2017 HIMSS Cybersecurity Survey

HIMSS North America

2017 HIMSS Cybersecurity Survey

Contents

1. Executive Summary

The **2017 HIMSS Cybersecurity Survey** provides insight into what healthcare organizations are doing to protect their information and assets, in light of increasing cyber-attacks and compromises affecting the healthcare sector.

THE FINDINGS IN THIS REPORT OFFER A "DIRECTIONALLY CORRECT" INSIGHT INTO THE CYBERSECURITY PERSPECTIVES AND PRACTICES OF INFORMATION SECURITY PROFESSIONALS IN U.S. HEALTHCARE ORGANIZATIONS

Based on the feedback from **126** U.S. health information security professionals, an analysis of the findings yielded a few notable themes, which are explored in greater detail in this report:

- Healthcare organizations with information security professionals on staff are taking steps to enhance their cybersecurity programs.
- Healthcare organizations with a chief information security officer or other senior information security leader have adopted holistic cybersecurity practices and perspectives in critical areas.
- Information security professionals at acute care providers have more specific concerns about cybersecurity, compared to their non-acute care provider counterparts.

2. Methodology/Respondent Demographics

Findings from the **2017 HIMSS Cybersecurity Survey** are based on the feedback from **126** qualified[1] **information security professionals** from a variety of U.S. healthcare organizations, participating in a web survey commissioned by HIMSS North America from April through mid-May 2017. Survey participants included **Chief Information Security Officers** (CISOs) and **HIMSS Cybersecurity Community** members.

Respondents generally identified themselves as either **executive management** or **non-executive management, with primary responsibility or some responsibility for their organization's information security program**. In addition, most respondents worked at a healthcare provider organization. Among those respondents at healthcare provider organizations, the vast majority of respondents worked for acute care providers, such as hospitals and other non-ambulatory care organizations.

Table 1: Position in organization

Label	N	percent
Executive Management	**54**	**42.9%**
Non-Executive Management (*e.g., mid-level or senior management, but not executive level*)	51	40.5%
Non-Management (*e.g., analyst, specialist, etc.*)	21	16.7%

Q. Which title best describes the position that you hold at your organization?

Table 2: Information security responsibility

Label	N	percent
Primary responsibility	**79**	**62.7%**
Some responsibility	32	25.4%
Sometimes, as needed	15	11.9%

Q. To what extent are you responsible for oversight or day-to-day-operations of the cybersecurity program at your organization?

[1] To participate in the survey, respondents had to have some level of oversight or day-to-day-operations of the cybersecurity program at their organization. Of the 155 individuals responding to the survey invite, 26 individuals indicate they had "no oversight/influence at all", and three individuals elected not to answer the question. These 29 individuals were therefore excluded from this survey.

Table 3: Type of organization

Label	N	percent
Acute Care Providers[2]	**63**	**50.0%**
Other[3]	38	30.2%
Non-Acute Care Providers[4]	15	11.9%
Business Associate[5]	10	7.9%

Q. Which of the following best describes the type of organization for which you work?

Please note: As respondents reflect a segment of the market with some type of information security responsibility, the findings in this report can be considered a "**directionally correct**" reflection of the cybersecurity perspectives and practices of information security professionals in U.S. healthcare organizations. Readers are encouraged to exercise caution in extrapolating the findings to broader audiences outside those represented in this report.

[2] Acute care providers included integrated delivery healthcare systems, multi-hospital system, critical access hospitals, rural hospitals, community or regional hospitals, and research hospitals.
[3] "Other" included health IT vendors, consultants, and payers.
[4] Non-acute care providers included ambulatory practices or physician practices, mental/behavioral health facilities, home health care, skilled nursing or long-term care facilities, and independent rehabilitation facilities.
[5] Business associates included health information exchanges and regional health information organizations.

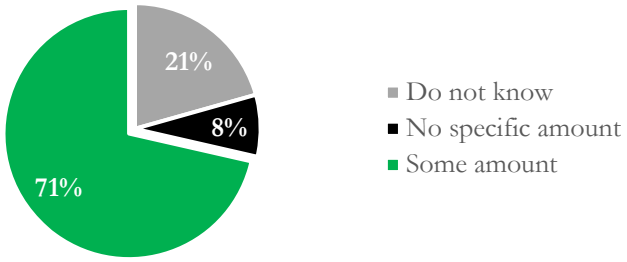
3. Findings

Observation 1: Healthcare Organizations with Information Security Professionals on Staff are Taking Steps to Enhance Their Cybersecurity Programs

The participants in this survey, all information security professionals within their respective healthcare organizations, are taking steps to enhance their cybersecurity programs. This observation is supported by the following data points:

1. **Budget Allocation**. The vast majority of respondents stated that their organizations (**71 percent**) allocate a specific part of their budget towards cybersecurity (Graph 1).

Graph 1: What percentage of your organization's current budget is allocated to cybersecurity?



Of the 90 respondents (**71 percent**) able to identify the percent of their organization's budget allocated for cybersecurity, 60 percent (N=54 respondents) claim cybersecurity commanded 3 percent or more of the budget (Table 4).

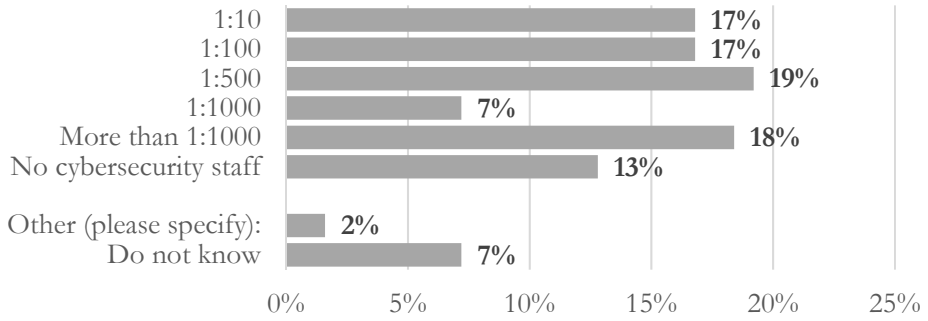
Table 4: Percent of Budget

Percent of Budget	N	percent
1-2 percent	36	40%
3-6 percent	29	32%
7-10 percent	15	17%
More than 10 percent	10	11%

However, 10 respondents (**7.9 percent**) indicated that no monies have been allotted for cybersecurity.

2. **Information Security Staffing**. **80 percent** of respondents indicate their organization employs cybersecurity staff. Specifically, **78 percent** of respondents were able to identify a cybersecurity staffing ratio, with **53 percent** reporting a ratio of **1:500 or lower** (Graph 2). The 1:500 ratio is significant because some researchers have found that a staff ratio of 1:500 is ideal for organizations that are information centric, have a considerable Internet exposure and a low risk appetite.[6]

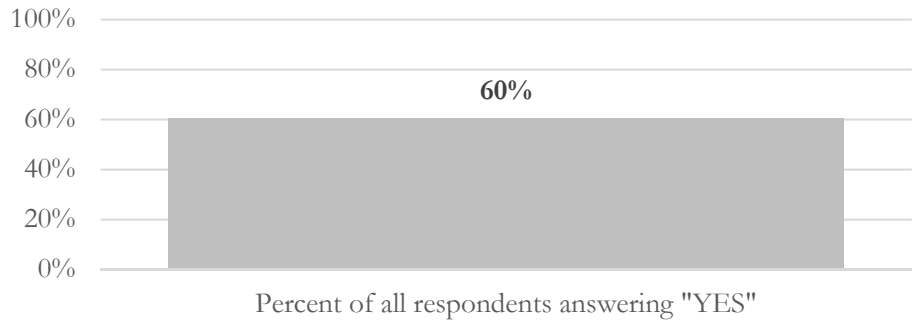
Graph 2: What is the approximate ratio of cybersecurity staff to IT users in your organization?



[6] *See Structuring the Chief Information Security Officer Organization*, *available at* https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf (*citing Tips and Guidelines for Sizing Your Information Security Organization* [Scholtz 2014]). Additionally, "[i]nformation security (IS) staff is typically 0.5% of total organizational staff (includes contractors, consultants, temporaries, and outsourced workers). This means that there is 1 security FTE for every 200 staff." *Id.* at 17 (*citing Information Security and Data Privacy Staffing Survey* [Wood 2012]). The authors of this paper also note that these figures are highly dependent upon the functions and activities that the CISO is responsible for performing and overseeing. *See id.*

3. **Information Security Leadership**. Over half of respondents (**60 percent**) indicate their organizations employ a senior information security leader, such as a Chief Information Security Officer ("CISO") (Graph 3). Essentially, these respondents' organizations have made the decision to dedicate an **executive role in information security** through this senior leader position, arguably making information security a business priority.[7]

Graph 3: Does your organization employ a senior information security leader (e.g. CISO)?



Benefits of a CISO

The inclusion of a senior information security leader in an organization is significant as it may help in the following ways:

- Provide deep knowledge and expertise in regard to achieving holistic information security in the healthcare environment
- Shape an organization's information security program with his or her in-depth knowledge about the threat landscape (including potential insider threat and cyber-attacks), methods and tools used for protecting information and IT assets, and analyzing and mitigating risks
- Lead an organization's information security program with holistic *and* business enabling perspectives
- Drive organizational change throughout an organization and establish priorities in light of the vision, needs, and mission of an organization's information security program
- Create a "culture" of cybersecurity, including helping to promote cybersecurity literacy and awareness
- Ensure that business and clinical operations, as well as workflow, are enabled (and not hampered by information security)[8]

Accordingly, in view of factors such as these and other considerations, it may be time for all healthcare organizations to evaluate whether it is time to hire a CISO or other

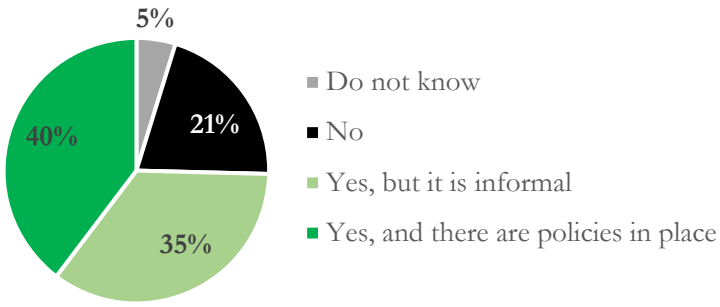
[7] According to the 2016 HIMSS Cybersecurity Study, 85.3% respondents stated that information security has increased as a business priority over the prior year.

