Medical Device Security: An Industry Under Attack and Unprepared to Defend

Sponsored by Synopsys

Independently conducted by Ponemon Institute LLC

Publication Date: May 2017

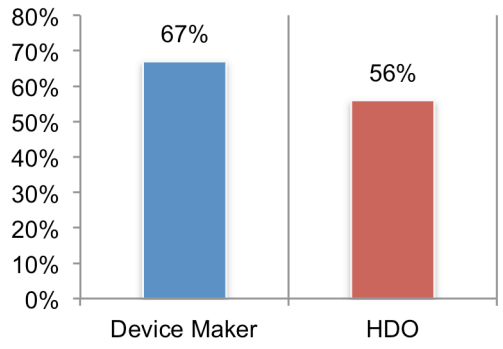
Medical Device Security: An Industry Under Attack and Unprepared to Defend

Presented by Ponemon Institute, May 2017

Part 1. Introduction

Ponemon Institute is pleased to present the findings of *Medical Device Security: An Industry Under Attack and Unprepared to Defend*, sponsored by Synopsys. The purpose of this research is to understand the risks to clinicians and patients because of insecure medical devices. We surveyed both device makers and healthcare delivery organizations (HDO) to determine if both groups are in alignment about the need to address risks to medical device. To ensure a knowledgeable respondent participants in this research have a role or involvement in the assessment of and contribution to the security of medical devices.

Figure 1. How likely is an attack on one or more medical devices built or in use by your organization over the next 12 months?
Very likely and Likely responses combined



In the context of this research, medical devices are any instrument, apparatus, appliance, or other article, whether used alone or in combination, including the software intended by its manufacturer to be used for diagnostic and/or therapeutic purposes. Medical devices vary according to their intended use. Examples range from simple devices such as medical thermometers to those that connect to the Internet to assist in the conduct of medical testing, implants, and prostheses.

The following medical devices are manufactured or used by the organizations represented in this research: robots, implantable devices, radiation equipment, diagnostic & monitoring equipment, networking equipment designed specifically for medical devices and mobile medical apps.

How vulnerable are these medical devices to attack and why both device makers and HDOs lack confidence in their security? As shown in Figure 1, 67 percent of device makers in this study believe an attack on one or more medical devices they have built by their organization is likely and 56 percent of HDOs believe such an attack is likely. Despite the likelihood of an attack, only 17 percent of device makers and 15 percent of HDOs are taking significant steps to prevent attacks. Further, only 22 percent of HDOs say their organizations have an incident response plan in place in the event of an attack on vulnerable medical devices and 41 percent of device makers say such a plan is in place.

In fact, patients have already suffered adverse events and attacks. Thirty-one percent of device makers and 40 percent of HDOs represented in this study say they are aware of these incidents. Of these respondents, 38 percent of respondents in HDOs say they are aware of inappropriate therapy/treatment delivered to the patient because of an insecure medical device and 39 percent of device makers confirm that attackers have taken control of medical devices.

Despite the risks, few organizations are taking steps to prevent attacks on medical devices. Only 17 percent of device makers are taking significant steps to prevent attacks and 15 percent of HDOs are taking significant steps.

The research reveals the following risks to medical devices and why clinicians and patients are at risk.

Both device makers and users have little confidence that patients and clinicians are protected. Both device makers and HDOs have little confidence that the security protocols or architecture built inside medical devices provide clinicians and patients with protection. HDOs are more confident than device makers that they can detect security vulnerabilities in medical devices (59 percent vs. 37 percent).

The use of mobile devices is affecting the security risk posture in healthcare organizations. Clinicians depend upon their mobile devices to more efficiently serve patients. However, 60 percent of device makers and 49 percent of HDOs say the use of mobile devices in hospitals and other healthcare organizations is significantly increasing security risks.

Medical devices are very difficult to secure. Eighty percent of medical device manufacturers and users in this study say medical devices are very difficult to secure. Further, only 25 percent of respondents say security protocols or architecture built inside devices adequately protects clinicians and patients.

In many cases, budget increases to improve the security of medical devices would occur only after a serious hacking incident occurred. Respondents believe their organizations would increase the budget only if a potentially life threatening attack took place. Only 19 percent of HDOs say concern over potential loss of customers/patients due to a security incident would result in more funds for medical device security.

Medical device security practices in place are not the most effective. Both manufacturers and users rely upon security requirements instead of more thorough practices such as security testing throughout the SDLC, code review and debugging systems and dynamic application security testing. As a result, both manufacturers and users concur that medical devices contain vulnerable code due to lack of quality assurance and testing procedures and rush to release pressures on the product development team.

Most organizations do not encrypt traffic among IoT devices. Only a third of device makers say their organizations encrypt traffic among IoT devices and 29 percent of HDOs deploy encryption to protect data transmitted from medical devices. Of these respondents, only 39 percent of device makers and 35 percent of HDOs use key management systems on encrypted traffic.

Medical devices contain vulnerable code because of a lack of quality assurance and testing procedures as well as the rush to release. Fifty-three percent of device makers and 58 percent of HDOs say there is a lack of quality assurance and testing procedures that lead to vulnerabilities in medical devices. Device makers say another problem is the rush to release pressures on the product development team (50 percent). HDOs say accidental coding errors (52 percent) is a problem.

Testing of medical devices rarely occurs. Only 9 percent of manufacturers and 5 percent of users say they test medical devices at least annually. Instead, 53 percent of HDOs do not test (45 percent) or are unsure if testing occurs (8 percent). Forty-three percent of manufacturers do not test (36 percent) or are unsure if testing takes place (7 percent).

Accountability for the security of medical devices manufactured or used is lacking. While 41 percent of HDOs believe they are primarily responsible for the security of medical devices, almost one-third of both device makers and HDOs say no one person or function is primarily responsible.

Manufacturers and users of medical devices are not in alignment about current risks to medical devices. The findings reveal a serious disconnect between the perceptions of device manufacturers and users about the state of medical device security and could prevent collaboration in achieving greater security. Some disconnects, as detailed in this report, include the following: HDOs are more likely to be concerned about medical device security and to raise concerns about risks. They are also far more concerned about the medical industry's lack of action to protect patients/users of medical devices.

How effective is the FDA in the security of medical devices? Only 44 percent of HDOs follow guidance from the FDA to mitigate or reduce inherent security risks in medical devices. Slightly more than half of device makers (51 percent) follow guidance. Only 24 percent of device makers have recalled a product because of security vulnerabilities with or without FDA guidance. Only 19 percent of HDOs have recalled a product.

Most device makers and users do not disclose privacy and security risks of their medical devices. Sixty percent of device makers and 59 percent of HDOs do not share information about security risks with clinicians and patients. If they do, it is primarily in contractual agreements or policy disclosure. Such disclosures would typically include information about how patient data is collected, stored and shared and how the security of the device could be affected.

Part 2. Key findings

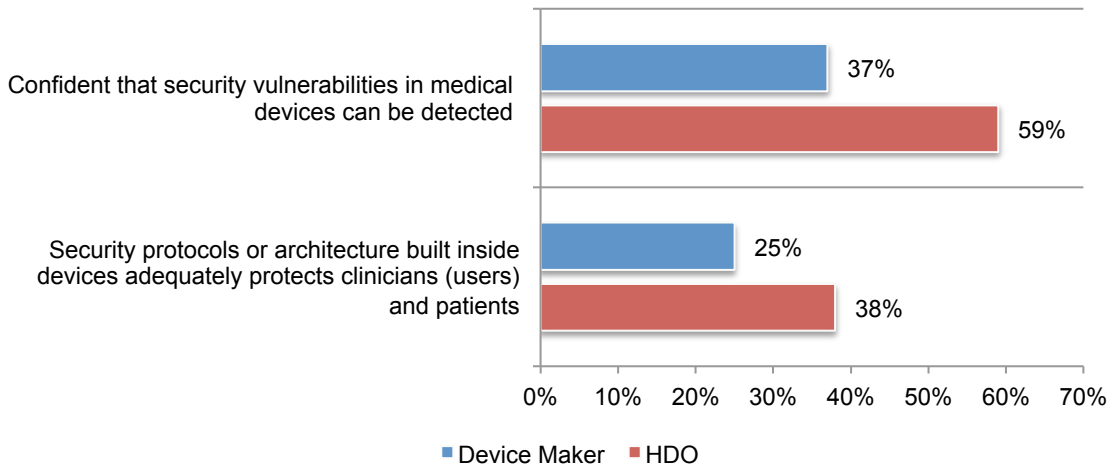
In this section, we provide a detailed analysis of the key findings. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following topics.

- Lack of confidence in the security of medical devices
- Building secure devices is challenging
- Lack of medical device security testing
- Lack of accountability
- Why medical devices are vulnerable to attack
- FDA Guidance is not enough

Lack of confidence in the security of medical devices

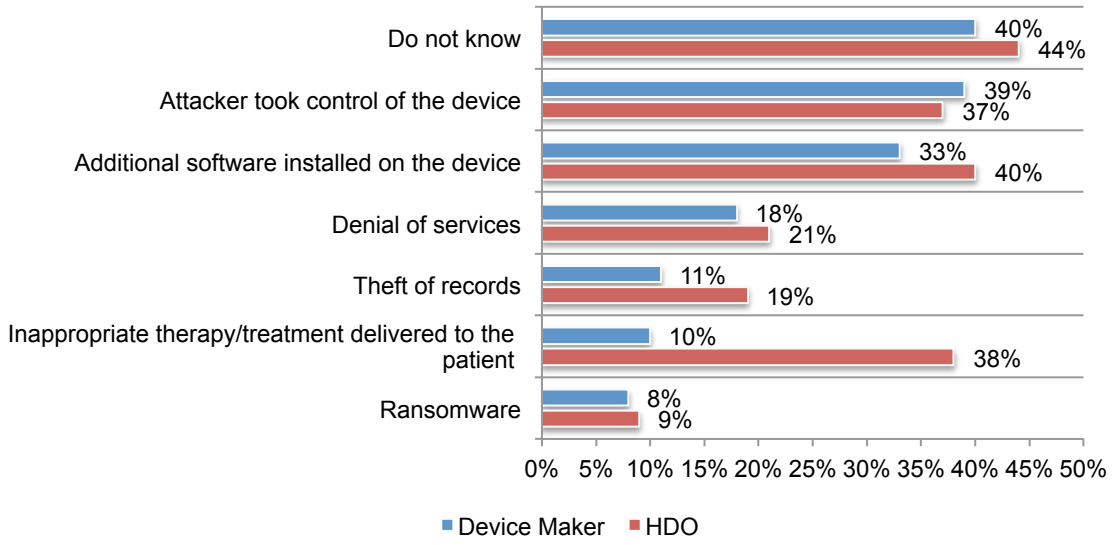
Both device makers and users have little confidence that patients and clinicians are protected. However, as shown in Figure 2, both device makers and users have little confidence that the security protocols or architecture built inside medical devices provide clinicians and patients with protection. HDOs are more confident than device makers that they can detect security vulnerabilities in medical devices (59 percent vs. 37 percent)

