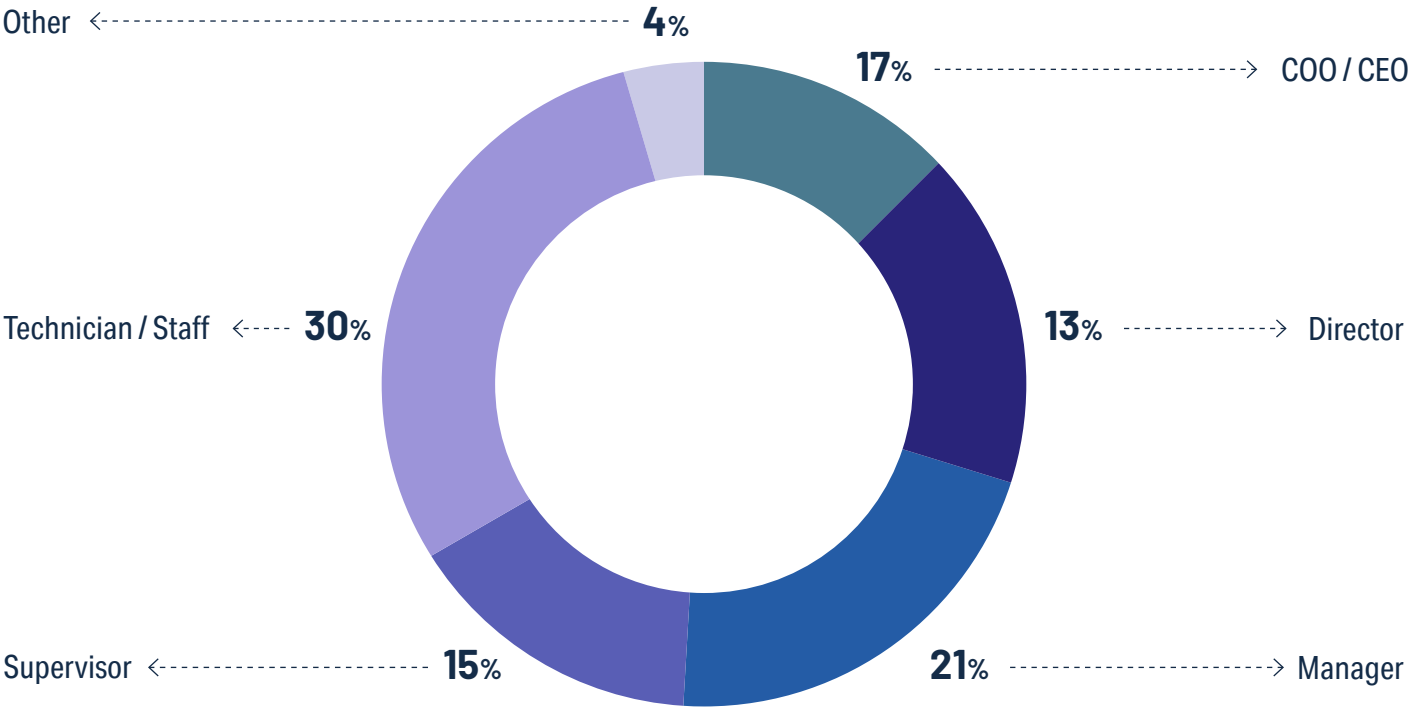
Methodology

A sampling frame of 13,455 healthcare experts in leadership positions within hospitals and healthcare systems throughout the United States were selected as participants to this survey. Table 1 shows 560 total returns. Screening and reliability checks required the removal of 43 surveys. Our final sample consisted of 517 surveys or a 3.8 percent response.

Table 1. Sample response	Freq	PCT%
Sampling frame	13,455	100.0%
Total returns	560	4.2%
Rejected or screened surveys	43	0.3%
Final sample	517	3.8%