[8] *See Preparing the Health Sector for Robust Cyber Defense*, *available at* http://www.himss.org/news/preparing-health-sector-robust-cyber-defense. *See also Health Care Industry Cybersecurity Task Force Report: Analysis and Recommendations*, *available at* http://www.himss.org/news/health-care-industry-cybersecurity-task-force-report-analysis-and-recommendations.

senior information security leader. As always, a proactive approach to security is much better than a reactive approach. Nonetheless, the catalyst for hiring a CISO (or equivalent) has, at times, been a major breach or other significant security incident.

4. **Insider Threat.** Three-quarters of respondents (**75 percent**) indicate that they have some type of insider threat management program at their organization (Graph 4).

Graph 4: Does your organization have an insider threat management program?



Insider threat may be characterized as unintentional or malicious.

An **unintentional insider** threat may be defined as follows: [9]

- An individual, such as a current or former employee, contractor, or business partner, who currently has, or previously had, authorized access to an organization's network, system or data;
- Through action *or* inaction and without malicious intent, the individual actually causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, and availability to the organization's information or information systems.

A **malicious insider** threat may be defined as follows:[10]

- An individual, such as a current or former employee, contractor, or business partner, who currently has, or previously had, authorized access to an organization's network, system or data;
- Has intentionally exceeded or has intentionally used that access in a manner that negatively affected the confidentiality, integrity, and availability to the organization's information or information systems.

In the healthcare context, examples of an unintentional insider threat include a workforce member or a contractor who leaves behind an unencrypted flash drive with patient information or who accidentally posts patient information publicly (thinking

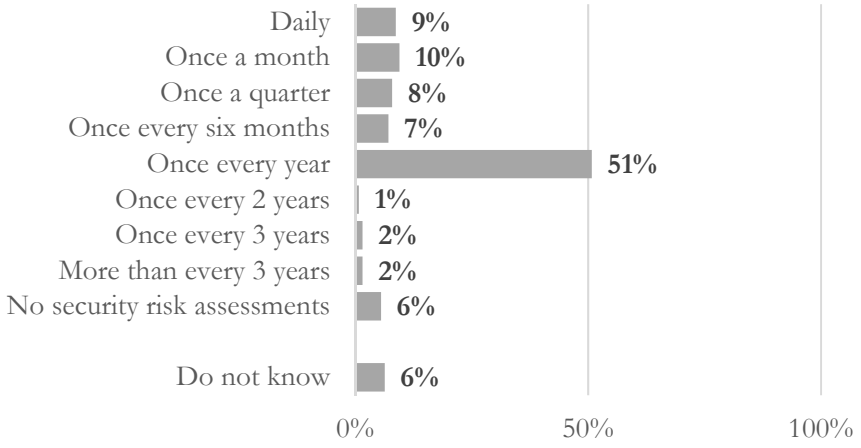
[9] *See Unintentional Insider Threats: A Foundational Study*, *available at* https://www.sei.cmu.edu/reports/13tn022.pdf.
[10] *See Common Sense Guide to Mitigating Insider Threats, Fifth Edition*, *available at* https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf.

that the information would be posted privately, such as on a patient portal). Examples of malicious insider threat include a workforce member who steals patient billing information to commit fraud or sets up a "logic bomb" to intentionally destroy the data of an organization based upon the occurrence of a certain event.

In either case, insider threat activity can go undetected for significant periods of time. Insider threat activity may be even more damaging than an external cyber-attack. For these reasons, it is a positive finding that so many respondents have indicated that they do have insider threat management programs. However, a formal insider threat management program may be more effective than an informal one. The formal insider threat management program may be consistently applied, enforced, and the organization may have formal policies, procedures, and sanctions in place.

5. **Risk Assessments**. The vast majority of respondents (**85 percent**) state that they conduct a risk assessment at least once a year (Graph 5).

Graph 5: How frequently are security risk assessments conducted at your organization?



One of the requirements of the HIPAA Security Rule is to conduct a security risk analysis (45 CFR §164.308(a)(1)(ii)(A)).[11] In addition, the meaningful use program has been a major driver in ensuring that healthcare providers do so. Healthcare providers have had to attest, under the meaningful use program, for each electronic health record ("EHR") reporting period that a security risk analysis has been conducted.[12]

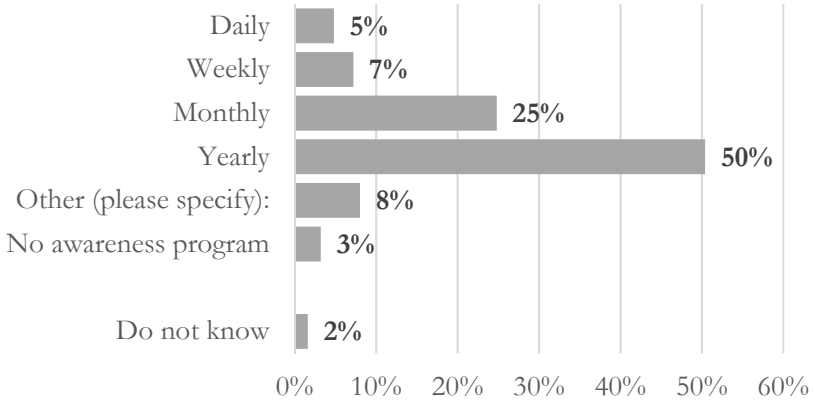
[11] In regard to periodic review and updates to the risk assessment, the US Department of Health and Human Services states the following: "The Security Rule does not specify how frequently to perform risk analysis as part of a comprehensive risk management process. The frequency of performance will vary among covered entities. Some covered entities may perform these processes annually or as needed…depending on circumstances of their environment." *See Guidance on Risk Analysis, available at* https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html ("Periodic Review and Updates to the Risk Assessment").

[12] Generally, the attestation is done on an annual basis.

Thus, many healthcare providers are now conducting security risk analyses at least once a year to meet this requirement.[13]

6. **Awareness**. The vast majority of respondents (**87 percent**) state that they conduct security awareness training classes for their staff at least once a year (Graph 6).

Graph 6: How frequently is security awareness training conducted at your organization

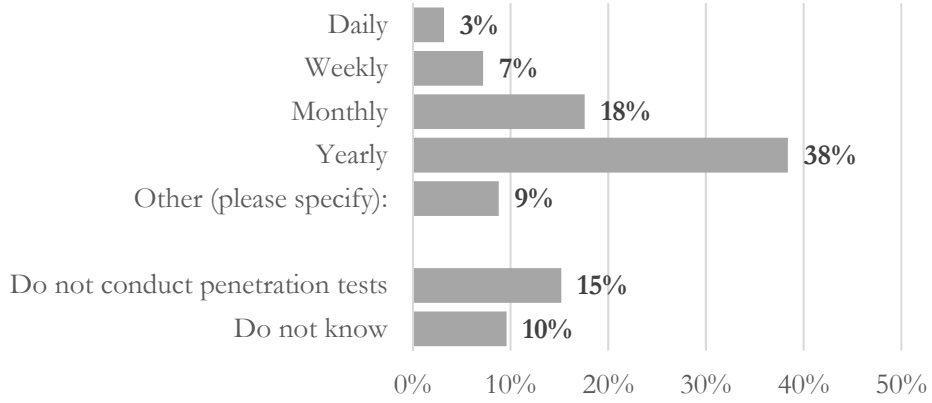


Security awareness and training are required under the HIPAA Security Rule as set forth in 45 CFR §164.308(a)(5). Furthermore, in helping to satisfy the risk analysis requirement, many providers have regularly conducted security awareness and training. As an example, a workforce member at a hospital may inadvertently click on a malicious link in an e-mail and infect his or her computer—and perhaps other systems that are connected to the hospital network, too. Mitigating this risk may include security awareness and training so that the workforce member knows how to detect a phishing e-mail, what to do with it, and how to report the incident to the IT department.

[13] Now, under the Quality Payment Program, it is anticipated that healthcare providers will continue doing the security risk analysis since it is a requirement of the Advancing Care Information category. *See Quality Payment Program: Advancing Care Information*, *available at* https://qpp.cms.gov/mips/advancing-care-information.

7. **Penetration Testing**. The vast majority of respondents (**75 percent**) indicate that they do regularly conduct penetration testing (Graph 7).

Graph 7: How frequently is penetration testing conducted at your organization?



According to NIST, penetration testing is a specialized type of assessment that is conducted on information systems or individual system components to identify vulnerabilities that may be exploited by adversaries.[14] As such, penetration testing allows the organization to test its security defenses through the penetration testing process. When properly done, penetration testing is not meant to cause damage, disruption, or harm to information systems or individual system components.[15]

Given the increase in volume, velocity, and numbers of cyber-attacks, many organizations recognize penetration testing as a best practice. Many conduct penetration testing exercises regularly. Penetration testing includes phases such as, but not limited to, information gathering, identifying vulnerabilities, and exploitation of the target.