Figure 2. Disconnect in confidence in security of medical devices
1 = no confidence to 10 = very confident, 7 + responses reported



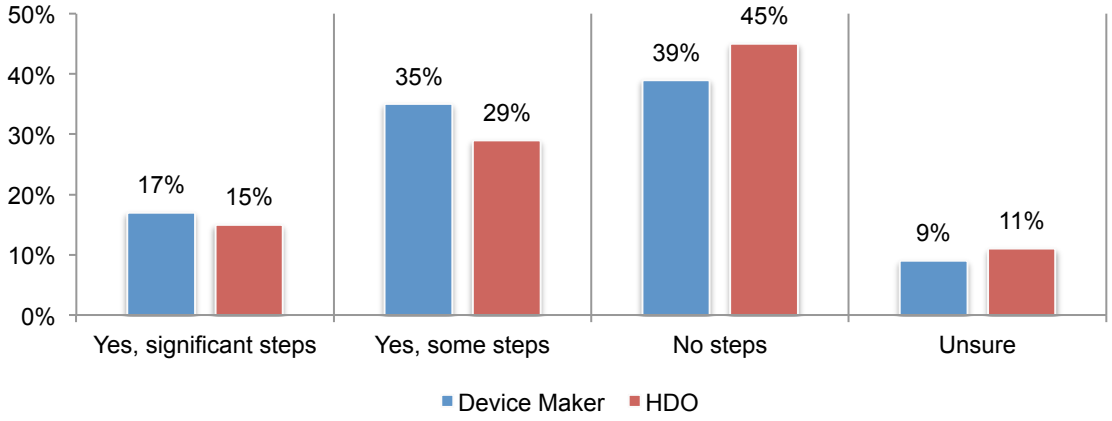
Patients have experienced adverse events or harms because of an insecure medical device. Forty percent of HDOs and 31 percent of device makers are aware that due to an insecure medical device, patients experienced an adverse event or harm. According to Figure 3, while these respondents are aware that patients were affected they do not know what the event or harm was (44 percent and 40 percent of respondents, respectively).

Figure 3. If you are aware of an adverse event or harm, what was the cause?
More than one choice permitted



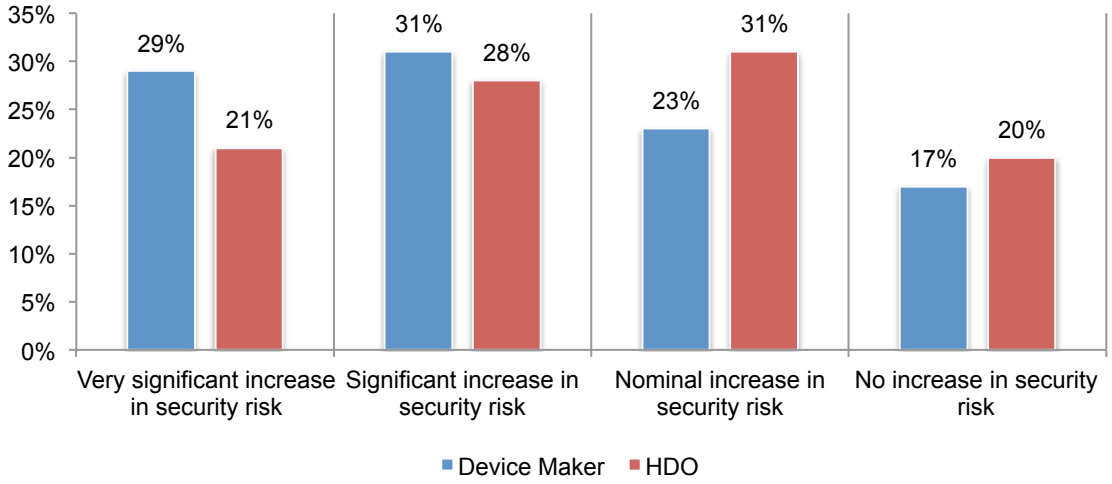
Despite the risks, few organizations are taking steps to prevent attacks on medical devices. As shown in Figure 4, only 17 percent of device makers are taking significant steps to prevent attacks and 15 percent of HDOs are taking significant steps.

Figure 4. Does your organization take steps to prevent attacks on medical devices?



The use of mobile devices is affecting the security risk posture in healthcare organizations. Clinicians depend upon their mobile devices to more efficiently serve patients. However, 60 percent of device makers and 49 percent of HDOs say the use of mobile devices in hospitals and other healthcare organizations is significantly increasing security risks, as shown in Figure 5.

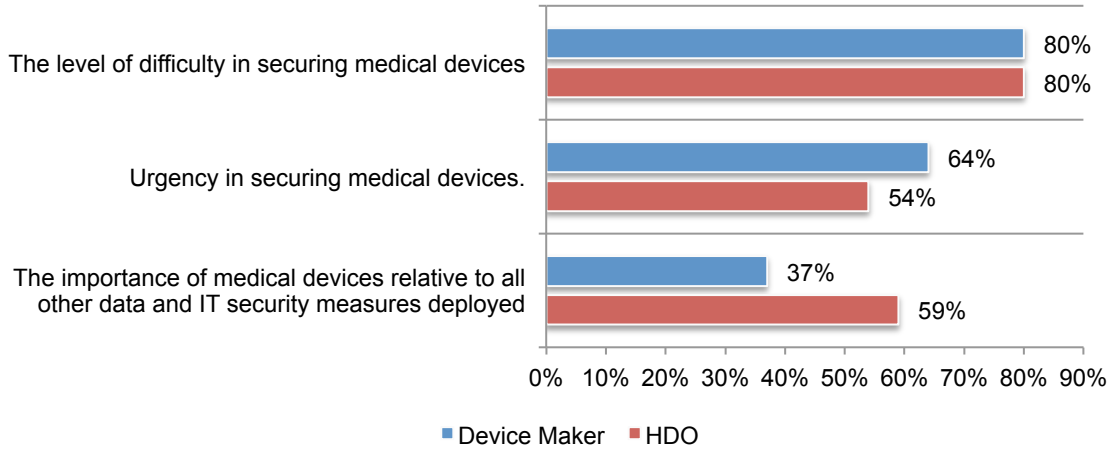
Figure 5. How does the use of mobile devices affect the security risk posture of healthcare organization that use these devices?



Building secure devices is challenging

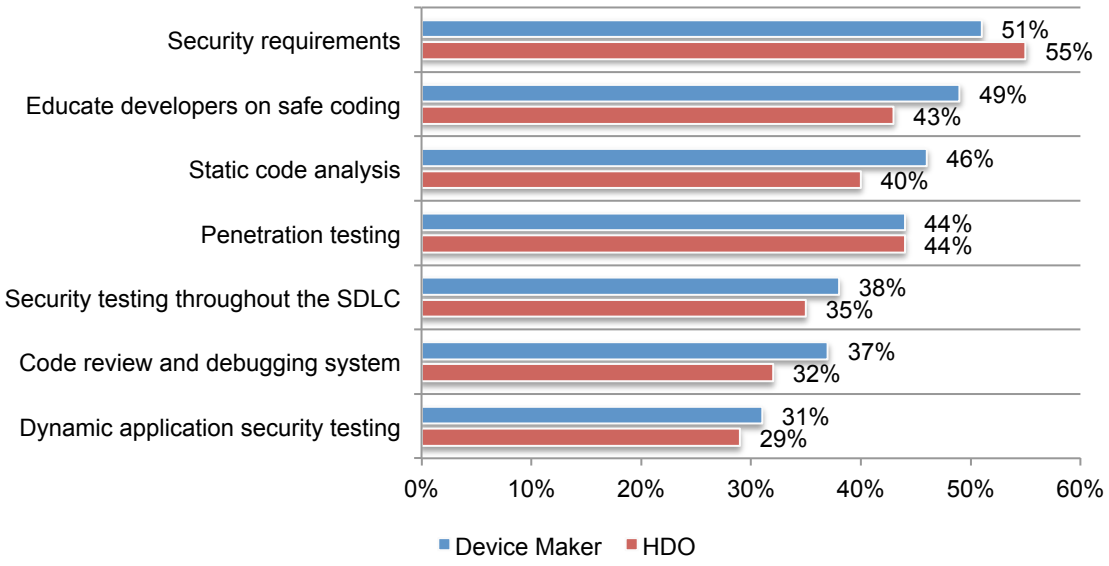
Medical devices are difficult to secure. According to Figure 6, both 80 percent of device makers and HDOs rate the level of difficulty in securing medical devices as very high (7+ on a scale of 1 = not difficult to 10 = very difficult). However, a smaller percentage of device makers (64 percent) and HDOs (54 percent) rate their organizations' urgency in securing medical devices as very high. Further, only 37 percent of device makers rate the importance of medical devices relative to all other data and IT security measures deployed by their organization as very high.