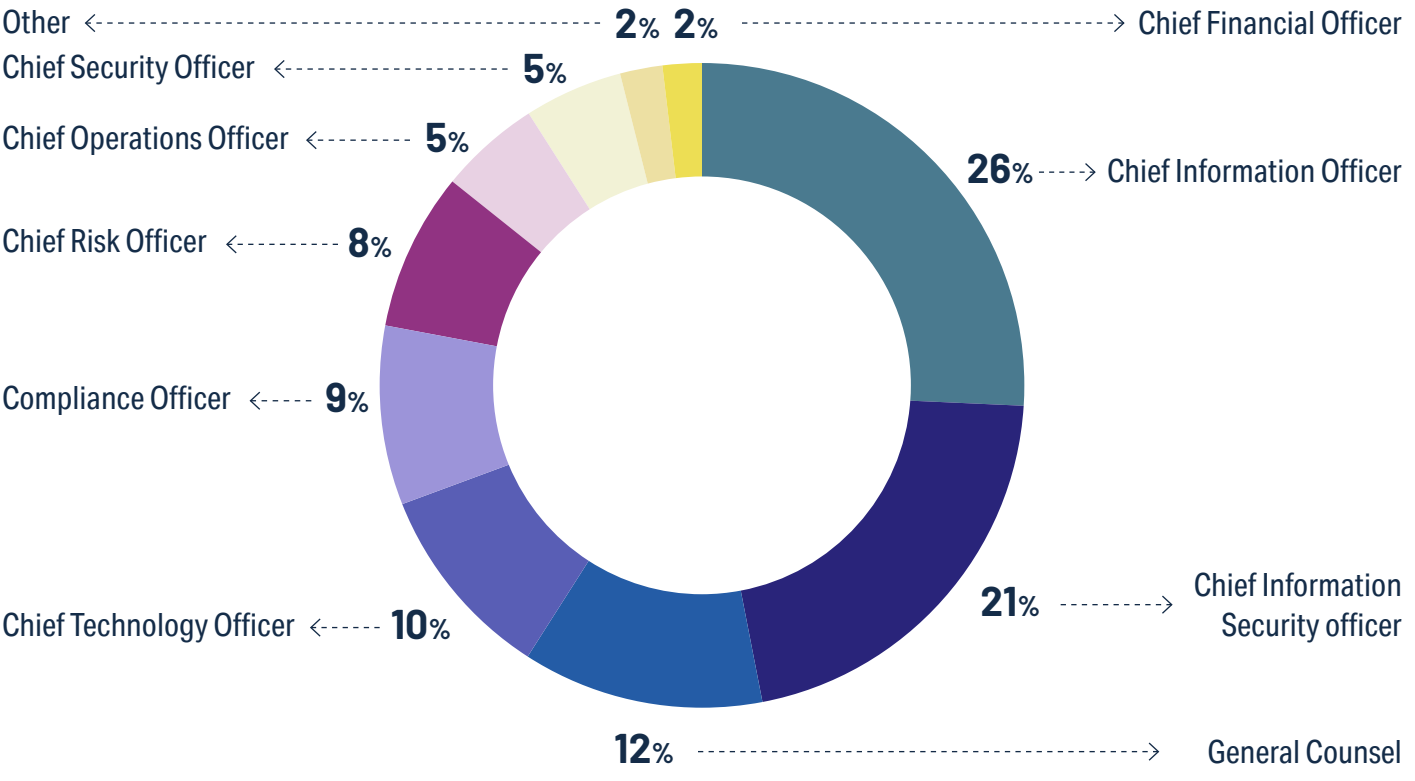
Pie chart 1 reports the respondent's position level within participating organizations. By design, more than half (66 percent) of respondents are at or above the supervisory levels. The largest category at 30 percent of respondents is technician or staff.

Pie chart 1. Current position within the organization



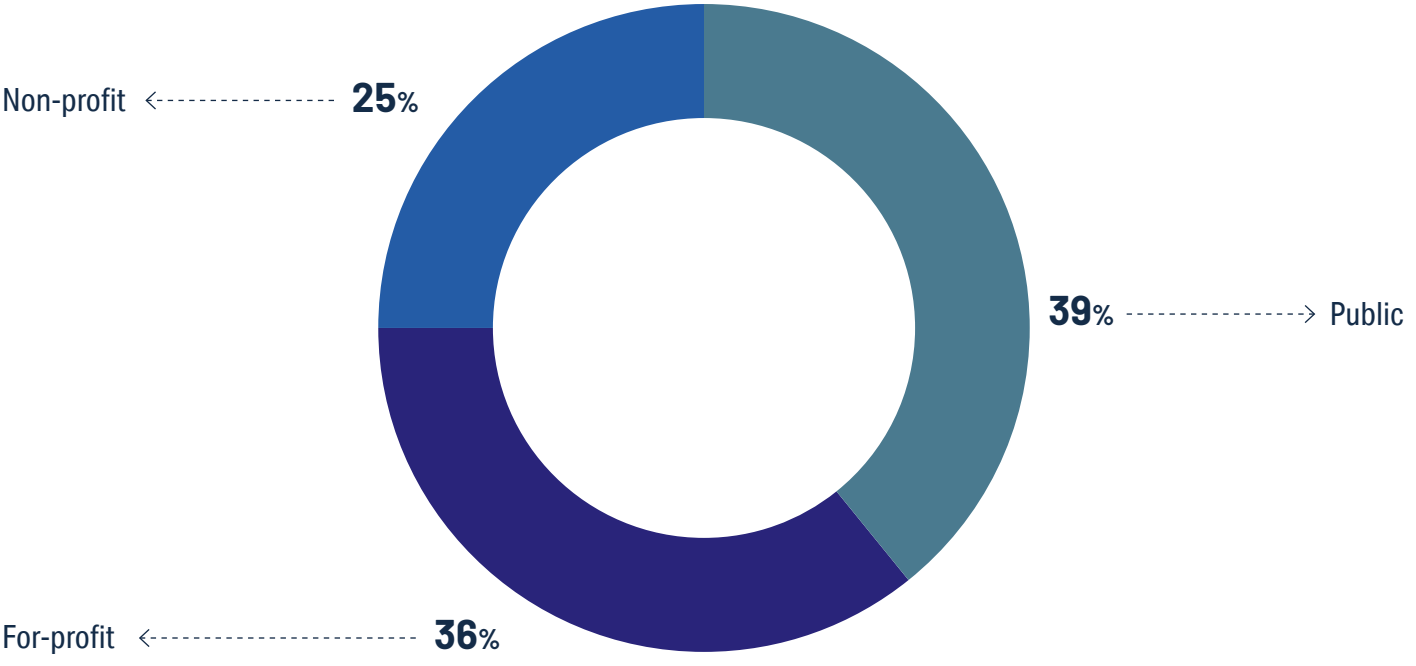
As shown in Pie chart 2, 26 percent of respondents report to the chief information officer, 21 percent of respondents report to the general council, 10 percent of respondents report to the chief technology officer and 9 percent of respondents report to the compliance officer.