However, penetration testing is not just limited to the technical environment, rather it may include the testing of administrative and physical safeguards as well.[16] As an example, mock phishing exercises of workforce members (or even information security staff) can be conducted to determine how well (or poorly) these individuals perform. In another example, a mock cyber-attack can be launched to gauge how well (or poorly) a computer security incident response team responds.

Essentially, one of the best ways to test an organization's cybersecurity defenses is to regularly conduct penetration testing. Otherwise, the "real test" of an organization's cybersecurity defenses may be in the face of an actual security incident (and, likely, a significant security incident or a breach).

---

[14] *See NIST Special Publication 800-53 (Rev. 4): Security Controls and Assessment Procedures for Federal Information Systems and Organizations CA-8 Penetration Testing, available at* https://nvd.nist.gov/800-53/Rev4/control/CA-8.

[15] In healthcare, some of these systems or components may be mission critical, such as electronic health record systems, medical devices, and other things. Accordingly, the penetration test should ideally be conducted by a qualified and experienced professional, especially one who has experience in the healthcare cybersecurity field.

[16] An information security professional (who is on the "blue team") may develop and/or implement administrative, physical, and technical safeguards to help protect information. In contrast, a person who is on the "red team" (a penetration tester) seeks to "test" the safeguards which are in place.

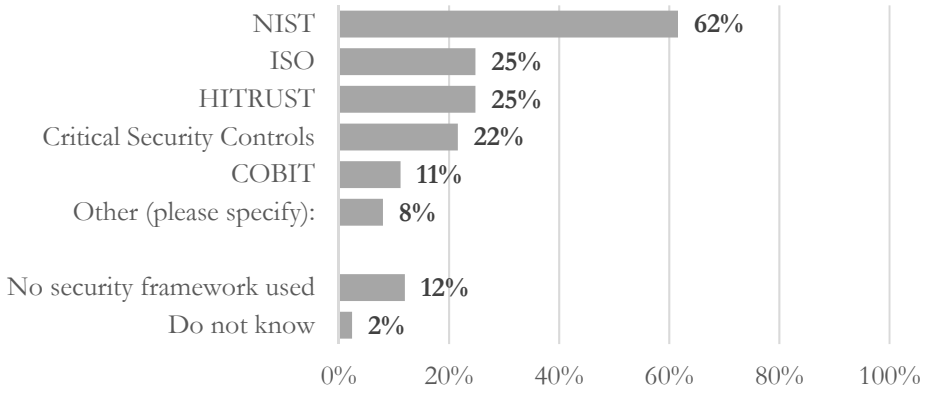
Observation 2: Healthcare Organizations with a CISO or Other Senior Information Security Leader Tend to Adopt Holistic Cybersecurity Practices and Perspectives in Critical Areas

The survey asked respondents to indicate whether or not their organization employed an information security leader, such as a Chief Information Security Officer or other senior information security leader. An analysis of the responses from respondents with a CISO or other senior information security leader revealed that their organizations have adopted holistic cybersecurity practices in a number of critical areas. Intuitively, this makes sense, as the role of a senior information security leader is to help drive organizational change and establish priorities for an organization's information security program.

1. **Security Frameworks**. *Widespread adoption of the NIST Cybersecurity Framework at organizations with CISOs or senior information security leaders.*

   The majority of all respondents (**86 percent**) indicate that their organizations use **at least one or more** security frameworks (Graph 8).

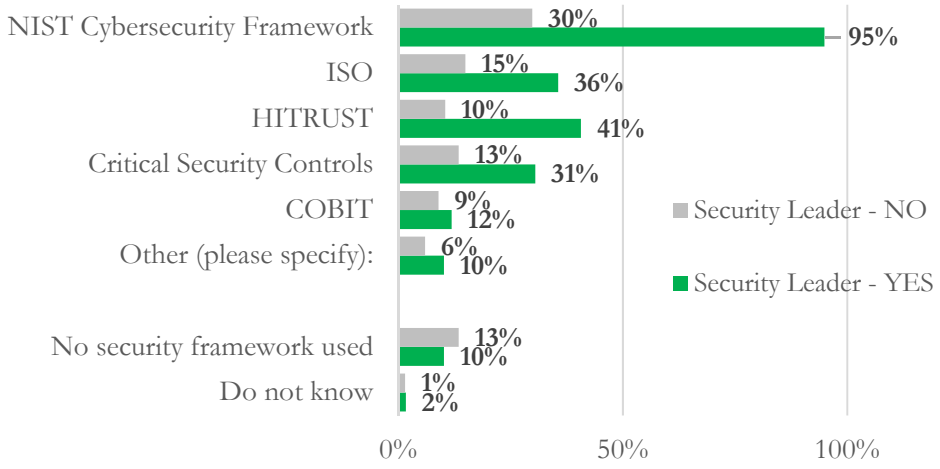
   Graph 8: Which of the following security framework(s) does your organization use? (*Please select all that apply.*)



Security Frameworks: Organizations with a CISO or Other Senior Information Security Leader

With a CISO or other senior information security leader, **95 percent** of organizations use the NIST Cybersecurity Framework with its core functions of identify, protect, detect, respond, and recover (Graph 9).[17]

Graph 9: Which of the following security framework(s) does your organization use?



Many stakeholders in critical infrastructure sectors, including the healthcare and public health ("HPH") sector, have adopted the NIST Cybersecurity Framework. The NIST Cybersecurity Framework is the result of a public-private partnership with the United States government and private sector stakeholders.

The NIST Cybersecurity Framework continues to evolve to this day, with input from the private sector. In addition, it is written in such a way that technical, non-technical, and executive audiences can more easily read and understand it.

HITRUST has a common security framework ("CSF") which is a popular security framework in the healthcare sector with **41 percent** of respondents indicating that their organizations have adopted it.[18] In addition, HITRUST has mapped its framework to the NIST Cybersecurity Framework.[19] Accordingly, many healthcare cybersecurity professionals are aware of the HITRUST common security framework and many have used it as well.

The International Organization for Standardization ("ISO") has a popular security framework which many healthcare cybersecurity professionals have adapted to the healthcare sector. **41 percent** of respondents indicate that their organizations have adopted it. Specifically, ISO/IEC 27000 is a family of standards that helps

[17] *See* NIST Cybersecurity Framework, *available at* https://www.nist.gov/cyberframework.
[18] *See* HITRUST CSF, *available at* https://hitrustalliance.net/hitrust-csf/.
[19] *See id.*

organizations keep information assets secure. Popular standards include ISO/IEC 27001,[20] ISO/IEC 27002,[21] and ISO/IEC 80001.[22]

In summary, security frameworks help organizations build a comprehensive security program with guidance on how to identify and prioritize actions for reducing cybersecurity risk. Many CISOs and other senior information security leaders know that HIPAA compliance alone is not enough and that adopting and implementing a robust security framework is a necessary prerequisite for having a robust security program.

Security Frameworks: Organizations without a CISO or Other Senior Information Security Leader

In contrast, there is a lot more variety in terms of which security framework an organization has adopted among organizations without a CISO or other information security leader. Leading the pack is the NIST Cybersecurity Framework with **30 percent** of such respondents stating that their organizations are using it. However, there does not seem to be as strong of a preference for other security frameworks, according to respondents at these organizations.

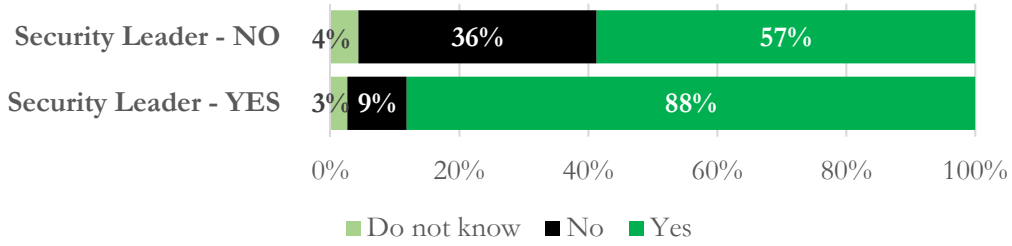
[20] ISO/IEC 27001 is an international standard which sets forth requirements for establishing, implementing, maintaining, and continually improving an information security management system ("ISMS") within the context of an organization. *See ISO/IEC 27000 family - Information security management systems, available at* https://www.iso.org/isoiec-27001-information-security.html.
[21] ISO/IEC 27002 is an international standard for good practices in information security. *See ISO/IEC 27002:2013, available at* https://www.iso.org/standard/54533.html.
[22] ISO/IEC 80001-1 is an international standard for the application of risk management for IT networks incorporating medical devices. *See IEC 80001-1:2010, available at* https://www.iso.org/standard/44863.html.

2. **Procurement**. *Widespread cybersecurity due diligence of technology products and services (pre-acquisition) at organizations with CISOs or senior information security leaders.*

Procurement: Organizations with a CISO or Other Senior Information Security Leader

With a CISO or other senior information security leader at the helm, the vast majority of these respondents (**88 percent**) conduct cybersecurity due diligence on technology products and services, prior to acquisition (Graph 10).

Graph 10: Do you include a cybersecurity assessment as part of your due diligence analysis when acquiring a product or service for your organization?