Figure 6. Disconnect in medical device security practices
1 = lowest to 10 = highest, 7 + responses reported



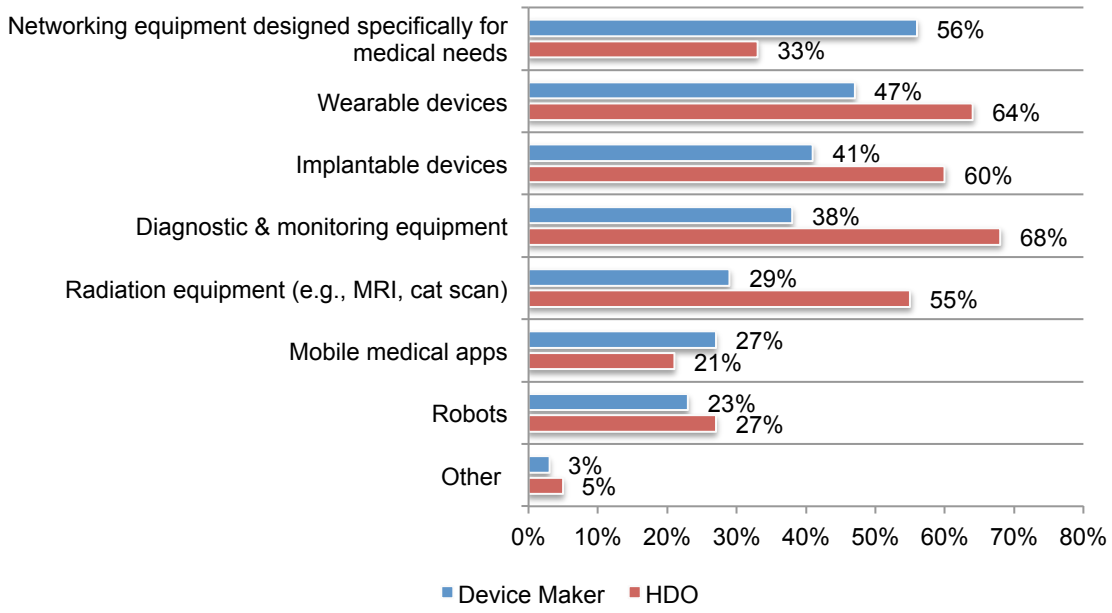
Medical device security practices in place are not the most effective. As shown in Figure 7, Both manufacturers and users rely upon following specified security requirements instead of more thorough practices such as security testing throughout the SDLC, code review and debugging systems and dynamic application security testing. As a result, both manufacturers and users concur that medical devices contain vulnerable code due to lack of quality assurance and testing procedures and rush to release pressures on the product development team.

Figure 7. What are the primary means of securing medical devices?
More than one choice permitted



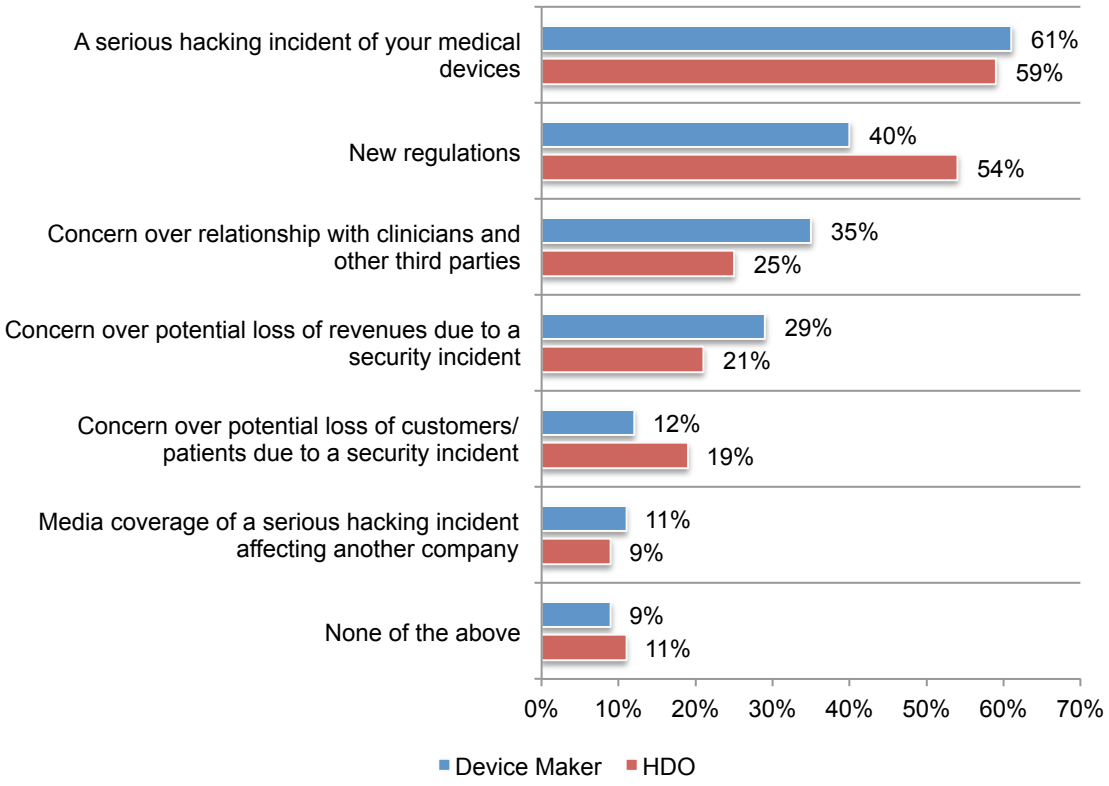
Medical device security practices should target the most widely used devices. As shown in Figure 8, HDOs are mostly purchasing diagnostic & monitoring equipment (68 percent of respondents) and wearable devices (64 percent of respondents). The device makers in this study are primarily manufacturing networking equipment designed specifically for medical needs and wearable devices (56 percent and 47 percent of respondents, respectively). On average, device makers are manufacturing 27 different types of medical devices or "products".

Figure 8. The types of medical devices designed, developed and used
More than one choice permitted



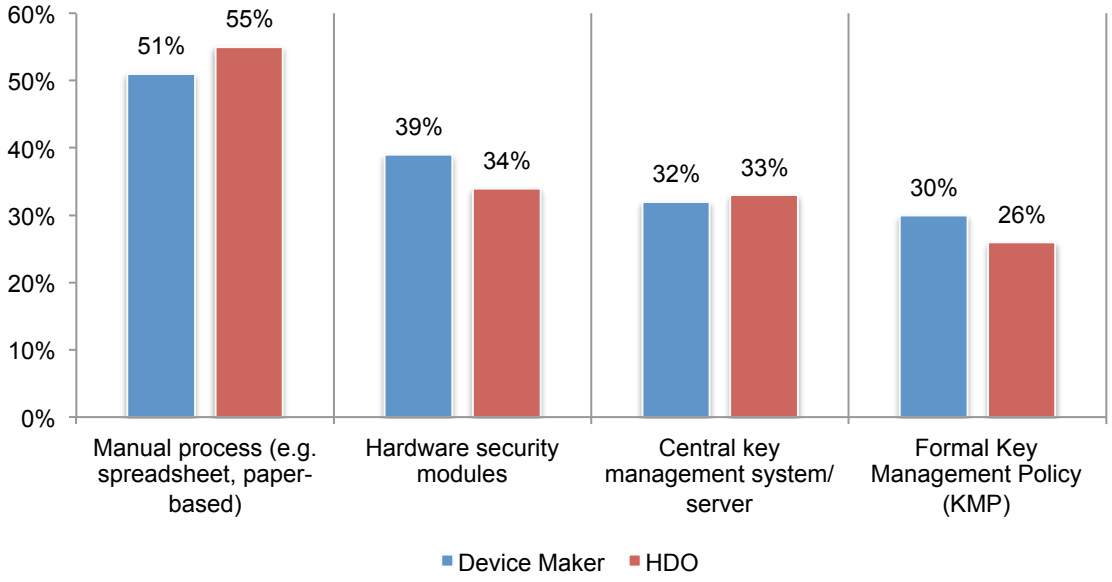
In many cases, budget increases to improve the security of medical devices would occur only after a serious hacking incident occurred. Device makers, on average, spend approximately $4 million on the security of their medical devices and HDOs spend an average of $2.4 million each year. As shown in Figure 9, a serious hacking incident or new regulations would influence their organizations to increase the security budget.

Figure 9. What would influence your organization to increase the budget?
Two choices permitted



Most organizations do not encrypt traffic among IoT devices. Only a third of device makers say their organizations encrypt traffic among IoT devices and 29 percent of HDOs deploy encryption to protect data transmitted from medical devices. Of these respondents, only 39 percent of device makers and 35 percent of HDOs use key management systems on encrypted traffic. The types of key management systems used are shown in Figure 10.

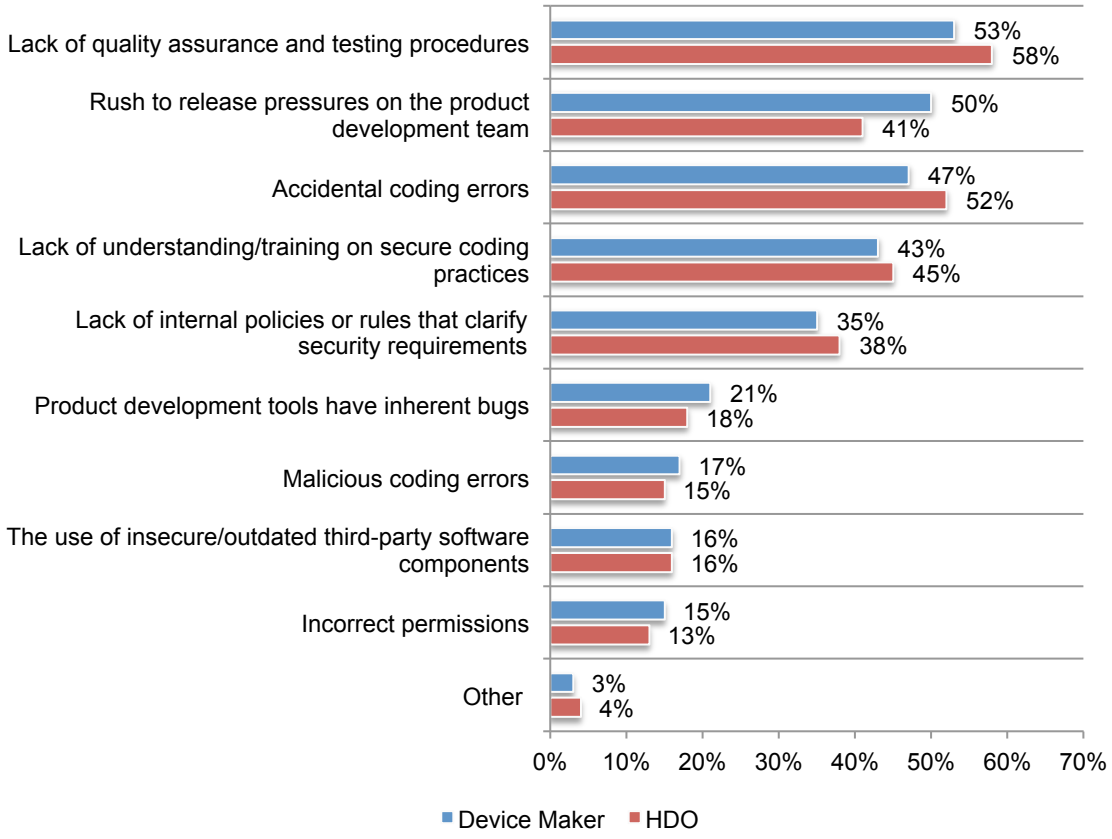
Figure 10. What key management systems are used?



