2018 HIMSS Cybersecurity Survey

HIMSS North America

2018 HIMSS Cybersecurity Survey

Contents

1. Executive Summary

The **2018 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 impacting the healthcare and public health ("HPH") sector.

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

Based on the feedback from **239** health information security professionals,[1] an analysis of the findings yielded a few notable themes, which are explored in greater detail in this report and highlights are summarized below:

- Healthcare organizations with cybersecurity programs are making positive efforts towards improvement. More resources are dedicated to cybersecurity programs. Proactive measures are taken as a result of regular risk assessments. Penetration testing and security awareness training are regularly conducted.
- Most healthcare organizations' cybersecurity programs have room for improvement. Significant barriers exist for remediating and mitigating security incidents. Some organizations do not yet have formal insider threat management programs. Risk assessments widely vary from organization to organization.
- Looking to the future, healthcare organizations have certain concerns and priorities which will shape the direction of healthcare cybersecurity. More resources will continue to be dedicated to cybersecurity programs in the future.

2. Methodology and Demographics

Findings from the **2018 HIMSS Cybersecurity Survey** are based on the feedback from **239** qualified[2] **information security professionals** from a variety of healthcare organizations, participating in a web survey commissioned by HIMSS North America from December, 2017 through January, 2018. Survey participants

[1] Please note: While there were 239 qualified health information security professionals for the survey, not all of them answered all of the questions in the survey. Thus, the number of respondents (the "n" number) may be less than or equal to 239, depending upon the circumstances.

[2] To participate in the survey, respondents had to have some degree of oversight or day-to-day-operations of the cybersecurity program at their organization. Of the 279 individuals responding to the survey invite, 40 individuals indicated they had "no responsibility at all." These 40 individuals were therefore excluded from this survey.

included **HIMSS** members, including those members of the **HIMSS Cybersecurity Community**, and **non-HIMSS** members.

Respondents' positions in organization: generally executive or non-executive management

Respondents with some degree of responsibility for oversight or day-to-day operations of cybersecurity programs generally described their positions as either executive management (36.8%) or non-executive management (37.2%), as noted in Table 1. Yet other respondents indicated that they were non-management (25.9%). These numbers included full-time, part-time, and contract positions.

Table 1: Position in organization

Title	N	percent
Executive Management	**88**	**36.8%**
Non-Executive Management (*e.g., mid-level or senior management, but not executive level*)	**89**	**37.2%**
Non-Management (*e.g., analyst, specialist, etc.*)	62	25.9%

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

Respondents' degree of responsibility for cybersecurity program: fairly even split between primary and some responsibility/sometimes, as needed

In the aggregate, respondents generally indicated that they had either primary responsibility (41%), some responsibility (33%), or sometimes, as needed (12%), as noted in Table 2. Thus, there was a roughly even split between those with primary or some degree of responsibility for oversight or day-to-day operations of cybersecurity programs.

Table 2: Cybersecurity program responsibility

Role	N	percent
Primary responsibility	**115**	**41.2%**
Some responsibility	91	32.6%
Sometimes, as needed	33	11.8%

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

Respondents' organization types: mostly healthcare providers, consultants, and vendors

We also took note of the organization types of the respondents. Most respondents stated that they worked for a healthcare provider, consulting firm, or healthcare IT vendor. As noted in Table 3, most respondents indicated that they work at hospitals, multi-hospital systems, or integrated delivery (31.5%) or at health IT vendors (15.3%). Still others indicated that they work at consulting firms (7.7%), academic medical centers (6.8%), independent ambulatory clinics (5.4%), federal, state, or local government office (4.50%), academic education institutions (4.1%), and critical access hospitals (3.15%). Other work sites identified by respondents are noted below in Table 3.