Simply buying and implementing *any* product or service "off the shelf" could introduce an organization to significant risks.[23] For example, malware may be implanted (intentionally or unintentionally) in hardware, software, or other components somewhere along the IT supply chain.[24] Hardware, software, mobile devices, medical devices, and other components may have severe vulnerabilities and, thus, could expose the organization to significant risk (if such vulnerabilities were successfully exploited).[25] Moreover, default configurations or misconfigurations of a product or service may also potentially expose an organization to significant risks. (The same is true in terms of running outdated or deprecated software.)[26]

In light of the foregoing findings, if a healthcare organization is looking to purchase a technology product or service from a vendor, it is generally a best practice to do the appropriate due diligence. Merely buying a product or service off the shelf, based upon vendor's claims and statements alone, may be a recipe for disaster. An ounce of prevention is worth a pound of cure. So, it may be worthwhile to carefully select and vet technology products and services from technical, business, and legal due diligence

[23] *See Navigating the IT Market with Due Diligence, available at* https://gcn.com/articles/2017/07/31/navigating-the-it-market-with-due-diligence.aspx.
[24] A recent international malware outbreak (NotPetya) has been attributed to a software supply chain attack. *See also A2: Analog Malicious Hardware*, *available at* http://static1.1.sqspcdn.com/static/f/543048/26931843/1464016046717/A2_SP_2016.pdf) *and* the HIMSS Healthcare and Cross-Sector Cybersecurity Reports, *available at* http://www.himss.org/cyberreport.
[25] For example, a critical buffer overflow vulnerability may exist for an application that, if exploited by an attacker, may lead to arbitrary code execution. The application may exist on a computer, in the cloud, on a virtual machine, or even as an embedded application within a device.
[26] *See Health Care Industry Cybersecurity Task Force: Report on Improving Cybersecurity in the Health Care Industry*, *available at* https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

perspectives to ensure that the product or service that is ultimately selected by an organization is the right one, given its risk appetite, goals, vision, and mission—including in light of potential cybersecurity risks and concerns.[27]

Procurement: Organizations with a CISO or Other Senior Information Security Leader

On a positive note, **88 percent** of respondents from organizations with a CISO or other information security leader indicated that they do a cybersecurity assessment as part of their due diligence analysis when acquiring a product or service (Graph 10).

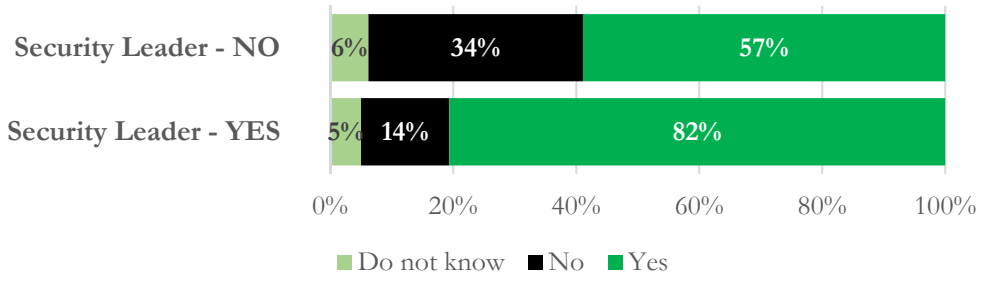
Procurement: Organizations without a CISO or Other Senior Information Security Leader

In contrast, only **57 percent** of respondents from organizations without a CISO or other senior information security leader indicated that they do a cybersecurity assessment as part of their due diligence analysis when acquiring a product or service (Graph 10).

3. **Education and Training**. *Generally supportive of cybersecurity staff in education and training to further their cybersecurity skills and knowledge.*

Cybersecurity is a field that is constantly changing. There are always new threats, threat actors, attack vectors, vulnerabilities, and exploits. Plus, operating systems, applications, software components, and devices may frequently change in an environment such as healthcare. Thus, protecting information and IT assets can be a moving target. As a result, education and training are necessary for cybersecurity staff to further their skills and knowledge. Stale knowledge and skills may hurt (not help) the security posture of an organization.

Graph 11: Does your organization support cybersecurity staff in education and training to further their cybersecurity security skill set and knowledge?



[27] *See id.* at 23.

Education and Training: Organizations with a CISO or Other Senior Information Security Leader

Accordingly, **82 percent** of respondents at healthcare organizations with a CISO or senior information security leader at the helm indicate that their organizations are generally supportive of cybersecurity staff in terms of education and training to help further their skill set and knowledge (Graph 11).

In the survey, we did not specify whether the "support" was financial (e.g., paying for a security course or workshop) or just simply letting the cybersecurity staff member take time off to further their education and training. Nonetheless, ensuring that a healthcare organization supports its cybersecurity staff members by allowing them to take additional education and/or training to further their knowledge or skill set is a best practice. It is a holistic (and necessary) step towards achieving a proactive security posture.

Education and Training: Organizations without a CISO or Other Senior Information Security Leader

In contrast, in organizations without a CISO or senior information security leader at the helm, significantly fewer respondents (**57 percent**) indicated that their organizations are supportive of cybersecurity staff in terms of education and training (Graph 11). It can be difficult for such staff, then, to update their knowledge and skills without the support of their organization. Barriers may include lack of financial resources and lack of time.

4. **Business Continuity and Disaster Recovery.** *More likely to test for failure of technology resources for business continuity and disaster recovery testing purposes.*

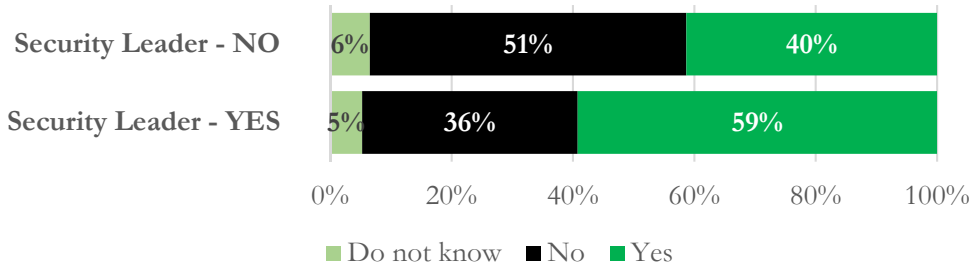
In light of the wave of ransomware, denial of service, and wiper attacks affecting healthcare and other critical infrastructure sectors, an increasing number of organizations are more closely scrutinizing their business continuity and disaster recovery plans.

On a related note, technology resources may not always be available or accessible. Natural or manmade disasters may cause disruption or unavailability of these resources. As an example, a natural disaster may cause a data center to be unavailable (e.g., flash flood, tornado, etc.). A manmade disaster can range from anything such as a sprinkler system malfunction (or accident), a fire, a denial of service ("DoS") attack, a ransomware attack, a logic bomb, or other things. In addition, hardware failures, power failures, and even actions or inactions by unintentional or malicious insiders may cause technology resources to fail.

Business Continuity and Disaster Recovery: Organizations with a CISO or Other Senior Information Security Leader

In the survey, **59 percent** of respondents with CISOs or other senior information security leaders at their organizations indicate that their organization tests for failure of technology resources for business continuity and disaster recovery purposes (Graph 12).

Graph 12: Do you conduct mock exercises to test for failure of technology resources at your organization (*e.g., equipment breakdown, software or hardware crashes, natural disasters, human error, etc.*)?

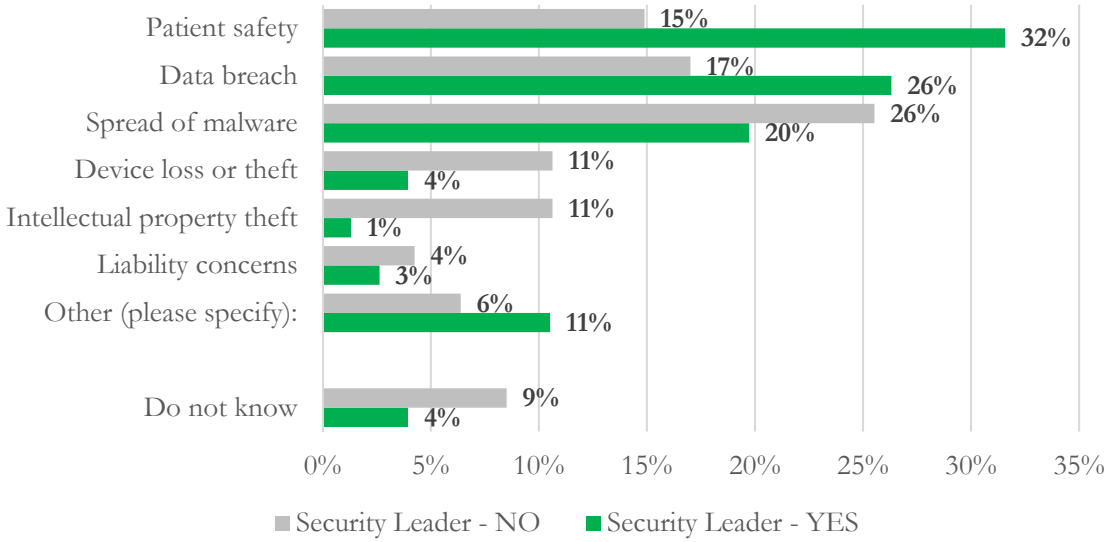


Business Continuity and Disaster Recovery: Organizations without a CISO or Other Senior Information Security Leader

However, significantly fewer respondents at organizations *without* such a senior security leader (**40 percent**) report doing such testing (Graph 12). The consequences of **not** testing for technology failure, include having to deal with technology failure on an *ad hoc* basis (which can be chaotic) or putting an organization's business continuity and disaster recovery plan to the test for the first time in the face of an actual incident (i.e., a trial by fire situation).

5. **Medical Device Security**. *Patient safety, data breaches, and spread of malware are top concerns regarding medical device security amongst CISOs and other senior information security leaders at healthcare organizations.*

   Graph 13: What is your greatest concern about medical device security at your organization?



Patient Safety is the #1 Concern.