Lack of security testing

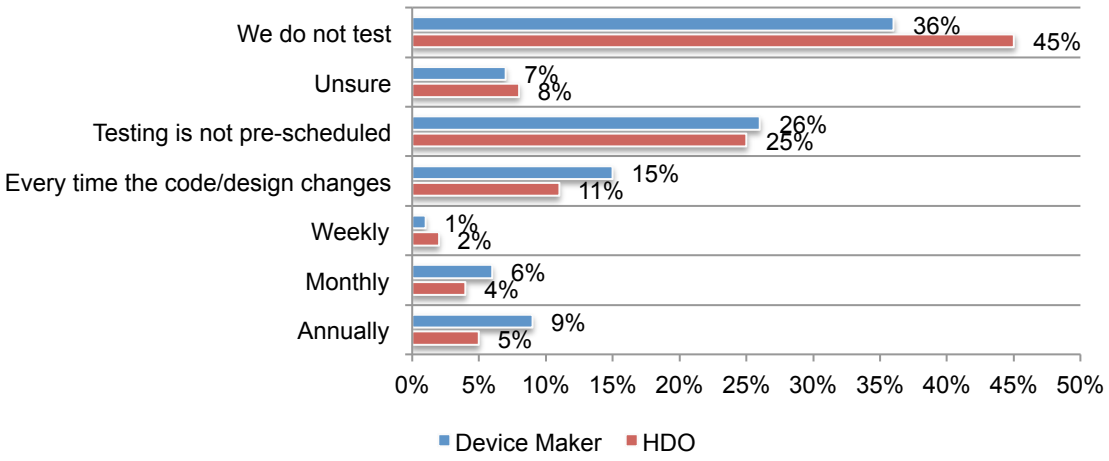
Medical devices contain vulnerable code because of a lack of quality assurance and testing procedures as well as the rush to release. As shown in Figure 11, 53 percent of device makers and 58 percent of HDOs say there is a lack of quality assurance and testing procedures that lead to vulnerabilities in medical devices. Device makers say another problem is the rush to release pressures on the product development team (50 percent). HDOs say accidental coding errors (52 percent) is a problem.

Figure 11. Why medical devices contain vulnerable code
Three choices permitted



Testing for security vulnerabilities rarely occurs. More than half of HDOs do not test medical devices (45 percent) or are unsure if testing occurs (8 percent), according to Figure 12. Forty-three percent of device makers do not test released medical devices (36 percent) to find new or previously unidentified vulnerabilities or are unsure (7 percent).

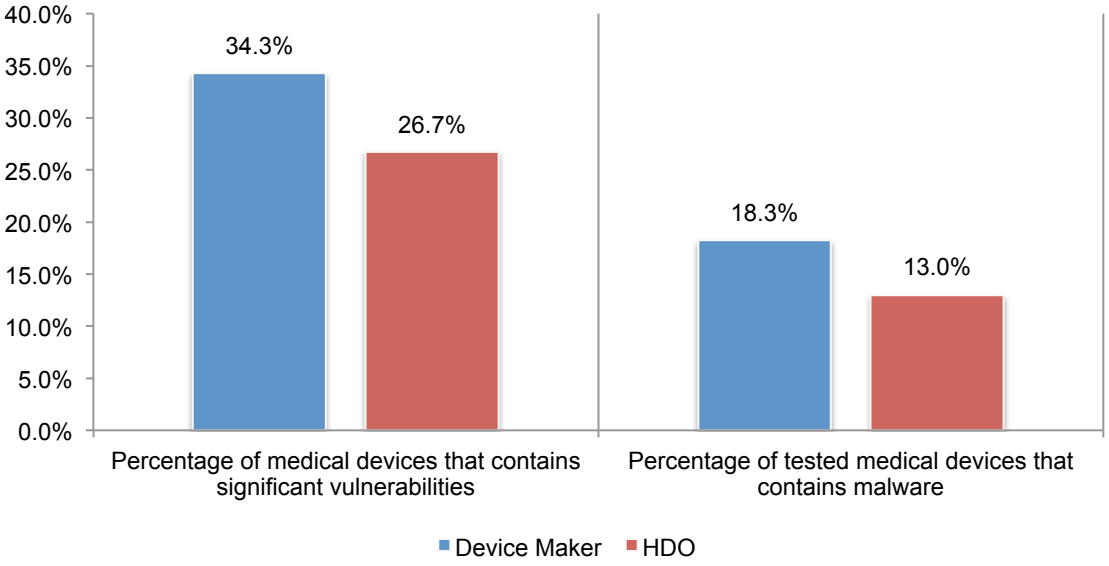
Figure 12. Does your organization test its medical devices?



Testing reveals malware and vulnerabilities in medical devices. If they do test, device makers test an average of 30 percent of medical devices and HDOs test an average of 22 percent of medical devices. As shown in Figure 13, according to device makers, an average of 18 percent of medical devices contain malware and HDOs say they discover malware in an average of 13 percent of medical devices.

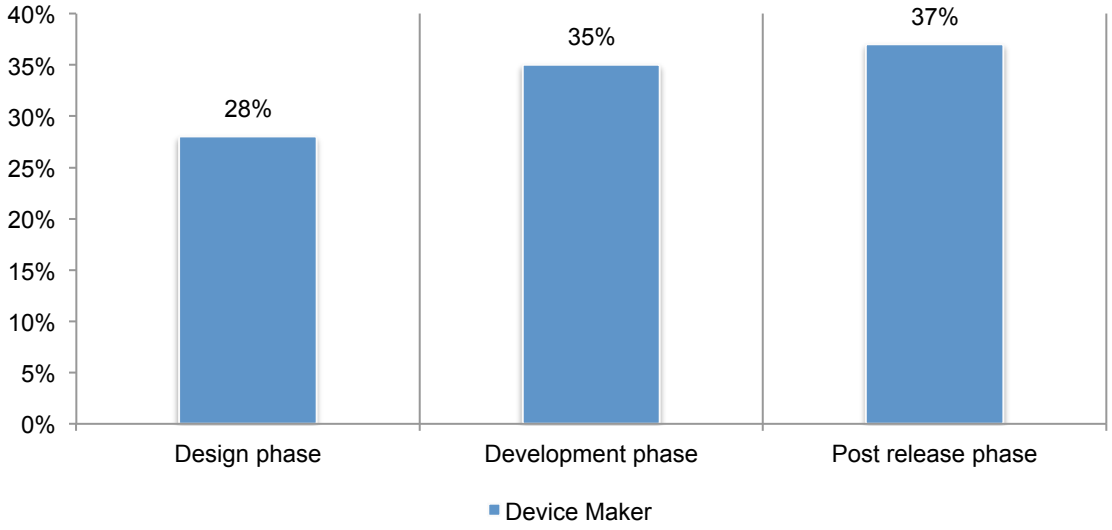
More devices contain significant vulnerabilities. According to device makers, an average of 34 percent of medical devices and HDOs say approximately 27 percent of medical devices contain significant vulnerabilities.

Figure 13. Percentage of medical devices that contain malware and significant vulnerabilities
Extrapolated values



Testing occurs too late. Few medical devices are tested in the design phase, as shown in Figure 14. Only 28 percent of respondents say testing is done before development and post release. Further, 62 percent of device makers say they do not follow a published Secure Development Life Cycle (SDLC) process for medical devices.

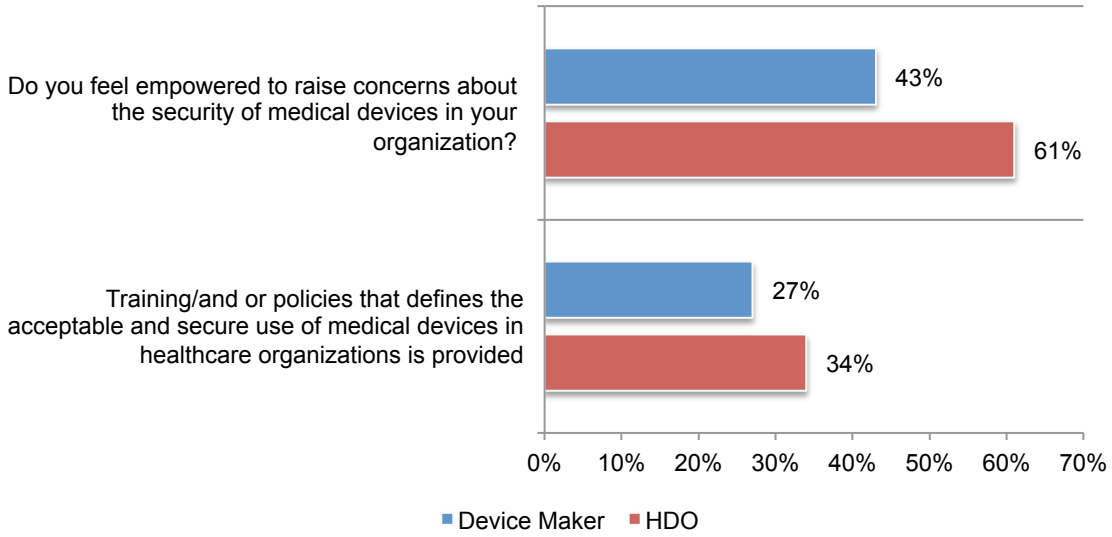
Figure 14. Where are medical devices tested for security vulnerabilities?