Table 3: Type of organization

Organization Type	N	percent
Hospital, Multi-Hospital System, Integrated Delivery	**70**	**31.5%**
Healthcare IT Vendor	34	15.3%
Consulting Firm	17	7.7%
Academic Medical Center	15	6.8%
Independent Ambulatory Clinic	12	5.4%
Federal, State or Local Government Office	10	4.5%
Academic Education Institution	9	4.1%
Critical Access Hospital	7	3.2%
Public Health	7	3.2%
Mental/Behavioral Health Facility	6	2.7%
Payer, Insurance Company, Managed Care	6	2.7%
Community Health Center Clinic	5	2.3%
Banks/Financial Services	3	1.4%
HIE Organization	3	1.4%
Professional Society	2	1.0%
Long Term Care Facility	2	1.0%
Home Healthcare Organization	1	0.5%
IDS/hospital-owned ambulatory clinic	1	0.5%

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

Respondents are generally HIMSS members, but a fair number of respondents were non-HIMSS members

The majority of respondents indicated that they are members of HIMSS (76.1%), but a fair number of respondents indicated that they were not HIMSS Members (20.3%), as noted in Table 4. Typically, respondents indicated that they were HIMSS Members and a member of the HIMSS cybersecurity community (41.0%) or that they were HIMSS members but not a member of the community (35.1%). But, a fair number of respondents indicated that they were not HIMSS members at all (20.3%). A minority of respondents were unaware of their membership status with HIMSS (3.6%).

Table 4: Membership

HIMSS Membership	N	percent
Yes… and a member of the HIMSS Cybersecurity Community	**91**	**41.0%**
Yes… but I am not a member of the HIMSS Cybersecurity Community	**78**	**35.1%**
No	45	20.3%
Don't Know	8	3.6%

Q. Are you a member of HIMSS?

Please note: As respondents reflect a segment of the market with some degree 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 healthcare organizations. Readers are encouraged to exercise caution in extrapolating the findings to broader audiences outside those represented in this report.

3. Findings

What's Happening: Healthcare organizations continue to experience significant security incidents.

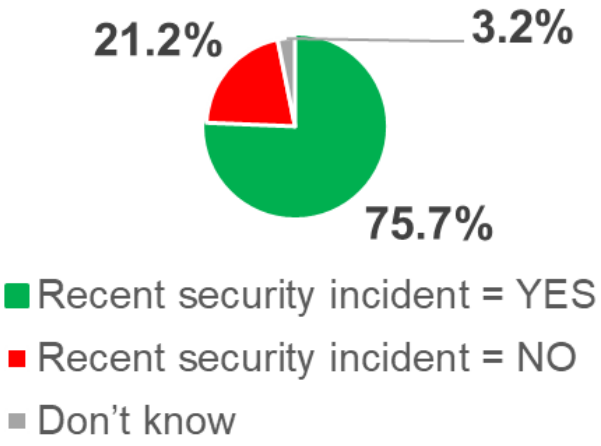
Significant security incidents at healthcare organizations have not slowed down by any means. If anything, it is projected that significant security incidents will continue to grow in number, complexity, and impact. As an example, in the past year, the WannaCry and NotPetya international cyber-attacks affected some healthcare organizations and, for some organizations, these attacks affected them and may have constituted significant security incidents.

We also asked respondents various questions related to recent significant security incidents in the past 12 months. The following explains in more detail about the recent significant security incidents, including the characterization of threat actors, timeframe for discovery, and who discovered such incidents.

Most healthcare organizations have experienced a recent significant security incident in past 12 months[3]

The majority of respondents (75.7%) indicated that their organizations experienced a significant security incident in the past 12 months as noted in Graph 1. However, 21.2% indicated that they did not have a recent significant security incident in the past 12 months and 3.2% indicated that they did not know.