Medical Device Security—Patient Safety: Organizations with a CISO or Other Senior Information Security Leader

Patient safety, including issues such as patient harm or serious injury to the patient, is a top concern regarding medical device security, according to **32 percent** of respondents at organizations with CISOs or other senior information security leaders (Graph 13). Such senior information security leaders know that cyber-attacks on medical devices may lead to serious consequences, especially if the medical device is life-sustaining or life-saving. A hacked insulin pump may deliver a fatal bolus of insulin to a patient. A "connected" pacemaker may deliver a fatal shock to a patient. The technical know-how and skill set exists among cyber adversaries to compromise these devices. Unfortunately, it is a matter of "when" and not "if." This is not a theoretical problem.

Medical Device Security—Patient Safety: Organizations without a CISO or Other Senior Information Security Leader

In contrast, only **15 percent** of respondents at organizations without a senior information security leader indicate that patient safety is a concern (Graph 13). (Patient safety ranked **third**, in terms of top concerns relating to medical device security, for organizations without the senior information security leader.)

Data Breach is the #2 Concern.

Historically, data breaches have been a leading concern among healthcare organizations. However, in light of targeted and untargeted campaigns by sophisticated threat actors (and others), especially in the last several years, this perspective change. As we have seen, thousands or millions of patient records have been breached. This, too, is the tip of the iceberg.

Not only is the prospect of a massive breach concerning, but it can also be costly and disruptive to any affected organization. Nonetheless, the prospect of a data breach is not as concerning as patient safety, according to respondents with CISOs or other senior information security leaders at their healthcare organizations.

Medical Device Security—Data Breach: Organizations with a CISO or Other Senior Information Security Leader

26 percent of respondents with such senior security leaders reported data breaches were a secondary concern in regard to medical device security (Graph 13).

Medical Device Security—Data Breach: Organizations without a CISO or Other Senior Information Security Leader

Data breaches are also the **#2** concern for respondents without CISOs or other senior information security leaders at their organizations (Graph 13).

Spread of Malware is the #3 Concern.

Medical devices (just like unpatched and/or unsupported software, unpatched and/or unsupported operating systems, and misconfigurations) have the potential of being compromised by an attacker (with some medical devices being easier to infiltrate than others). Such (successfully) compromised devices can serve as a "pivot point" into an organization's network environment.

Furthermore, if an organization's network is a "flat" network (which is not segmented), a malware infection could potentially spread to each and every vulnerable system on the network. For example, in the case of a malware with worm-like capabilities, the malware may self-replicate without the need of human intervention.[28] The consequences of such an infection which spreads pervasively throughout an organization can be quite severe, ranging from damaged IT infrastructure, disruptions in operations, significant data loss, etc. Naturally, this is a nightmarish scenario that information security professionals want to avoid.

Medical Device Security—Spread of Malware: Organizations with a CISO or Other Senior Information Security Leader

Accordingly, the spread of malware on the same network is another top concern among **20 percent** of respondents at organizations with a CISO or other senior information security leader (Graph 13).[29]

However, senior information security leaders at healthcare organizations—and those that work for them—often bring in-depth cybersecurity knowledge and expertise to the table. Thus, vulnerabilities are addressed and risks are mitigated to the best extent possible.

Further, senior information security leaders may bring in-depth knowledge about the threat landscape and contribute to the organizational "culture" of cybersecurity (such as by promoting cybersecurity literacy and awareness among workforce members and others). In addition, such leaders can ensure that cybersecurity is a priority at their respective organizations. This can lead to a different perspective and potentially a proactive focus on cybersecurity as a whole.

Medical Device Security—Spread of Malware: Organizations without a CISO or Other Senior Information Security Leader

Yet, respondents at organizations *without* a senior information security leader tend to indicate that the spread of malware on the same network is a **top concern** (**26 percent**) (Graph 13). These organizations (that lack a senior information security leader) may not have personnel with the in-depth cybersecurity knowledge and

[28] The WannaCry and NotPetya malware are reported to have worm-like capabilities and, thus, possess the ability to spread across computer networks. *See UPDATED: #WannaCry #WCry Ransomware: an International Cyber Threat*, *available at* http://www.himss.org/news/wannacry-wcry-ransomware-international-cyber-threat and *NotPetya/Petya/ExPetr: Another Global Malware Epidemic #HITsecurity*, *available at* http://www.himss.org/news/notpetya-another-global-malware-epidemic-hitsecurity.

[29] An example of malware has the capability to spread across the network is the WannaCry ransomware. The WannaCry ransomware has the capability to spread from machine-to-machine on the same network. *See #WannaCry #WCry Ransomware: an International Cyber Threat*, *available at* *http://www.himss.org/news/wannacry-wcry-ransomware-international-cyber-threat*.

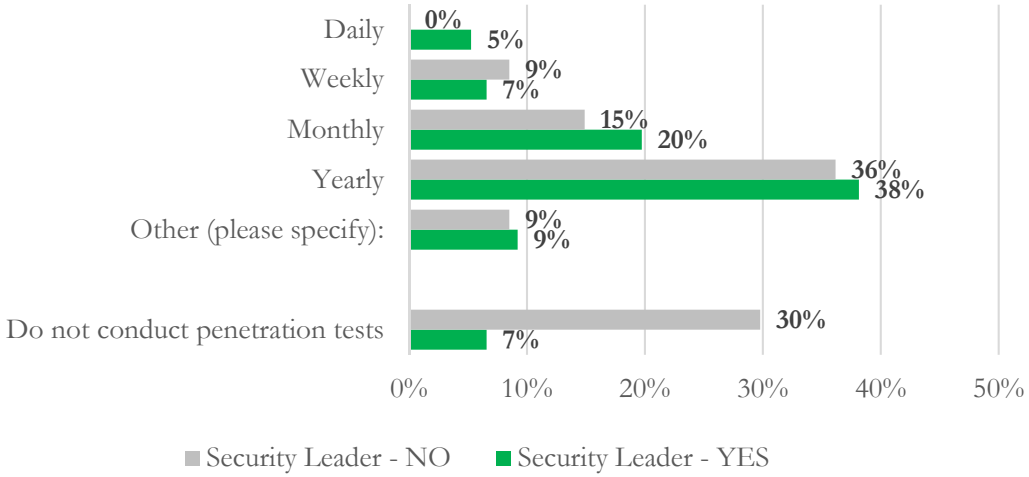
expertise of such a senior information security leader. In addition, such organizations may not have the "executive at the table" that can bring about a proactive stance and approach to cybersecurity (including ensuring that such things as medical device and network security are addressed).

6. Penetration Testing. *Penetrating testing is regularly done.*

Penetration testing services are more in demand in light of recent, significant cyber-attacks affecting the healthcare sector. Thus, there is a growing awareness amongst healthcare stakeholders generally that their defenses need to be tested. Hopefully, such healthcare stakeholders are evaluating and potentially implementing the recommendations of the penetration tester's report (as appropriate). A penetration test report that sits on the shelf has limited value to an organization. (The same is true for risk assessment reports, or for any such report which is not carefully evaluated and analyzed.)

Furthermore, penetration testing is important, as it tests the organization's cybersecurity defenses (including people, processes, and technology). For example, while an authorized penetration test has been approved by the organization, the security incident response team may not necessarily know about the test. Accordingly, the penetration test may test the skill and acumen of the security incident response team. In another example, a penetration tester may send phishing e-mails to gauge how workforce members respond to them.

Graph 14: How frequently is penetration testing conducted at your organization?



Penetration Testing with Regular Frequency: Organizations with or without a CISO or Other Senior Information Security Leader

There is no notable difference between organizations with or without a CISO or senior information security leader, in terms of the frequency of conducting penetration tests **when the organization decides to conduct such tests**. In other words, such respondents indicated that penetration testing is conducted at their organizations on a regular basis. Most of these respondents indicated that their organizations conduct penetration testing on a **yearly** basis (**38 percent** with a security leader; **36 percent** without a security leader) (Graph 14).

No Penetration Tests Conducted At All: Organizations with a CISO or other Information Security Leader

Only **7 percent** of respondents at organizations with a CISO or other information security leader indicated that their organizations **do not** conduct penetration tests at all. Accordingly, **93 percent** of respondents at such organizations do conduct penetration tests in one form or another (Graph 14). Thus, there seems to be a wide consensus that penetration testing is important and vital to the "health" of the organization's information security program.

No Penetration Tests Conducted At All: Organizations without a CISO or other Information Security Leader

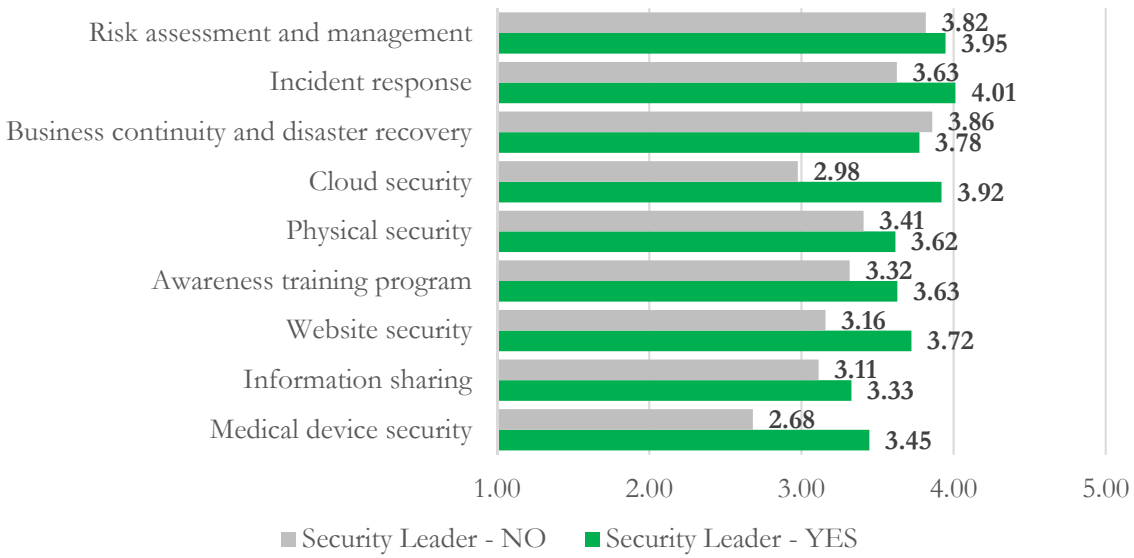
In contrast, organizations *without* a CISO or senior information security leader are much more likely *not* to conduct penetration tests at all (**30 percent**) than those with a CISO/senior information security leader (**7 percent**) (Graph 14). Organizations that do not conduct penetration tests at all may have various reasons for not doing so. Penetration test services can be expensive (especially when they are done by third parties). In addition, organizations without such security leadership may not realize the benefits that a penetration test may provide.