Lack of accountability

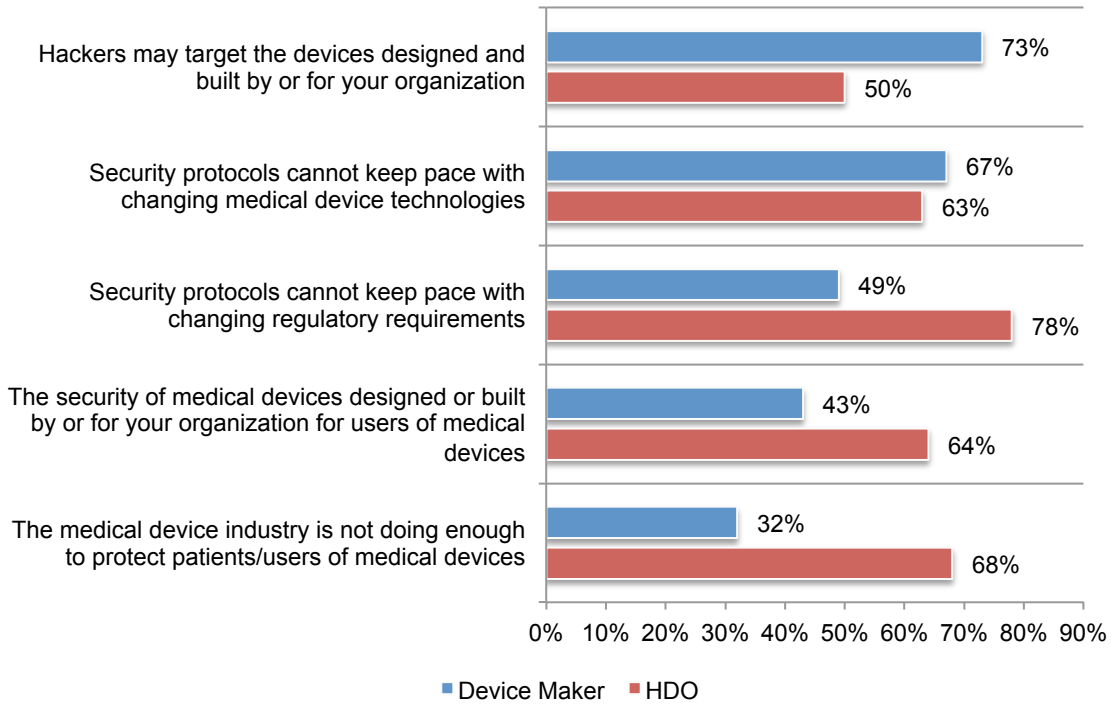
HDOs are more likely to raise security concerns and provide training and policies. More HDOs are creating a culture that encourages employees to raise concerns about the security of medical devices (61 percent of HDOs vs. 43 percent of device makers), as shown in Figure 15. While only 34 percent of HDOs are providing training and policies as it is still higher than device makers (27 percent).

Figure 15. Disconnect in reporting security concerns and providing training
Yes responses



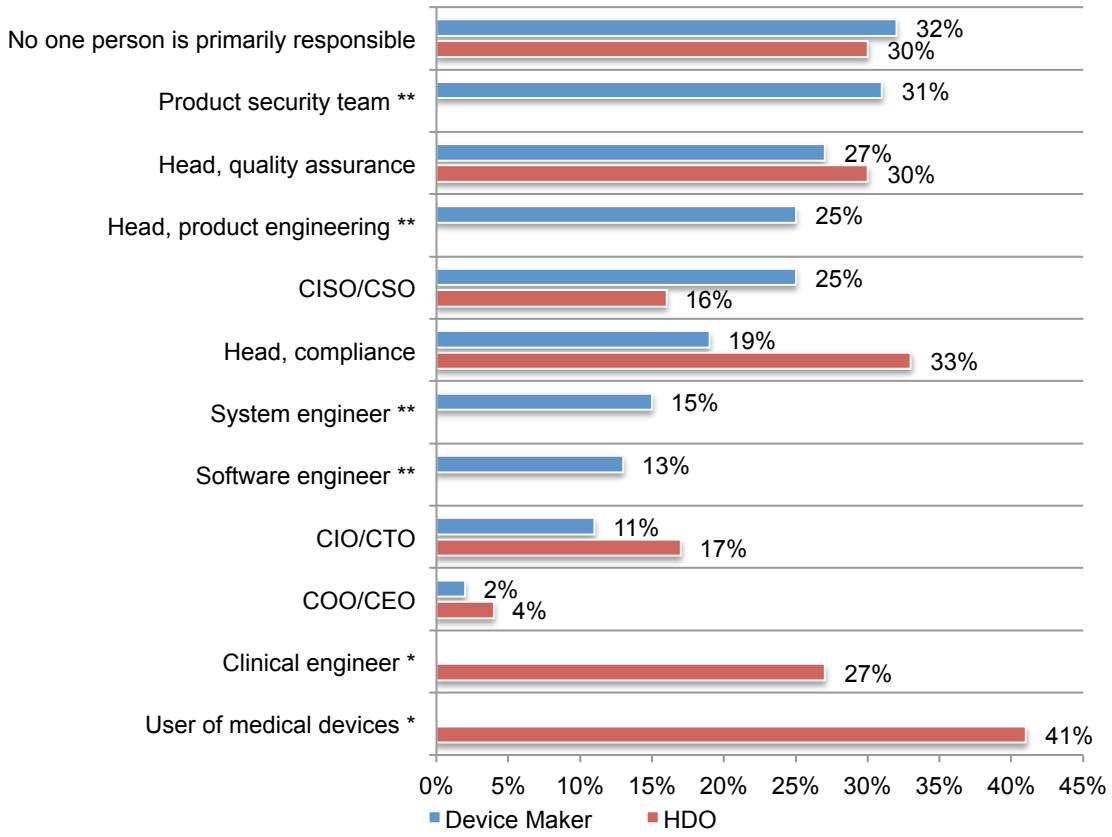
HDOs are more concerned about the security of medical devices. Figure 16 presents differences in the lack of concern about the state of medical device security. In addition to being far more concerned than device makers about the security of devices, HDOs worry a lot more than device makers about the industry's lack of protection for patients/users of medical devices and the inability of security protocols to keep pace with changing regulatory requirements. Device makers are more concerned about hackers targeting devices.

Figure 16. Disconnect in concerns about medical device security
1 = no concern to 10 = very concerned, 7 + responses reported



Accountability for the security of medical devices manufactured or used is lacking. According to Figure 17, 41 percent of HDOs say it is the user of medical devices who is primarily responsible for medical device security followed by the head of quality assurance or no one is responsible (both 30 percent of respondents). Device makers are more likely to have no one person responsible (32 percent of respondents) followed by the product security team. In both manufacturers and users, the CISO/CSO function rarely has primary responsibility for medical device security (25 percent and 16 percent of respondents, respectively).

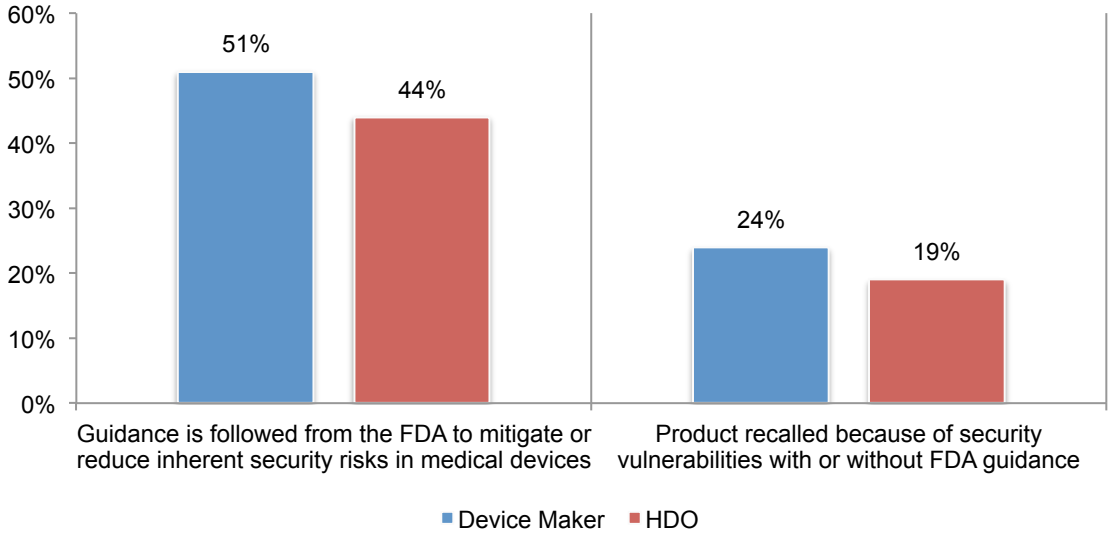
Figure 17. Who is primarily responsible for the security of medical devices?
More than one choice permitted