Graph 1: Prevalence of recent significant security incidents in past 12 months



[3] Every organization has its own definition of what constitutes a "security incident" and a "significant security incident." Such incidents may range from sophisticated, advanced persistent threat ("APT") attacks to negligent insider activity. *See, e.g., Critical Infrastructure Partnership Advisory Council: Year in Review 2017.*

Threat actors responsible for recent significant security incidents have been generally characterized as online scam artists, negligent insiders, and hackers

We asked respondents to characterize the threat actor associated with their organizations' most recent significant security incident over the past 12 months. As noted in Table 5, about 96% of respondents who indicated that their organization had such a recent significant security incident were able to characterize the threat actor. Only 4% of respondents (whose organizations had a recent significant security incident) were not able to characterize the threat actor (i.e., don't know).

In the aggregate, the top threat actor was the online scam artist involved in activities such as phishing and spear phishing (29.6%). Still others indicated that negligent insiders were responsible for the most significant security incident (16.4%) or hackers (15.9%). Inasmuch as hackers (e.g., cybercriminals, script kiddies, or otherwise) have been in the news this past year, it is interesting that this was not more of a predominant trend.

Malicious insiders (4.2%), social engineers (3.7%), hacktivists (3.2%), and nation state actors (2%) also were identified as threat actors. However, as can be seen by the numbers, relatively few respondents attributed the recent significant security incidents to such threat actors.

Table 5: Recent Significant Security Incident: Threat Actors

Threat actors	N	percent
Online scam artist (e.g., phishing, spear phishing)	**56**	**37.6%**
Negligent insider (well-meaning but negligent individuals with trusted access who may facilitate or cause a data breach or other cyber incident)	**31**	**20.8%**
Hacker (e.g., cybercriminal, script kiddie, or other bad actor)	**30**	**20.1%**
Malicious insider (bad actors with trusted access who seek to steal information or damage IT infrastructure)	8	5.4%
Social engineer (e.g., vishing or otherwise) (not via online means)	7	4.7%
Hacktivist (hacking for a politically or socially motivated purpose; not a nation state actor)	6	4.0%
Don't know	6	4.0%
Nation state actor	3	2.0%
Other	2	1.3%

Q. Thinking about your organization's most recent significant incident, which of the following best characterizes the threat actor?

Initial point of compromise is most often e-mail (e.g., phishing e-mail) for recent significant security incidents

We asked respondents to describe the initial point of compromise. As noted in table 6, majority of respondents (61.4%) indicated that the initial point of compromise was via e-mail (e.g., phishing e-mail). Yet others indicated that the initial point of compromise was in the "other" category (13.2%). For the "other" category (12.7%), the initial point of compromise ranged from web application attacks, compromised customer networks, weak passwords, misconfigured cloud servers, and human error—for those respondents

who could identify an initial point of compromise. However, many respondents indicated that the initial point of compromise was not known (11.6%).

A minority of respondents (about 3% or less) indicated that the initial point of compromise was by way of a compromised organizational website (3.2%), hardware or software infected with malware "off the shelf" (3.2%), infected or compromised mobile device or medical device (each 2.1%), third party websites (1.6%), or a compromised cloud provider/service (1.6%).

From these results as noted in Table 6, it appears that e-mail (such as phishing e-mails) tend to be popular modes of compromise. With the plethora of tools available to generate phishing e-mails and relative ease to generate and send targeted e-mails or mass e-mails (plus, relatively little time commitment), it is not surprising that phishing is the most popular initial point of compromise for recent significant security incidents. The likelihood of exploitability via phishing e-mails is high for reasons such as these. Both technical and human components may be compromised via such activity.

Table 6: Recent Significant Security Incident: Initial Point of Compromise

Initial Point of Compromise	N	percent
E-mail (e.g., phishing e-mail)	**117**	**61.9%**
Compromised organizational website	6	3.2%
Hardware or software infected with malware "off the shelf" (e.g., pre-loaded malicious software)	6	3.2%
Infected or compromised mobile device	4	2.1%
Infected or compromised medical device	4	2.1%
Third party website (e.g., watering hole attack or otherwise)	3	1.6%
Compromised cloud provider/service	3	1.6%
Other	24	12.7%
Don't know	22	11.6%

Q. Thinking about your organization's most recent significant incident, which of the following best describes the initial point of compromise?