7. **Cybersecurity Priorities**. *CISOs and senior information security leaders tend to give a much higher priority to "open door" concerns, such as cloud, medical device, and website security.*

In the 2015 HIMSS Cybersecurity Survey and the 2016 HIMSS Cybersecurity Study, we previously asked healthcare organizations about whether information security has increased as a business priority over the past year. The results from both years were roughly comparable with 87 percent of respondents from the 2015 survey and 85 percent of respondents from the 2016 study stating that information security had indeed increased as a business priority over the previous year. However, in this survey, we decided to ask respondents in more granular detail what their specific cybersecurity priorities are.

Respondents were presented with a list of nine security focus areas and asked to rate their top security priorities for the coming year (where *"Not a priority"* = 1; *"Essential"* = 5).

Graph 15: To what extent are these issues a priority for your organization's security program in the coming year?



Cybersecurity Priorities: Organizations with a CISO or Other Senior Information Security Leader

Cloud, medical device, and websites can all be "open doors" to any organization. From an attacker's perspective, he or she may only need one "open door" to access in order to infiltrate an organization. These "open doors" can include cloud, medical device, and website resources. These resources may be accessible via the Internet and, hence, potentially open to the world. Thus, these doors need to be secured (as much as they can be).

Respondents from organizations with a CISO or other senior information security leader varied notably from organizations *without* a CISO/senior information security leader in three areas: **cloud security** (**3.92/5**), **medical device security** (**3.45/5**), and **website security** (**3.72/5**) (Graph 15).

Cybersecurity Priorities: Organizations without a CISO or Other Senior Information Security Leader

In contrast, organizations without a CISO or other senior information security leader may either not know to make these items a priority *or* may lack the organizational will or clout to make these things a priority. Those respondents without a senior information security leader indicate that cloud security (**2.98/5**), medical device security (**2.68/5**), and website security were moderate priorities (**3.16/5**) (Graph 15). Instead, more of a priority was given to risk assessment and management (**3.82/5**) and incident response (**3.63/5**) (Graph 15).

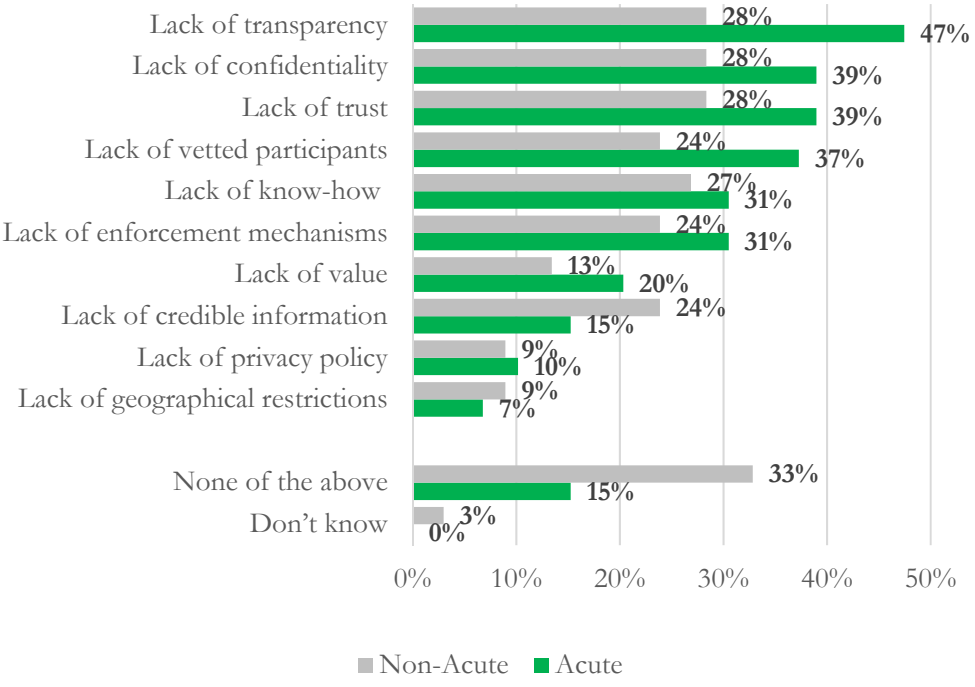
Observation 3: Information Security Professionals at Acute Care Providers Have More Specific Concerns about Cybersecurity, Compared to Their Non-acute Care Provider Counterparts

Respondents generally identified themselves as working for either an **acute care** provider (e.g., hospitals) or a **non-acute care** provider type of organization (e.g., ambulatory care organizations such as physician practices, home health agencies, etc.).

Based upon an analysis of responses from information security professionals at these types of healthcare organizations, respondents at acute care providers have more specific concerns about cybersecurity, compared to their non-acute care provider counterparts.

1. **Information Sharing Barriers.** The top concerns of information security professionals at **acute care providers** regarding information sharing are **lack of transparency** (**47 percent**), **lack of confidentiality** (**39 percent**), **lack of trust** (**39 percent**), and **lack of vetted participants** (**37 percent**) (Graph 16).

   Graph 16: Which of the following challenges do you have in exchanging your internal organizational information regarding cybersecurity threats, vulnerabilities, mitigation, and security incidents with external organizations?
   (*Please check all that apply.*)



Traditionally, many healthcare organizations have not participated in external information sharing with others in regard to cyber threat indicators, defensive measures, mitigation information, and other information (such as for situational awareness). In addition, those that have participated in external information sharing with others *may* be very cautious about what they decide to share and with whom. Thus, information sharing *may*, at times, occur within a "closed circle" of trusted and vetted colleagues and within a forum where the rules of engagement are clear (and enforced, as appropriate).

Lack of Transparency is the #1 Concern: *What happens with the information I share with others?*

A very common question that is asked by information security professionals at acute care providers in regard to an information sharing opportunity is the following: What happens with the information that I share with others? In other words, such information that is shared across with others could potentially be used against that individual and/or his or her organization. Some organizations, too, have liability concerns associated with information sharing. (Thus, some organizations choose to consume information, instead of divulging information to others.)

Acute Care Providers: Lack of Transparency and Information Sharing Barriers

For reasons such as the foregoing, **47 percent** of respondents, and namely information security professionals at acute care providers, indicate that this lack of transparency is a top barrier to information sharing (Graph 16).

Non-acute Care Providers: Lack of Transparency and Information Sharing Barriers

In contrast, however, only **28 percent** of respondents, and namely information security professionals at non-acute care providers, indicate that this lack of transparency is a barrier to information sharing (Graph 16). In addition, there are a number of other information sharing barriers that are also concerns by roughly the same amount of respondents (Graph 16).

Lack of Confidentiality is the #2 Concern: *Lack of confidentiality, lack of trust, and lack of vetted participants.*

Exploring further the barriers to information sharing, lack of confidentiality, lack of trust, and lack of vetted participants can be characterized as "interrelated" in that each barrier can depend upon the other.

First, there may be no guarantees that the information shared will be held in confidence vis-à-vis the information sharing forum or platform. There may also be a lack of an enforcement mechanism to ensure that any information shared will be kept in strict confidence. Thus, a lack of confidentiality may deter a healthcare organization from participating in information sharing at all. Or, if it does participate, the organization may listen more than "share."

Second, there may be a lack of trust. Thus, there may be a lack of a comfort level with sharing information in view of the absence of trust amongst the parties doing the information sharing. Information sharing with people (and entities) whom you know is much different from information sharing with people (or entities) you really do not know. In addition, there may be a lack of trust in the information being shared as well.

Third, there may be a lack of vetted participants. The information sharing forum or platform may be open to the public or anyone (or almost anyone) may be able to sign up. In such a case, this, too, may deter information sharing due to the *lack* of a "closed circle" of participants.

Acute Care Providers: Lack of Confidentiality and Information Sharing Barriers

In light of the foregoing, the second biggest concern among such information security professionals was in regard to a **lack of confidentiality** (**39 percent**), **lack of trust** (**39 percent**), and a **lack of vetted participants** (**37 percent**) (Graph 16).