* Choice not available for device maker **Choice not avaiilable for device user

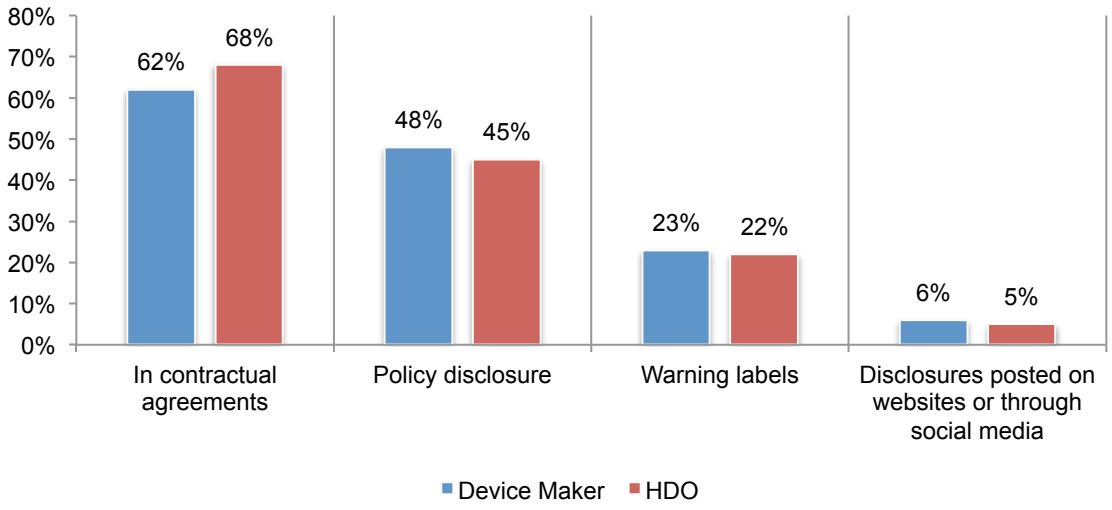
How effective is the FDA in the security of medical devices? According to Figure 18, only 44 percent of HDOs follow guidance from the FDA to mitigate or reduce inherent security risks in medical devices. Slightly more than half of device makers (51 percent) follow guidance. Only 24 percent of device makers have recalled a product because of security vulnerabilities with or without FDA guidance. Only 19 percent of HDOs have recalled a product.

Figure 18. Is FDA guidance followed?
Yes responses



Most device makers and users do not disclose privacy and security risks of their medical devices. Sixty percent of device makers and 59 percent of HDOs do not share information about security risks with clinicians and patients. If they do, as shown in Figure 19, it is primarily in contractual agreements or policy disclosure. Such disclosures would typically include information about how patient data is collected, stored and shared and how the security of the device could be affected.

Figure 19. How are medical device privacy and security risks disclosed to clinicians and patients?



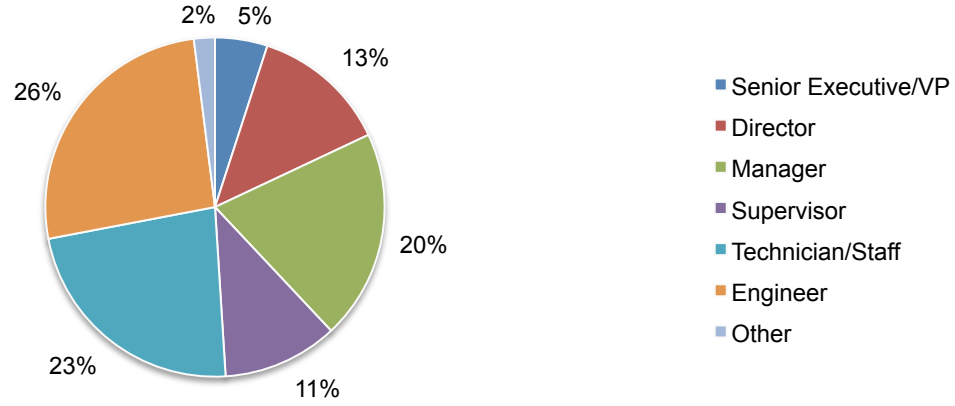
Part 3. Methods

This report consists of two sets of survey responses. The first group of participants is a sampling frame of 5,996 individuals who are involved or have a role as a device maker. Table 2 shows 277 total returns. Reliability checks required the removal of 35 surveys. Our final sample consisted of 242 surveys, or a 4.0 percent response rate. The second group of participants is a sampling frame of 7,991 individuals who are involved or has a role as a healthcare delivery organization. Table 2 shows 287 total returns. Reliability checks required the removal of 25 surveys. Our final sample consisted of 262 surveys, or a 3.3 percent response rate.

Table 2. Sample response	Device Maker	Devise User
Sampling frame	5,996	7,991
Total returns	277	287
Rejected surveys	35	25
Final sample	242	262
Response rate	4.0%	3.3%

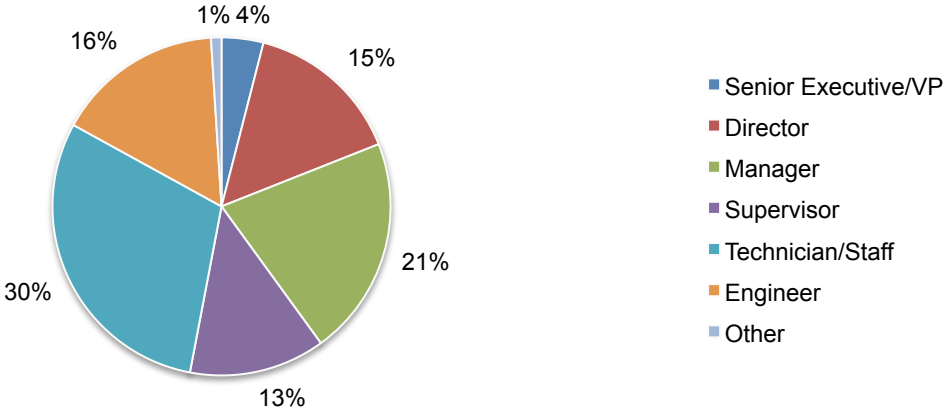
Pie Chart 1 reports the Device Maker's organizational level within participating organizations. By design, almost half of the respondents (49 percent) are at or above the supervisory levels.

Pie Chart 1. Device Maker position level within the organization
(Device Maker n = 242)



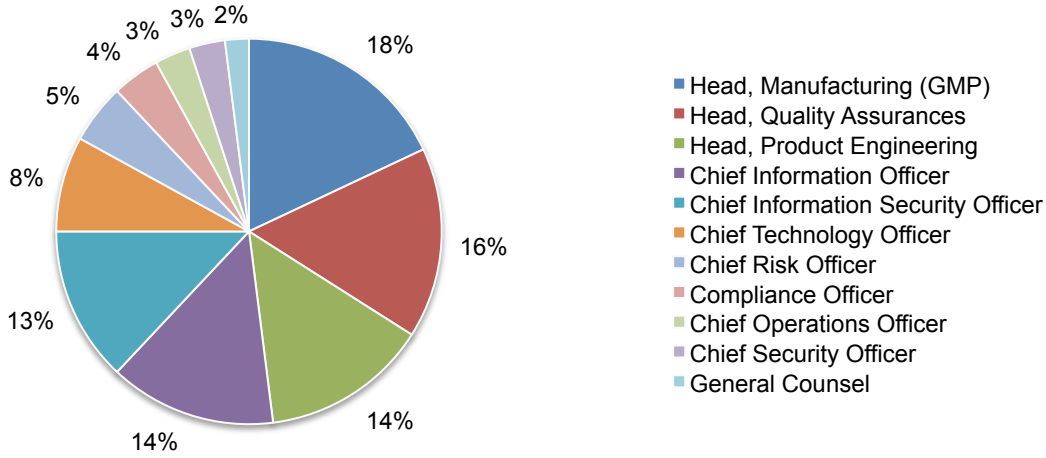
Pie Chart 2 reports the HDO's organizational level within participating organizations. By design, half of the respondents (53 percent) are at or above the supervisory levels.

Pie Chart 2. HDO position level within the organization
(HDO n = 262)



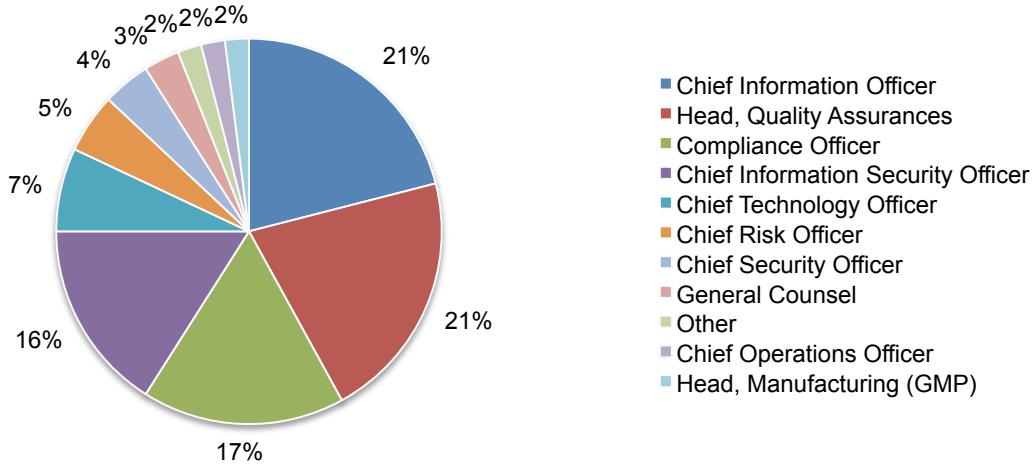
As shown in Pie Chart 3, 18 percent of Device Makers report directly to the head of manufacturing (GMP), 16 percent of respondents report to the head of quality assurances, 14 percent of respondents report to the head of product engineering and 14 percent report to the chief information officer.