Discovery of the initial point of compromise is generally from internal resources for recent significant security incidents

As noted in Table 7, the majority of respondents (40.7%) indicated that they learned about the most significant security incident from their internal security team or internal personnel (other than the internal security team) (27.5%). With this in mind, it is not uncommon to hear about "third parties" notifying organizations of significant security incidents. But, at least for the respondents to the current survey, only 5.3% learned about the incident from a retained third party vendor or an unsolicited third party vendor (3.7%).

Unsolicited third party vendors may include consultants, cybersecurity firms, security researchers, or others who may have discovered vulnerabilities (e.g., exposed terminal servers, medical devices, imaging modalities, etc.) and/or the results of exploitation of such vulnerabilities (e.g., breaches, data leakage, etc.).

Table 7: Recent Significant Security Incident: Discovery of Initial Point of Compromise

Source	N	percent
Internal security team	**77**	**40.7%**
Internal personnel (other than internal security team)	**52**	**27.5%**
Don't know	21	11.1%
Other	17	9.0%
Retained third party vendor (i.e. cybersecurity firm, firm offering managed privacy and security services)	10	5.3%
Unsolicited third party vendor (i.e. cybersecurity firm, firm offering managed privacy and security services)	7	3.7%
Patient whose information was compromised (e.g., identity theft – medical, financial, or otherwise)	5	2.7%

Q. Thinking about your organization's most recent significant incident, which of the following best describes how your organization initially learned about the incident?

Time to discover recent significant security incidents is generally 7 days or less

We asked respondents to indicate how long it took for their organizations to discover the attack in regard to their organizations' most recent significant security incident in the past 12 months. The majority of respondents (47.1%) indicated that it took less than 24 hours, 13.2% of respondents indicated 1 to 2 days, and 7.4% of respondents indicated 3 to 7 days, as noted in Table 8.[4] Accordingly, the time to discover the recent significant security incident for our respondents was generally 7 days or less.

Table 8: Recent Significant Security Incident: Time to Discover

Time to discover	N	percent
Less than 24 hours	**89**	**47.1%**
1 to 2 days	**25**	**13.2%**
3 to 7 days	**14**	**7.4%**
More than 1 week but less than 1 month	7	3.7%
1 to 3 months	10	5.3%
4 to 6 months	1	0.5%
7 to 9 months	1	0.5%
10 to 12 months	1	0.5%
Don't know	14	7.4%

Q. Thinking about your organization's most recent significant incident in the past year, how long did it take for your organization to discover the attack?

[4] This appears to be consistent with the results of the 2015 HIMSS Cybersecurity Survey with 56.7% of respondents (n=115) indicating within 24 hours, 23.6% of respondents (n=48) within 1 week, and 6.4% of respondents (n=13) within 1 month.

Observation 1: Healthcare organizations are making progress in improving their cybersecurity programs

The use of resources has increased to address cybersecurity concerns since last year

More resources (e.g., people, assets, other resources) are being used to address cybersecurity concerns since last year for the vast majority of respondents to the survey. On a related note, in the 2015 and 2016 HIMSS Cybersecurity Surveys, the vast majority of respondents to the survey indicated that cybersecurity was a business priority for their respective organizations. In our 2017 HIMSS Cybersecurity Survey, we noted that 60% of respondents indicated that their organization employs a senior information security leader.

Specifically, in this survey, we asked respondents how their organization's use of resources to address cybersecurity concerns has changed, compared to this time last year—i.e., whether or not there was a change.

As noted in Table 9, the vast majority of respondents (84.3%) indicated that their organizations' use of resources to address cybersecurity concerns has increased. Yet others indicated that there has not been a change in resources since last year (11.0%). Still others indicated that their organizations' use of resources has decreased (3.3%). Only 1.4 percent of respondents indicated that they did not know whether their organizations' use of resources had changed.