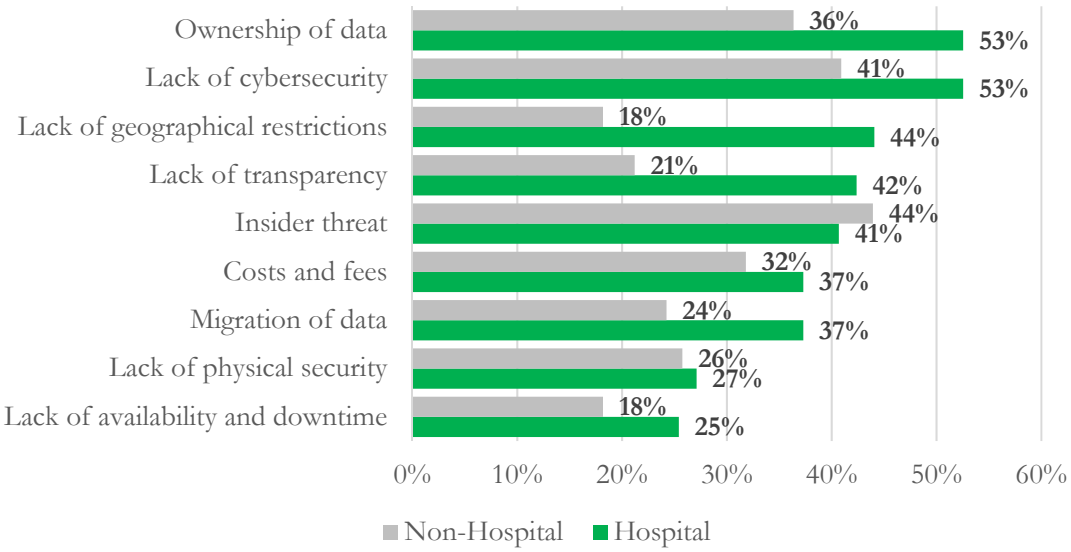
Based upon these concerns, having trusted and vetted participants within a "known group" (i.e., a closed circle) with information being shared in the strictest of confidence may help to encourage information sharing amongst information security professionals at acute care providers.

Non-acute Care Providers: Lack of Confidentiality and Information Sharing Barriers

In contrast, the concerns about information sharing from information security professionals at **non-acute care providers** were relatively non-specific. Respondents from non-acute care providers gave virtually equal weight to many of the identified barriers to information sharing (e.g., lack of confidentiality (**28 percent**), lack of trust (**28 percent**), lack of vetted participants (**24 percent**), lack of know-how (**27 percent**), enforcement mechanisms (**24 percent**), etc.) (Graph 16).

2. **Cloud Security.** Information security professionals at **acute care providers** have concerns about **cloud security**, especially in terms of **ownership of data** (**53 percent**), **lack of cybersecurity** (**53 percent**), **insider threat** (**41 percent**), **lack of transparency** (**42 percent**), and **lack of geographical restrictions** (**44 percent**) (Graph 17).

Graph 17: Which of the following security concerns do you have surrounding the use of the cloud at your organization?
(Please check all that apply.)



Ownership of Data and Lack of Cybersecurity are the #1 Concerns

Ownership of data and Cloud Security Concerns

The Office for Civil Rights at the US Department of Health and Human Services has issued guidance that a business associate (which can include a cloud service provider) of a covered entity may **not** block or terminate access to the protected health information maintained by the business associate for or on behalf of the covered entity.[30]

Nonetheless, information security professionals at acute care providers are still concerned about what happens to the entity's protected health information at the end of the contract or business relationship with the cloud service provider. This is what providers generally mean in terms of "ownership" of data.

[30] *See May a Business Associate of a HIPAA Covered Entity Block or Terminate Access by the Covered Entity to the Protected Health Information (PHI) Maintained by the Business Associate For or On Behalf of the Covered Entity?, available at* https://www.hhs.gov/hipaa/for-professionals/faq/2074/may-a-business-associate-of-a-hipaa-covered-entity-block-or-terminate-access/index.html.

Acute Care Providers: Ownership of Data and Cloud Security Concerns

The top concern of information security professionals at acute care providers pertains to ownership of data (**53 percent** of respondents at acute care providers) (Graph 17). Acute care providers may especially be concerned about the disposition of its data (in possession of the cloud service provider) at the end of the contract (or business relationship) with the cloud service provider. For example, if there is a fee dispute or other dispute, can the acute care provider get its data back? Or, can the cloud service provider hold the data hostage?

Non-acute care providers: Ownership of Data and Cloud Security Concerns

In contrast, ownership of data for non-acute care providers were less of a concern. In particular, only **36 percent** of these respondents had a concern about ownership of data (Graph 17).

Lack of cybersecurity and Cloud Security Concerns

In the past few years, there have been more reports of breaches and cyber-attacks affecting cloud service providers. Coupled with concerns such as insider threat and lack of transparency into the information security operations (and policies and procedures) of the cloud service provider, information security professionals at acute care providers may be hesitant to go "to the cloud." However, some organizations have taken advantage of cloud services due to business necessity, convenience, and other factors.

Acute care providers: Lack of Cybersecurity and Cloud Security Concerns

Lack of cybersecurity, as it relates to cloud service providers, was also a top concern among **53 percent** of respondents at acute care providers (Graph 17).

Non-acute care providers: Lack of Cybersecurity and Cloud Security Concerns

In contrast, a lack of cybersecurity was identified as a concern among **41 percent** of respondents at non-acute care providers (Graph 17). However, these respondents identified other concerns that were perceived just about as important. These concerns include insider threat (**44 percent**) (Graph 17).[31]

Nonetheless, IT security professionals at acute care organizations are still concerned about what happens to the entity's protected health information at the end of the contract or business relationship with the cloud provider. Some cloud providers may be cognizant of OCR's guidance. However, others may not be.

[31] Insider threat has been defined previously in this report. Please see the discussion on insider threat at pages 10 to 11 of this report.

Insider Threat, Lack of Transparency, and Lack of Geographical Restrictions are the #2 Concerns

Insider Threat and Cloud Security Concerns

Unintentional insider threat or malicious insider threat may exist in the context of cloud computing. An example of an unintentional insider threat may be an action or inaction by a workforce member of the cloud service provider which results in a leak of customer information from the cloud (e.g., resulting from a misconfiguration). An example of a malicious insider threat is that cloud service providers can, in some situations, have administrative access to customer information. (This is sometimes the case in regard to software as a service ("SaaS") applications.) Thus, a malicious insider threat may exist in regard to potential abuse or misuse of administrative rights by the cloud service provider workforce member (e.g., intentional data leakage or stealing of data).

Acute care providers: Insider Threat and Cloud Security Concerns

Accordingly, insider threat, as it relates to cloud security, was another top concern (**41 percent**) among respondents at acute care providers (Graph 17).

Non-Acute care providers: Insider Threat and Cloud Security Concerns

Similarly, **44 percent** of respondents at non-acute care providers also were concerned about insider threat as it relates to cloud security (Graph 17).

Another top concern of respondents at acute care providers pertains to the lack of cybersecurity (i.e., lax security) of cloud service providers.

Lack of transparency and Cloud Security Concerns

Cloud service providers sometimes are perceived to be not very transparent about their cybersecurity practices and operations. For example, a cloud service provider may refuse to divulge the most recent results of a risk assessment. (However, this may be for valid, *bona fide* reasons, such as safeguarding the security of its customer data and infrastructure.) Or, a cloud service provider may not be forthcoming about the cause of recent outages or downtime.

Acute care providers: Lack of transparency and Cloud Security Concerns

A top concern among respondents (**42 percent**) at acute care providers was the lack of transparency as it relates to cloud service providers and cloud security in particular (Graph 17).

Lack of geographical restrictions and Cloud Security Concerns

Many acute care providers have traditionally sought out US-based cloud service providers, in part, due to concerns about HIPAA. However, the Office for Civil Rights at the US Department of Health and Human Services ("OCR") has clarified that a covered entity (or business associate) may enter into a business associate

agreement with a cloud service provider that is outside of the United States. The cloud service provider must comply with the applicable requirements of HIPAA.[32]

But, OCR also cautioned that HIPAA does **not** include requirements specific to the protection of electronic protected health information ("ePHI") processed or stored by a cloud service provider, or any other business associate, outside the United States. [33] OCR has also noted that risks to such ePHI vary greatly, depending upon the geographic location and that outsourcing storage or other services for ePHI overseas may increase the risks and vulnerabilities to the information or present special considerations with respect to enforceability of privacy and security protections over the data. [34]

Acute care providers: Lack of geographical restrictions and Cloud security concerns

A good proportion of respondents from acute care providers (**44 percent**) indicated that the lack of geographical restrictions, as it pertains to cloud providers and cloud security in particular, was a top concern. It is not unusual for entities, such as acute care providers, to prefer US-based cloud service providers and, specifically, those that will store and maintain their data only in the United States (and not elsewhere). This may be due to their concerns about HIPAA compliance. However, it may be due to other factors, such as data privacy laws.

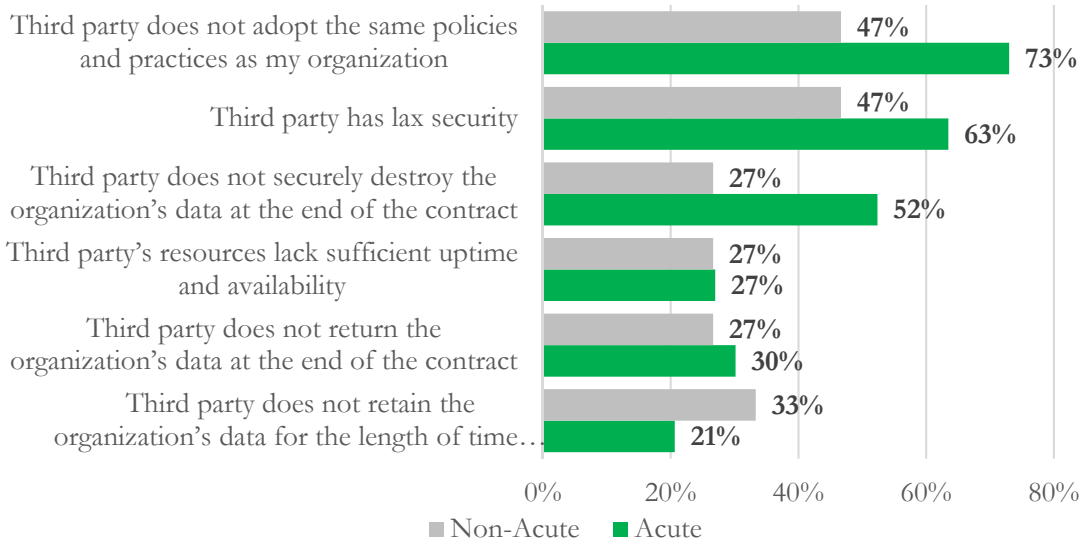
Non-acute care providers: Lack of geographical restrictions and Cloud security concerns

Relatively fewer respondents from non-acute care providers (**18 percent**) indicated that the lack of geographical restrictions, as it pertains to cloud providers and cloud security in particular, was a concern. Acute care providers and non-acute care providers may make different uses of cloud service providers (including the types of data that is handled and different cloud computing models, such as private clouds). (Some may opt not to "go to the cloud" at all.)