Pie Chart 3. The primary person reported to within the organization
(Device Maker n = 242)



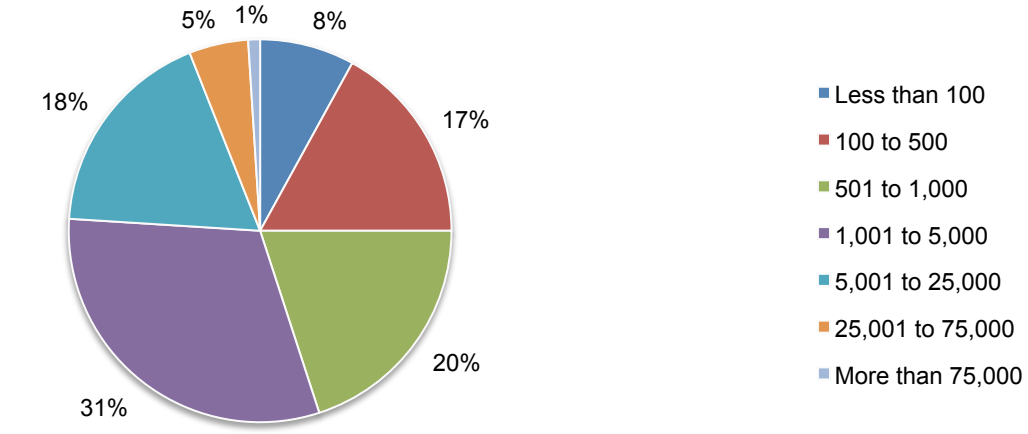
As shown in Pie Chart 4, 21 percent of HDOs report directly to the chief information officer, 21 percent of respondents report to the head of quality assurances, 17 percent of respondents report to the compliance officer and 16 percent report to the chief information security officer.

Pie Chart 4. The primary person reported to within the organization
(HDO n = 262)



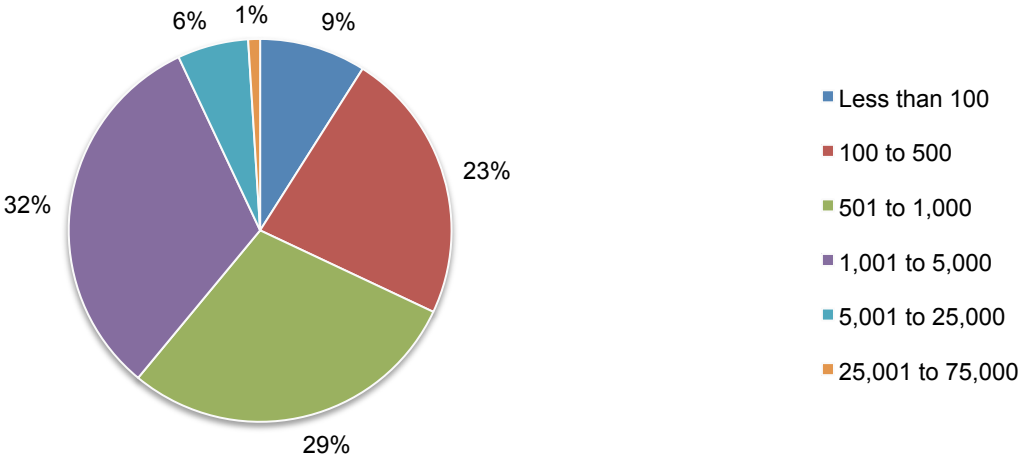
Fifty-five percent of the Device Makers are from organizations with a global headcount of more than 1,000 employees, as shown in Pie Chart 5.

Pie Chart 5. Worldwide headcount of the organization
(Device Maker n = 242)



Thirty-nine percent of the HDOs are from organizations with a global headcount of more than 1,000 employees, as shown in Pie Chart 6.

Pie Chart 6. Worldwide headcount of the organization
(HDO n = 262)



Part 4. 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 individuals who have a role or are involvement in contributing to or assessing the security of medical devices. 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 or truthful responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were gathered in March 2017.

Survey response	Device Maker	HDO
Total sampling frame	5,996	7,991
Total returns	277	287
Rejected surveys	35	25
Final sample	242	262
Response rate	4.0%	3.3%
Weighting	0.48	0.52

Part 1. Screening

S1a. Do you have any role or involvement in contributing to or assessing the security of medical devices?	Device Maker	HDO
Yes, significant involvement	31%	27%
Yes, some involvement	58%	63%
Yes, minimal involvement	11%	10%
No involvement (Stop)	0%	0%
Total	100%	100%

S1b. If you are involved, how many years have you spent contributing to or assessing the security of medical devices?	Device Maker	HDO
Less than 1 year	20%	25%
2 to 4 years	43%	52%
5 to 7 years	24%	17%
8 to 10 years	8%	4%
More than 10 years	5%	2%
Total	100%	100%

S2. How familiar are you with your organization's security practices in the development and/or use of medical devices?	Device Maker	HDO
Very familiar	42%	38%
Familiar	45%	39%
Somewhat familiar	13%	23%
No knowledge (stop)	0%	0%
Total	100%	100%

S3. What best describes your organization's role in development of medical devices for use by clinicians and/or patients?	Device Maker	HDO
I use medical devices for patient care	0%	100%
I design and build medical devices for use by clinicians	85%	0%
I am both a user and maker of medical devices (allocated to device maker)	15%	0%
None of the above (stop)	0%	0%
Total	100%	100%

S4. What best describes your role?	Device Maker	HDO
IT or non-IT professional employed in medical device manufacturing	100%	0%
IT or non-IT professional employed in healthcare delivery organizations	0%	100%
None of the above (stop)	0%	0%
Total	100%	100%

Part 2. Background

Q1. What type of medical devices does your organization design, develop and/or use? Please select all that apply.	Device Maker	HDO
Robots	23%	27%
Implantable devices	41%	60%
Wearable devices	47%	64%
Radiation equipment (e.g., MRI, cat scan)	29%	55%
Diagnostic & monitoring equipment	38%	68%
Networking equipment designed specifically for medical needs	56%	33%
Mobile medical apps	27%	21%
Other (please specify)	3%	5%
Total	264%	333%

Q2. Using the US Food & Drug Administration's (FDA) three-tier risk classification schema, what class of medical devices does your organization design, develop and/or use? Please provide your response according to the proportion of medical devices by risk level.	Device Maker	HDO
Class I	5%	11%
Class II	50%	54%
Class III	45%	35%
Total	100%	100%

Q3a. If your organization manufacturers medical devices, who is primarily responsible for their security? Top two choices.	Device Maker	HDO
CIO/CTO	11%	
CISO/CSO	25%	
COO/CEO	2%	
Software engineer	13%	
System engineer	15%	
Product security team	31%	
Head, compliance	19%	
Head, product engineering	25%	
Head, quality assurance	27%	
No one person is primarily responsible	32%	
Other (please specify)	0%	
Total	200%	

Q3b. If your organization is a healthcare provider, who is primarily responsible for medical device security? Top two choices.	Device Maker	HDO
CIO/CTO		17%
CISO/CSO		16%
COO/CEO		4%
Head, quality assurance		30%
Head, compliance		33%
Clinical engineer		27%
User of medical devices		41%
No one person is primarily responsible		30%
Other (please specify)		2%
Total		200%

Q4. Does your organization provide training/and or policies that defines the acceptable and secure use of medical devices in healthcare organizations?	Device Maker	HDO
Yes	27%	34%
No	73%	66%
Total	100%	100%

Q5. Do you feel empowered to raise concerns about the security of medical devices in your organization?	Device Maker	HDO
Yes	43%	61%
No	57%	39%
Total	100%	100%

Please rate the following statements using the 10-point scale from 1 = not concerned to 10 = very concerned.		
Q6. How concerned are you about the security of medical devices designed or built by or for your organization for users of medical devices?	Device Maker	HDO
1 or 2	12%	6%
3 or 4	19%	11%
5 or 6	26%	19%
7 or 8	23%	27%
9 or 10	20%	37%
Total	100%	100%
Extrapolated value	5.90	7.06

Q7. How concerned are you that the medical device industry is not doing enough to protect patients/users of medical devices?	Device Maker	HDO
1 or 2	16%	3%
3 or 4	27%	7%
5 or 6	25%	22%
7 or 8	20%	25%
9 or 10	12%	43%
Total	100%	100%
Extrapolated value	5.20	7.46

Q8. How concerned are you that your security protocols cannot keep pace with changing medical device technologies?	Device Maker	HDO
1 or 2	7%	4%
3 or 4	12%	8%
5 or 6	14%	25%
7 or 8	21%	29%
9 or 10	46%	34%
Total	100%	100%
Extrapolated value	7.24	7.12

Q9. How concerned are you that your security protocols cannot keep pace with changing regulatory requirements?	Device Maker	HDO
1 or 2	13%	3%
3 or 4	18%	6%
5 or 6	20%	13%
7 or 8	23%	29%
9 or 10	26%	49%
Total	100%	100%
Extrapolated value	6.12	7.80

Q10. How concerned are you that hackers may target the devices designed and built by or for your organization?	Device Maker	HDO
1 or 2	5%	10%
3 or 4	9%	16%
5 or 6	13%	24%
7 or 8	39%	27%
9 or 10	34%	23%
Total	100%	100%
Extrapolated value	7.26	6.24

Please rate the following statements using the 10-point scale from 1 = not confident to 10 = very confident.		
Q11. How confident are you that the security protocols or architecture built inside your organization's devices adequately protects clinicians (users) and patients.	Device Maker	HDO
1 or 2	21%	16%
3 or 4	25%	21%
5 or 6	29%	25%
7 or 8	13%	21%
9 or 10	12%	17%
Total	100%	100%
Extrapolated value	4.90	5.54

Q12. How confident are you that you can detect security vulnerabilities in medical devices?	Device Maker	HDO
1 or 2	11%	8%
3 or 4	27%	12%
5 or 6	25%	21%
7 or 8	22%	34%
9 or 10	15%	25%
Total	100%	100%
Extrapolated value	5.56	6.62

Part 3. Medical device risks

Q13. How familiar are you with the FDA's three-tier risk classification scheme for medical devices?	Device Maker	HDO
Very familiar	33%	25%
Familiar	41%	38%
Somewhat familiar	17%	24%
No familiarity	9%	13%
Total	100%	100%

Q14. Approximately, how many different types of medical devices or "products" are manufactured by your organization today?	Device Maker	HDO
Less than 5	4%	
5 to 10	12%	
11 to 15	23%	
16 to 25	20%	
26 to 50	26%	
More than 50	15%	
Total	100%	
Extrapolated value	27.0	

Q15. How likely is an attack on one or more medical devices built or in use by your organization over the next 12 months?	Device Maker	HDO
Very likely	33%	26%
Likely	34%	30%
Somewhat likely	13%	18%
Not likely	20%	26%
Total	100%	100%