Pie chart 2. Direct reporting channel



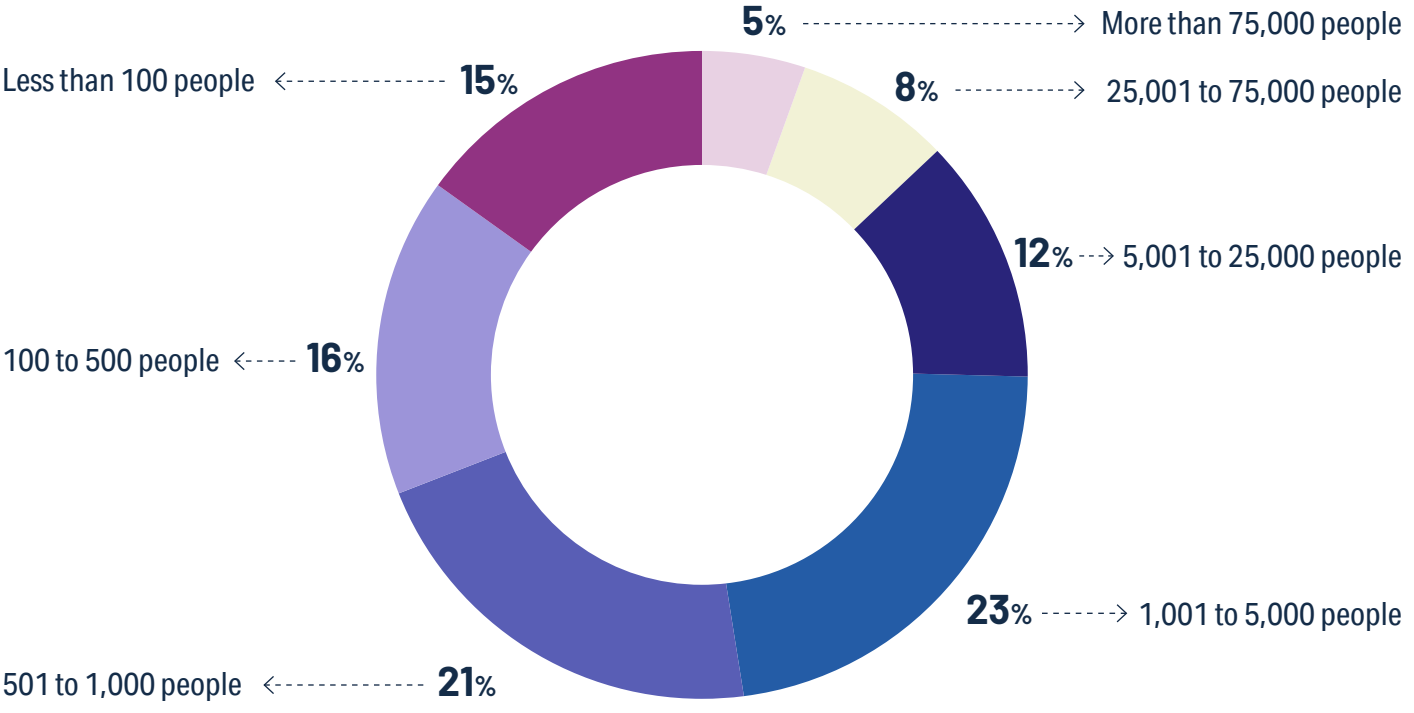
Pie chart 3 reports the funding structure of respondents' organizations. This chart identifies public funding structure (39 percent) as the largest funding structure. This is followed by for-profit structure (36 percent of respondents), and non-profit funding structure (25 percent of respondents).