[32] *See Guidance on HIPAA & Cloud Computing, available at* https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html.
[33] *See id.*
[34] *See id.* at 32.

3. **Third Party Security**. Information security professionals at **acute care providers** have more specific concerns regarding the security posture and practices of third parties. These specific concerns included **not adopting the same policies and practices**, **lax security**, and **secure data destruction.**

Graph 18: Which of the following information security concerns do you have at your organization in regards to exchanging healthcare information with third parties? (*Please check all that apply.*)



Third party does not adopt the same policies and practices as my organization is the #1 Concern

Acute care providers: Third party security and policies and practices

A significant top concern of information security professionals at acute care providers (**73 percent**) is that third parties do not adopt the same policies and practices (Graph 18). A best practice, when dealing with third parties, is aligning an organization's policies and practices with the third party—especially if the healthcare organization has a robust information security program.

However, an acute care provider may be compromised by the third party (or through the third party, in the case of an attacker attacking the third party to infiltrate the acute care provider). This scenario can happen in the case of a business associate or a vendor with whom the acute care provider has dealings with. Or, it can happen if the acute care provider is acquiring (or merging with) a smaller organization with a less sophisticated information security program.

Non-acute care providers: Third party security and policies and practices

Interestingly, only **47 percent** of respondents at non-acute care providers indicated that they were concerned about third parties not adopting the same policies and practices as their organizations (Graph 18).

Third party has lax security is the #2 Concern

If a third party has lax security, this can introduce significant risk for any organization. An attacker may gain access to the acute care provider's IT infrastructure through the third party. This may be made easier for the attacker if the third party has elevated privileges and wide access to the acute care provider's IT infrastructure.

Acute care providers: Third party security and lax security

63 percent of respondents at acute care providers indicated that they had a concern about third parties having lax security (Graph 18).

Non-Acute care providers: Third party security and lax security

In contrast, only **47 percent** of respondents at non-acute care providers indicated that they had a concern about third parties having lax security (Graph 18).

Third party does not securely destroy the organization's data at the end of the contract is the #3 Concern

Information security professionals from acute care providers were also concerned that third parties do not securely destroy the organization's data at the end of the contract. It is typical for many contracts to contain language that the information shall be destroyed and for a certificate of destruction to be issued after such information has been destroyed. However, some third parties may not provide additional assurances (beyond the standard contract language) that the organization's data has been destroyed. (No one likes the prospect of having to report a breach of their data, due to a third party with lax security practices, such as, but not limited to, "insecure" document and media destruction. In other words, if document or electronic media is not securely destroyed, there is the possibility that the document or data from the media can be reassembled, recovered, or reconstituted, in part or in whole.)

Since there have been reported instances of covered entities **not** securely destroying data (e.g., documents containing protected health information not being shredded and electronic protected health information left on a photocopier's hard drive), many information security professionals have been specifically concerned about secure destruction of their data in the hands of third parties. HIPAA requires covered entities *and* business associates to appropriately dispose of protected health information.[35]

Acute care providers: Third party security and secure data destruction

Respondents at acute care providers (**52 percent**) were concerned about the third party not securely destroying the organization's data at the end of the contract (Graph

[35] *See What do the HIPAA Privacy and Security Rules Require of Covered Entities When They Dispose of Protected Health Information?, available at* https://www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html. *See also May a Covered Entity Dispose of Protected Health Information in Dumpsters Accessible by the Public?, available at* https://www.hhs.gov/hipaa/for-professionals/faq/576/may-a-covered-entity-dispose-of-information-in-dumpsters/index.html. *See also* 45 CFR §164.530(c) *and* 45 CFR §164.310(d)(2)(i).

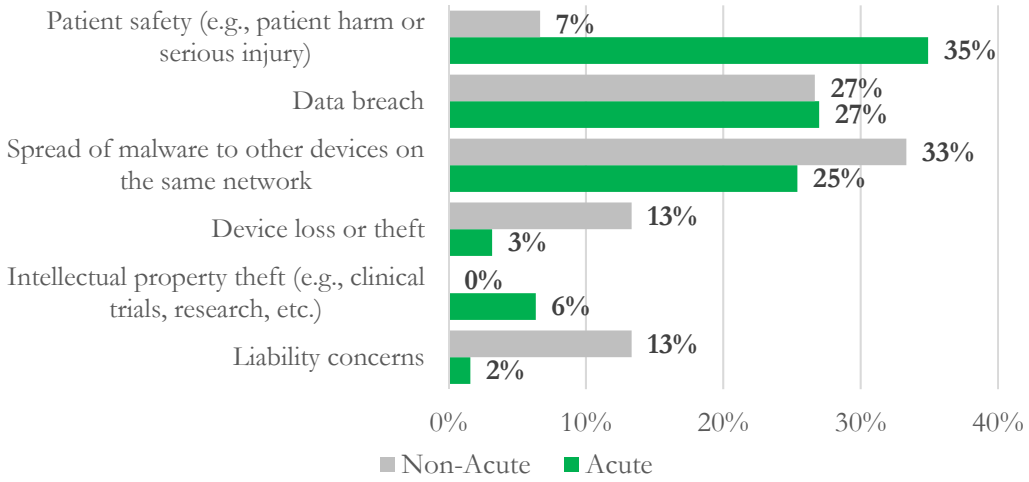
18). Thus, acute care providers may go to greater lengths to ensure that such data is securely destroyed. As an example, acute care providers may have additional assurances in the contracts in regard to data destruction. Additionally, acute care providers may want additional "proof" that data is indeed being securely destroyed (such as by having visibility into the third party's data destruction practices and policies).

Non-acute care providers: Third party security and secure data destruction

Interestingly, significantly fewer respondents (**27 percent**) had the concern about third parties not securely destroying the organization's data at the end of the contract (Graph 18).

4. **Medical Device Security**. Information security professionals at acute care providers are most concerned about **patient safety** (**35 percent**) (Graph 19).

Graph 19: What is your greatest concern about medical device security at your organization?



Medical device security has been a topic of great interest and concern in the healthcare sector. Moreover, in the healthcare sector, especially in the last few years, there has been a clear realization of the nexus between cybersecurity and patient safety. At the very least, the "proof of concept" of exploiting medical devices (which are life sustaining or lifesaving) has been demonstrated by security researchers.

Acute care providers: Medical device security

Respondents at acute care providers (**35 percent**) were most concerned about patient safety, such as patient harm or serious injury, which may result from a security compromise of a medical device (Graph 19). Medical devices, such as those that are life-sustaining or life-sustaining, are more likely to be used (and more frequently used and in larger numbers) in an acute care provider, compared to a non-acute care provider.

A secondary concern was the prospect of a data breach (**27 percent**) (Graph 19). Data breaches can be costly and disruptive to organizations. In addition, there may be concern about action from agencies such as the Office for Civil Rights at the US Department of Health and Human Services ("OCR").[36]

Non-acute care providers: Medical device security

Surprisingly, only **7 percent** of respondents are non-acute care providers were concerned about patient safety. However, the spread of malware to other devices on the same network was a much greater concern to these respondents (**33 percent**) as well as the prospect of a data breach (**27 percent**) (Graph 19).

[36] *See U.S. Department of Health and Human Services Office for Civil Rights: Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, available at* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

4. Conclusion

The findings of the **2017 HIMSS Cybersecurity Survey** reveal that information security professionals at both acute care and non-acute care providers are taking steps to significantly improve their cybersecurity posture, including regularly conducting penetration testing, performing risk assessments, and, at times, taking a more cautious approach to cybersecurity (especially in the case of acute care providers). In addition, healthcare organizations with a Chief Information Security Officer or other senior information security leader, have adopted holistic cybersecurity practices and perspectives in critical areas. While the healthcare sector may not have had decades to establish and improve its cybersecurity posture, like the chemical, manufacturing, and other sectors, significant strides have been made in the "growth" of information security programs within the healthcare sector. This growth was catalyzed, in part, by significant cyber-attacks targeting the healthcare sector and other sectors and industries. The other part is due to heightened situational awareness, know-how, and acumen in regard to cybersecurity and its best practices.

5. About HIMSS

The Healthcare Information and Management Systems Society (HIMSS) is a global, cause-based, not-for-profit organization focused on better health through information technology (IT). In North America, HIMSS focuses on health IT thought leadership, education, events, market research, and media services. Founded in 1961, HIMSS North America encompasses more than 64,000 individuals, of which more than two-thirds work in healthcare provider, governmental, and not-for-profit organizations, plus over 640 corporations and 450 not-for-profit partner organizations, that share this cause.

6. How to Cite This Survey

Individuals are encouraged to cite this report and any accompanying graphics in printed matter, publications, or any other medium, as long as the information is attributed to the **2017 HIMSS Cybersecurity Survey**.

7. For More Information

Joyce Lofstrom
Senior Director, Corporate Communications
HIMSS
33 W. Monroe, Suite 1700
Chicago, IL 60603
312-915-9237
jlofstrom@himss.org