Q16. Does your organization take steps to prevent attacks on medical devices?	Device Maker	HDO
Yes, significant steps	17%	15%
Yes, some steps	35%	29%
No steps	39%	45%
Unsure	9%	11%
Total	100%	100%

Q17. Does your organization follow guidance from the FDA to mitigate or reduce inherent security risks in medical devices?	Device Maker	HDO
Yes	51%	44%
No	49%	56%
Total	100%	100%

Q18. Has your organization ever recalled a product because of security vulnerabilities with or without FDA guidance?	Device Maker	HDO
Yes	24%	19%
No	76%	81%
Total	100%	100%

Q19. How does the use of mobile devices affect the security risk posture of the healthcare organizations that use these devices?	Device Maker	HDO
Very significant increase in security risk	29%	21%
Significant increase in security risk	31%	28%
Nominal increase in security risk	23%	31%
No increase in security risk	17%	20%
Total	100%	100%

Q20. Has your organization been audited for compliance with medical device security standards?	Device Maker	HDO
Yes	39%	30%
No	61%	70%
Total	100%	100%

Q21a. Does your organization disclose the privacy and security risks of its medical devices to clinicians and patients?	Device Maker	HDO
Yes	40%	41%
No	60%	59%
Total	100%	100%

Q21b. If yes, how are these risks disclosed?	Device Maker	HDO
In contractual agreements	62%	68%
Warning labels	23%	22%
Policy disclosure	48%	45%
Disclosures posted on websites or through social media	6%	5%
Total	139%	140%

Part 4. Medical device security practices

The following items are rated using a 10-point scale ranging from 1 = lowest to 10 = highest.		
Q22. Please rate the level of difficulty in securing medical devices.	Device Maker	HDO
1 or 2	3%	2%
3 or 4	5%	7%
5 or 6	12%	11%
7 or 8	28%	35%
9 or 10	52%	45%
Total	100%	100%
Extrapolated value	7.92	7.78

Q23. Please rate your organization's urgency in securing medical devices.	Device Maker	HDO
1 or 2	2%	3%
3 or 4	13%	12%
5 or 6	21%	31%
7 or 8	34%	34%
9 or 10	30%	20%
Total	100%	100%
Extrapolated value	7.04	6.62

Q24. Please rate the importance of medical devices relative to all other data and IT security measures deployed by your organization.	Device Maker	HDO
1 or 2	11%	8%
3 or 4	27%	12%
5 or 6	25%	21%
7 or 8	22%	34%
9 or 10	15%	25%
Total	100%	100%
Extrapolated value	5.56	6.62

Q25. On average, what percentage of medical devices is tested for security vulnerabilities?	Device Maker	HDO
None	15%	19%
1 to 10%	11%	18%
11 to 20%	12%	23%
21 to 30%	24%	19%
31 to 40%	16%	5%
41 to 50%	4%	6%
51 to 75%	7%	3%
76 to 100%	11%	7%
Total	100%	100%
Extrapolated value	0.30	0.22

Q26. On average, what percentage of tested medical devices contains malware?	Device Maker	HDO
None	24%	32%
1 to 10%	12%	17%
11 to 20%	21%	20%
21 to 30%	17%	19%
31 to 40%	18%	10%
41 to 50%	6%	2%
51 to 75%	2%	0%
76 to 100%	0%	0%
Total	100%	100%
Extrapolated value	18.3%	13.0%

Q27a. If your organization is a healthcare delivery organization, how often does it test medical devices?	Device Maker	HDO
Annually		5%
Monthly		4%
Weekly		2%
Every time the code/design changes		11%
Testing is not pre-scheduled		25%
Unsure		8%
We do not test		45%
Total		100%

Q27b. If your organization is a manufacturer, how often does it test released medical devices to find new or previously unidentified vulnerabilities?	Device Maker	HDO
Annually	9%	
Monthly	6%	
Weekly	1%	
Every time the code/design changes	15%	
Testing is not pre-scheduled	26%	
Unsure	7%	
We do not test	36%	
Total	100%	

Q28. On average, what percentage of medical devices contains significant vulnerabilities?	Device Maker	HDO
None	15%	19%
1 to 10%	9%	14%
11 to 20%	5%	6%
21 to 30%	7%	9%
31 to 40%	24%	21%
41 to 50%	19%	22%
51 to 75%	16%	9%
76 to 100%	5%	0%
Total	100%	100%
Extrapolated value	34.3%	26.7%

Q29. Where in the product development life cycle are medical devices tested for security vulnerabilities? Please check all that apply.	Device Maker	HDO
Design phase	28%	
Development phase	35%	
Post release phase	37%	
Total	100%	

Q30. Do you have an incident response plan in place in the event of an attack on vulnerable medical devices?	Device Maker	HDO
Yes	41%	22%
No	59%	78%
Total	100%	100%

Q31. Does your organization follow a published Secure Development Life Cycle (SDLC) process for medical devices?	Device Maker	HDO
Yes	38%	
No	62%	
Total	100%	

Q32. What do you see as the main reason(s) why your organization's medical devices contain vulnerable code? Please select the top three.	Device Maker	HDO
Accidental coding errors	47%	52%
The use of insecure/outdated third-party software components	16%	16%
Malicious coding errors	17%	15%
Lack of internal policies or rules that clarify security requirements	35%	38%
Lack of understanding/training on secure coding practices	43%	45%
Rush to release pressures on the product development team	50%	41%
Lack of quality assurance and testing procedures	53%	58%
Product development tools have inherent bugs	21%	18%
Incorrect permissions	15%	13%
Other (please specify)	3%	4%
Total	300%	300%

Q33. What is your organization's primary means of securing medical devices? Please select all that apply.	Device Maker	HDO
Educate developers on safe coding	49%	43%
Secure architecture process	21%	23%
Threat modeling	19%	21%
Design FMEAs or similar risk	16%	14%
Identification method	11%	18%
Security requirements	51%	55%
Code review and debugging system	37%	32%
Static code analysis	46%	40%
Software composition analysis	18%	22%
Fuzz testing	10%	15%
Dynamic application security testing	31%	29%
Penetration testing	44%	44%
Security testing throughout the SDLC	38%	35%
Data masking or redaction of live data (during testing)	17%	19%
Security patch management	20%	16%
Run-time application self protection	28%	25%
Other (please specify)	2%	3%
None of the above	30%	27%
Total	488%	481%

Q34a. Are you aware of any adverse events or harms to patients because of an insecure medical device either developed by or deployed within your organization?	Device Maker	HDO
Yes	31%	40%
No	50%	39%
Do not know	19%	21%
Total	100%	100%

Q34b. If yes, what was the adverse event? Please check all that apply	Device Maker	HDO
Denial of services	18%	21%
Additional software installed on the device	33%	40%
Inappropriate therapy/treatment delivered to the patient	10%	38%
Attacker took control of the device	39%	37%
Ransomware	8%	9%
Theft of records	11%	19%
Do not know	40%	44%
Total	159%	208%

Q35a. Does your organization encrypt traffic among IoT devices?	Device Maker	HDO
Yes	33%	29%
No	67%	71%
Total	100%	100%

Q35b-1. If yes, does your organization use key management systems on encrypted traffic among IoT devices?	Device Maker	HDO
Yes	39%	35%
No	61%	65%
Total	100%	100%

Q35b-2. If yes, what key management systems does your organization presently use? Please check all that apply	Device Maker	HDO
Formal Key Management Policy (KMP)	30%	26%
Manual process (e.g. spreadsheet, paper-based)	51%	55%
Central key management system/server	32%	33%
Hardware security modules	39%	34%
Total	152%	148%

Q36. Approximately, how much does your organization spend on medical device security 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.	Device Maker	HDO
None	9%	10%
1 to $100,000	4%	5%
100,001 to $250,000	11%	12%
250,001 to $500,000	12%	13%
500,001 to $1,000,000	21%	13%
1,000,001 to $2,500,000	16%	18%
2,500,001 to $5,000,000	9%	21%
$5,000,001 to $10,000,000	7%	5%
$10,000,001 to $25,000,000	8%	2%
$25,000,001 to $50,000,000	1%	1%
More than $50,000,000	2%	0%
Total	100%	100%
Extrapolated value ($millions)	$4.34	$2.37

Q37. Would any of the following factors influence your organization to increase the budget? Please select your top two concerns.	Device Maker	HDO
New regulations	40%	54%
A serious hacking incident of your medical devices	61%	59%
Media coverage of a serious hacking incident affecting another company	11%	9%
Concern over potential loss of revenues due to a security incident	29%	21%
Concern over potential loss of customers/patients due to a security incident	12%	19%
Concern over relationship with clinicians and other third parties	35%	25%
None of the above	9%	11%
Other	3%	2%
Total	200%	200%

Part 3. Your Role

D1. What organizational level best describes your current position?	Device Maker	HDO
Senior Executive/VP	5%	4%
Director	13%	15%
Manager	20%	21%
Supervisor	11%	13%
Technician/Staff	23%	30%
Engineer	26%	16%
Other	2%	1%
Total	100%	100%

D2. Check the Primary Person you or your supervisor reports to within the organization.	Device Maker	HDO
Chief Financial Officer	0%	1%
Chief Operations Officer	3%	2%
General Counsel	2%	3%
Head, Manufacturing (GMP)	18%	2%
Head, Product Engineering	14%	0%
Head, Quality Assurances	16%	21%
Chief Information Officer	14%	21%
Chief Technology Officer	8%	7%
Chief Information Security Officer	13%	16%
Chief Security Officer	3%	4%
Compliance Officer	4%	17%
Data center management	0%	1%
Chief Risk Officer	5%	5%
Other	0%	0%
Total	100%	100%

D3. What is the worldwide headcount of your organization?	Device Maker	HDO
Less than 100	8%	9%
100 to 500	17%	23%
501 to 1,000	20%	29%
1,001 to 5,000	31%	32%
5,001 to 25,000	18%	6%
25,001 to 75,000	5%	1%
More than 75,000	1%	0%
Total	100%	100%

Ponemon Institute

Advancing Responsible Information Management

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.

As a member of the **Insights Association,** we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.