Pie chart 3. Funding structure of the organization



As shown in Figure 24, almost half (48 percent) of respondents are from organizations with a global headcount of more than 1,000 employees.

Pie chart 4. Headcount of respondents' organization



Appendix B: Caveats To This Study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of healthcare experts in leadership positions in the United States. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix C: Detailed Audited Findings

The following tables provide the percentage frequency of responses to all survey questions. All survey responses were captured in June 2022

Survey Response	Freq
Total sampling plan	13455
Total survey returns	560
Total rejected survey	43
Final sample	517
Response rate	3.8%

Part 1. Screening

S1a. Do you have any role or involvement in contributing to or assessing the security of IoMT/IoT devices in your organization?	Pct%
Yes, significant involvement	47%
Yes, some involvement	34%
Yes, minimal involvement	19%
No involvement (Stop)	0%
Total	100%

S1b. What best describes your healthcare organization?	Pct%
Hospital	33%
Clinic	12%
Healthcare service provider	21%
Healthcare system	34%
None of the above (Stop)	0%
Total	100%

S1c. How many beds does your healthcare organization have?	Pct%
Less than 200 beds (stop)	17%
201 beds to 500 beds	20%
501 beds to 1,000 beds	31%
More than 1,000 beds	32%
No beds (stop)	0%
Total	100%

S1d. What best describes your position?	Pct%
IT leadership (CIO, etc.)	12%
IT or networking director	7%
IT or networking manager	6%
Information security leadership (CISO, VP)	20%
IT security director	15%
IT security manager	11%
Clinical/biomedical engineering leadership	9%
Clinical/biomedical engineering director	7%
Medical informatics leadership (CMIO, VP, etc.)	9%
Operations or facilities leadership	4%
None of the above (stop)	0%
Total	100%

Part 2. Background on IoMT/ IoT devices in healthcare

Q1. What best describes the maturity of your organization's cybersecurity IoMT/ IoT activities?	Pct%
Early stage – many activities have not been planned or deployed. Response to cybersecurity issues is reactive and ad hoc. Staffing and budget resources have not been allocated to IoT security activities.	22%
Middle stage – Cybersecurity activities are planned and defined but only partially deployed. Staffing and budget resources are inadequate to support these activities.	35%
Late-middle stage – Cybersecurity activities are deployed across the enterprise. The program has C-level support and adequate budget.	22%
Mature stage – Cybersecurity activities are fully deployed and maintained across the enterprise. C-level executives and board are regularly informed about the effectiveness of the program.	21%
Total	100%

Q2a. Do you currently use technologies to scan and identify IoMT/IoT devices in your organization?

	Pct%
Yes	46%
No (please skip to 3a)	54%
Total	100%

Q2b. If yes, does your organization keep an inventory of these devices?

	Pct%
Yes	33%
No (please skip to Q3a)	67%
Total	100%

Q2c. If yes, approximately how many of these devices are in the inventory?	Pct%
Less than 500	4%
500 to 1,000	6%
1,001 to 2,500	10%
2,501 to 5,000	9%
5,001 to 10,000	18%
10,001 to 25,000	23%
25,001 to 50,000	16%
50,001 to 100,000	9%
More than 100,000	5%
Total	100%
Extrapolated value	24,701

Q3a. How many of the IT staff are dedicated to IT security?

	Pct%
1 to 2	5%
3 to 5	11%
6 to 10	23%
11 to 15	32%
More than 15	29%
Total	100%
Extrapolated value	12.3

Q3b. How many of the IT security staff are responsible for ensuring the security of IoMT/ IoT devices?

	Pct%
None	5%
1 to 2	12%
3 to 4	25%
5 to 6	24%
6 to 7	21%
More than 7	13%
Total	100%
Extrapolated value	4.78

Q4. In your organization, who is most responsible for ensuring the security of IoMT/ IoT devices? Please select one choice only.

	Pct%
CIO/CTO	18%
CISO/CSO	14%
COO/CEO	2%
Quality assurance leadership	9%
Compliance leadership	7%
Operations leadership	14%
Network leadership	11%
Biomed/clinical engineer	8%
User of medical devices	9%
No one person is primarily responsible	5%
Other (please specify)	3%
Total	100%

Q5. Which organization should be responsible for the security of IoMT/IoT devices? Please select one choice only.

	Pct%
The manufacturer	28%
The third-party vendor	30%
The healthcare organization	32%
All of these organizations should be responsible	10%
Total	100%

Part 2. Data breaches, cyberattacks and threats

Q6. What are the top threats to medical IoT and other connected devices in your organization? Please select only four responses.	Pct%
Lack of visibility into IoT networks	45%
Phishing	45%
Zero-day attacks	41%
Ransomware attacks	39%
Web-borne malware attacks	33%
Account takeovers/credential theft	32%
DDoS attacks	32%
IT system failure	28%
Advanced persistent threats	27%
Malicious insider	23%
Botnet attacks	20%
Negligent insider	18%
Natural disasters such as flooding or hurricanes	15%
Other (please specify)	2%
Total	400%

Q7. Does your organization follow guidance from the following to reduce cybersecurity risks to IoMT/IoT devices? Please select all that apply.

	Pct%
Federal Drug Administration (FDA)	56%
National Institute of Standards & Technology (NIST)	43%
Canadian Standards Association (CSA)	13%
Cybersecurity and Infrastructure Security Agency (CISA)	26%
Device manufactures	35%
Other (please specify)	3%
Total	176%

Q8a. Did your organization experience one or more cyberattacks in the past 24 months involving an IoMT/IoT device?

	Pct%
Yes	56%
No (please skip to Q12a)	44%
Total	100%

Q8b. If yes, how many cyberattacks involving these devices did your organization have in the past 24 months?

	Pct%
1 to 3	18%
4 to 8	24%
9 to 15	26%
16 to 25	21%
More than 25	11%
Total	100%
Extrapolated value	12.5

Q8c. If yes, approximately, how much was the total cost of the largest cyberattack involving these devices? Please note that the cost estimate should include all direct cash outlays, direct labor expenditures, indirect labor costs, overhead costs and lost business opportunities.

	Pct%
Less than $100,000	4%
$100,000 to $250,000	7%
$250,001 to $500,000	9%
$500,001 to $1,000,000	19%
$1,000,001 to $5,000,000	24%
$5,000,001 to $25,000,000	18%
$25,000,001 to $50,000,000	12%
More than $50,000,000	7%
Total	100%
Extrapolated value	$ 12,306,000

Q9. What best describes the type of the largest cyberattack? Please select only two top choices.

	Pct%
Account takeovers/credential theft	30%
Advanced persistent threat	31%
Botnet attack	17%
DDoS attack	23%
IT system failure	19%
Phishing	14%
Web-borne malware attacks	34%
Zero-day attacks	30%
Other (please specify)	2%
Total	200%

Q10. What were the consequences of the cyberattack? Please select all that apply.	Pct%
Exposed patient data	53%
Exposed financial and payment data	29%
System downtime	50%
Loss of reputation	35%
Loss of revenues	31%
Lawsuits	16%
Regulatory fines	7%
Other (please specify)	3%
Total	224%

Q11a. Do you believe these cyberattacks involving these devices in your organization had an adverse impact on patient care?

	Pct%
Yes	45%
No (please skip to Q12a)	55%
Total	100%

Q11b. If yes, what was the cause of the adverse event? Please select all that apply.

	Pct%
Inability to provide patient services	54%
Additional software installed on the IoT or connected device	49%
Inappropriate therapy/treatment delivered to the patient	26%
Attacker took control of patient's device	31%
Theft of patient records	48%
Other (please specify)	4%
Total	212%

Q11c. If yes, what impact did the cyberattack have on patient care? Please select all that apply.	Pct%
An increase in mortality rate	53%
Delays in procedures and tests resulted in poor outcomes	37%
Increase in complications from medical procedures	28%
Increase in patients transferred or diverted to other facilities	47%
Longer length of stay	56%
Other (please specify)	4%
Total	225%

Q12a. Did your organization experience one or more data breaches that resulted in the loss or exposure of patient information in the past 24 months?

	Pct%
Yes	43%
No (please skip to Q16a)	57%
Total	100%

Q12b. If yes, how many data breaches did your organization experience in the past 24 months?

	Pct%
1 to 4	35%
5 to 10	20%
10 to 15	23%
More than 15	22%
Total	100%
Extrapolated value	9.77

Q12c. If yes, how many of these data breaches involved an IoMT/IoT device?

	Pct%
None	12%
1 to 2	19%
3 to 5	28%
6 to 10	22%
More than 10	19%
Total	100%
Extrapolated value	5.45

Q12d. If yes, approximately, how much was the total cost of the largest data breach involving a medical IoT or other connected devices? Please note that the cost estimate should include all direct cash outlays, direct expenditures, indirect labor costs, overhead costs and lost business opportunities.

	Pct%
Less than $100,000	4%
$100,000 to $250,000	7%
$250,001 to $500,000	11%
$500,001 to $1,000,000	14%
$1,000,001 to $5,000,000	23%
$5,000,001 to $25,000,000	21%
$25,000,001 to $50,000,000	13%
More than $50,000,000	7%
Total	100%
Extrapolated value	$ 13,070,000

Q13. What was the root cause of the largest data breach? Please select one choice only.

	Pct%
Negligent insider	13%
Malicious insider	16%
Malicious external attacker	37%
IT system failure or glitch	21%
Uncertain	13%
Total	100%

Q14. What were the consequences of the largest data breach? Please select all that apply.

	Pct%
Exposed patient data	56%
Exposed financial and payment data	45%
System downtime	37%
Loss of reputation	33%
Loss of revenues	29%
Lawsuits	17%
Regulatory fines	9%
Other (please specify)	3%
Total	229%

Q15a. Do you believe these data breaches had an adverse impact on patient care?

	Pct%
Yes	34%
No (please skip to Q16a)	66%
Total	100%

Q15b. If yes, what impact did the data breach have on patient care? Please select all that apply.

	Pct%
An increase in mortality rate	54%
Delays in procedures and tests have resulted in poor outcomes	37%
Increase in complications from medical procedures	43%
Increase in patients transferred or diverted to other facilities	32%
Longer length of stay	39%
Other (please specify)	3%
Total	208%

Q16a. Has your company experienced one or more ransomware attacks?

	Pct%
Yes	43%
No (please skip to Q20)	57%
Total	100%

Q16b. If yes, how many ransomware incidents did your organization experience in the last 24 months?

	Pct%
1 to 2	24%
3 to 5	43%
6 to 10	18%
More than 10	15%
Total	100%
Extrapolated value	5.32

Q17a. Did your organization pay the ransom?

	Pct%
Yes	47%
No (please skip to Q19)	53%
Total	100%

Q17b. If your organization paid the ransom, why?

	Pct%
We have cyber insurance that covers the ransom	23%
We cannot afford downtime	69%
We didn't want our data leaked	63%
All of the above	45%
Other (please specify)	3%
Total	203%

Q18. How much in Bitcoin or other currency was demanded?

	Pct%
$50,000 to $100,000	10%
$100,000 to $250,000	13%
$250,001 to $500,000	32%
$500,001 to $1,000,000	16%
$1,000,001 to $2,000,000	11%
$2,000,001 to $5,000,000	9%
More than $5,000,000	9%
Total	100%
Extrapolated value	$ 1,290,250

Q19. If you did not pay a ransom, why not?	Pct%
Effective backup strategy	53%
Company policy	49%
Law enforcement advice	13%
Lack of trust in the provision of decryption key	26%
Compromised data wasn't critical	25%
Other (please specify)	4%
Total	170%

Q20. How concerned is your organization about the legal liability if there was an attack against your organization's IoMT/IoT devices from 1 = no concern to 10 = very concerned.

	Pct%
1 or 2	13%
3 or 4	19%
5 or 6	24%
7 or 8	32%
9 or 10	12%
Total	100%
Extrapolated value	5.7

Part 3

IoT security practices: Strongly Agree or Agree response combined.	Pct%
Q21a. Our senior management requires assurances that IoMT/ IoT risk is being assessed, managed and monitored appropriately.	46%
Q21b. The pace of innovation in IoMT/ IoT and varying security standards makes it hard to ensure the security of these devices and applications.	51%
Q21c. The IoMT/IoT ecosystem is vulnerable to a ransomware attack.	63%

Please rate the following questions based on the 10-point scale below each item.

Q22. Please rate the ability of your organization to secure IoMT/ IoT devices from 1 = no ability to 10 = high ability.	Pct%
1 or 2	13%
3 or 4	28%
5 or 6	24%
7 or 8	23%
9 or 10	12%
Total	100%
Extrapolated value	5.4

Q23. Please rate the level of security risk created by IoMT/ IoT devices from 1 = low risk to 10 = significant risk.

	Pct%
1 or 2	10%
3 or 4	9%
5 or 6	10%
7 or 8	29%
9 or 10	42%
Total	100%
Extrapolated value	7.2

Q24. Please rate your organization's urgency in securing IoMT/IoT and other connected devices from 1 = low urgency to 10 = high urgency.

	Pct%
1 or 2	9%
3 or 4	6%
5 or 6	13%
7 or 8	32%
9 or 10	40%
Total	100%
Extrapolated value	7.3

Q25. How does your organization secure its IoMT/IoT devices? Please select all that apply.

	Pct%
Patch management	53%
Inventory tools	23%
EDR/XDR	40%
Network segmentation	39%
Service hardening	51%
Vendor access controls	37%
Dedicated IoMT security solution	45%
Other (please specify)	4%
Total	292%

Q26a. Does your organization measure the effectiveness of its IoMT/IoT security practices?

	Pct%
Yes	51%
No (please skip to Q28)	49%
Total	100%

Q26b. If yes, what metrics are used to determine the effectiveness of your organization's IoMT/IoT security practices. Please select all that apply.	Pct%
Reduction in the number of known vulnerabilities	45%
Reduction in the number of threats	42%
Reduction in the frequency of DDoS attacks	40%
Reduction in the number of data breach incidents	63%
Percentage of IoT devices free of malware and viruses	38%
Percentage of IoT devices tested	59%
Reduction in regulatory actions and lawsuits	23%
Reduction in unplanned system downtime	23%
Reduction in the cost of security management activities	35%
Reduction in the cost of cybercrime remediation	31%
Length of time to contain data breaches and security exploits	28%
Likelihood of a data breach	31%
Other (please specify)	3%
Total	461%

Q27. If yes, who is **most** responsible for measuring the effectiveness of IoMT/ IoT security practices? Please select one choice only.

	Pct%
Chief Executive Officer/Chief Operating Officer	2%
Chief Compliance Officer	3%
Director of Internal Audit	4%
General manager/VP lines of business	15%
Chief Clinical/Biomedical Engineering Officer	9%
Chief Risk Officer	12%
Chief Information Officer	18%
Chief Information Security Officer/Chief Security Officer	13%
Chief Technology Officer	6%
Chief Procurement Officer	9%
No one person is responsible	9%
Total	100%

Q28. How often does your organization test IoMT/IoT and connected devices to find new or previously unidentified vulnerabilities? Please select one choice only.

	Pct%
Annually	11%
Monthly	15%
Weekly	23%
After every update or modification	29%
Testing is not pre-scheduled	14%
We do not test	8%
Total	100%

Q29. On average, what percentage of IoMT/ IoT and other connected devices contains identified vulnerabilities that pose a significant risk?

	Pct%
None	4%
1 to 10%	7%
11 to 20%	8%
21 to 30%	11%
31 to 40%	14%
41 to 50%	18%
51 to 75%	22%
76 to 100%	16%
Total	100%
Extrapolated value	45%

Q30. Who is most responsible for providing security analysis updates of IoMT/IoT in the organization? Please check one choice only.

	Pct%
Chief executive officer/Chief operating officer	2%
General manager/ VP lines of business	9%
Chief Clinical/Biomedical Engineering Officer	11%
Chief Risk Officer	9%
Chief Information Officer	23%
Chief Information Security Officer/Chief Security Officer	18%
Chief Technology Officer	8%
Chief Procurement Officer	14%
No one person is responsible	6%
Total	100%

Q31. Using the following scale from 1 = no confidence to 10 = high confidence, how confident are you that your organization is patching IoMT/IoT and other connected devices in a timely manner?

	Pct%
1 or 2	20%
3 or 4	16%
5 or 6	31%
7 or 8	21%
9 or 10	12%
Total	100%
Extrapolated value	5.3

Part 4. Budget and investment

Q32. Approximately, what range best describes your organization's annual IT operations budget in the current fiscal year?	Pct%
Less than $1 million	6%
$1 to $10 million	8%
$11 to $25 million	13%
$26 to $50 million	23%
$51 to $100 million	15%
$101 to $250 million	16%
$251 to $500 million	9%
More than $500 million	10%
Total	100%
Extrapolated value (US$ millions)	$ 144.63

Q33. Approximately, what percentage of your company's IT budget is dedicated to IT security?

	Pct%
Less than 5%	6%
5% to 10%	19%
11% to 20%	31%
15% to 25%	23%
More than 25%	21%
Total	100%
Extrapolated value (US$ millions)	17%

Q34. What percentage of your company's IT security budget is dedicated to securing IoMT/ IoT devices?

	Pct%
Less than 5%	2%
5% to 10%	13%
11% to 20%	21%
15% to 25%	34%
More than 25%	30%
Total	100%
Extrapolated value (US$ millions)	20%

Q35. Would any of the following factors influence your organization to increase the budget? Please select your top two concerns.

	Pct%
New regulations	41%
A serious hacking incident of your medical devices	45%
Media coverage of a serious hacking incident affecting another company	21%
Concern over potential loss of revenues due to a security incident	26%
Concern over potential loss of customers due to a security incident	27%
Concern over relationships with clinicians and other third parties	38%
Other (please specify)	2%
Total	200%

Q36. Approximately, how much does your organization spend on the security of IoMT/IoT devices each year? Please choose the range that best approximates the total investment in terms of technologies, personnel, managed or outsourced services and other cash outlays.

	Pct%
None	0%
Less than $100,000	6%
100,000 to $250,000	10%
250,001 to $500,000	8%
500,001 to $1,000,000	16%
1,000,001 to $2,500,000	21%
2,500,001 to $5,000,000	14%
$5,000,001 to $10,000,000	12%
$10,000,001 to $25,000,000	8%
More than $25,000,000	5%
Total	100%
Extrapolated value	4,865,400

Part 3. Your Role

D1. What organizational level best describes your current position?	Pct%
Senior Executive/VP	13%
Director	17%
Manager	21%
Supervisor	15%
Technician/Staff	30%
Other	4%
Total	100%

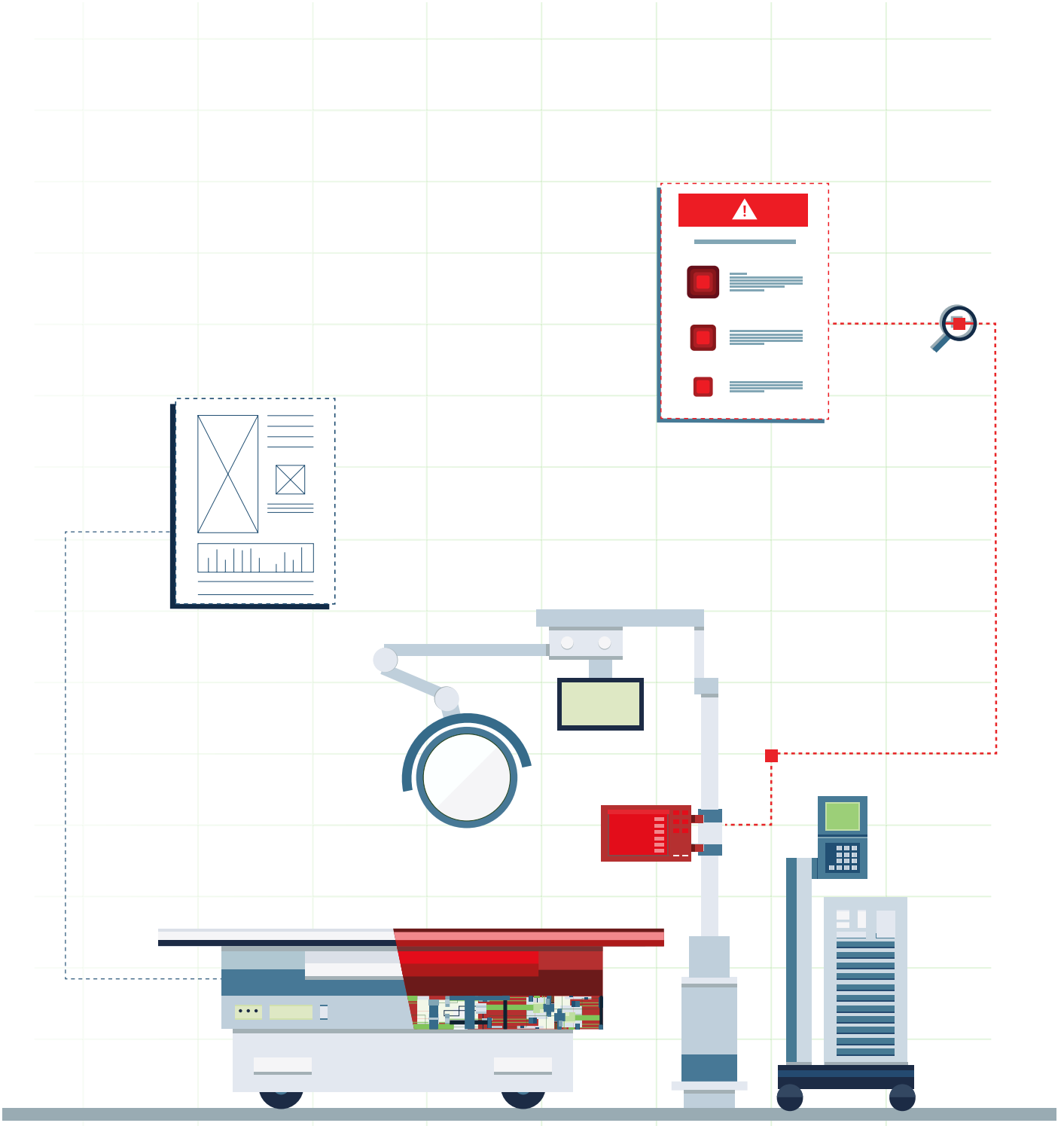
D2. Check the **Primary Person** you report to within the organization.	Pct%
Chief Financial Officer	2%
Chief Operations Officer	5%
General Counsel	12%
Chief Information Officer	26%
Chief Technology Officer	10%
Chief Information Security Officer	21%
Chief Security Officer	5%
Compliance Officer	9%
Chief Risk Officer	8%
Other	2%
Total	100%

D3. What best describes the funding structure of your organization?

	Pct%
Public	39%
Non-profit	25%
For-profit	36%
Total	100%

D4. What is the headcount of your organization?

	Pct%
Less than 100 people	15%
100 to 500 people	16%
501 to 1,000 people	21%
1,001 to 5,000 people	23%
5,001 to 25,000 people	12%
25,001 to 75,000 people	8%
More than 75,000 people	5%
Total	100%



Cynerio

Secure. Faster

Healthcare IoT Cybersecurity