Table 9: Use of Resources to Address Cybersecurity Concerns[5]

Change in Use of Resources	N	percent
Yes – it increased	**177**	**84.3%**
Yes – it decreased	7	3.3%
No	23	11.0%
Don't Know	3	1.4%

Q. Compared to this time last year, has your organization's use of resources to address cybersecurity concerns (e.g. people, assets, other resources) changed?[6]

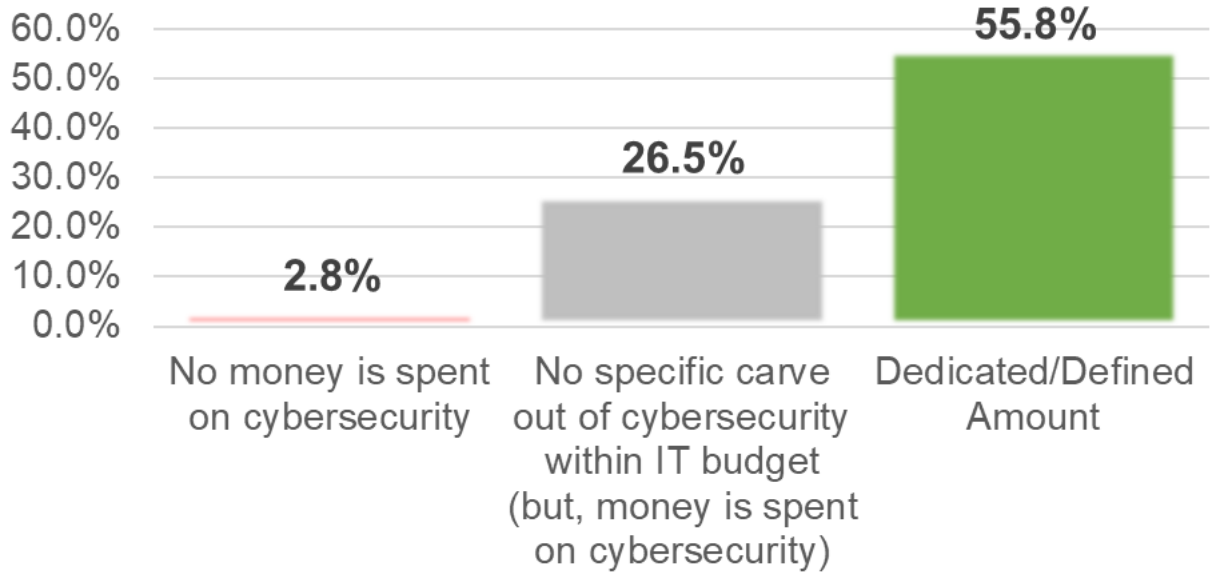
Most organizations have a dedicated or defined allocation for cybersecurity within the current IT budget

As noted in Graph 2, the majority of respondents (55.8%) have a dedicated or defined amount of the current IT budget allocated for cybersecurity. (The specific amounts allocated are discussed later in this report in the Observation 3: Room for Improvement section.) However, a fair amount of respondents (26.5%) have no specific carve out of cybersecurity within the IT budget (but, money is spent on cybersecurity). (Whether this is a benefit or a detriment to the cybersecurity program is yet another question. On the one hand, this can be a very flexible proposition in that dollars available for cybersecurity may be generously available as requested. On the other hand, this may be quite restrictive in light of the lack of specific carve out.) Still other respondents indicated that no money is spent on cybersecurity (2.8%).

[5] Please see Table 28 for what respondents thought in terms of the use of resources to address cybersecurity concerns for the next year.

[6] An organization that is expending more resources to address cybersecurity concerns may not necessarily be expending more money to do so. "Assets" is one possible reason listed in the survey question as to why an organization's use of resources may have changed. Other possible reasons include the increased use of people (personnel) and other types of resources (other than assets).

Graph 2: Percentage of organization's current IT budget allocated to cybersecurity.



Q. What percentage of your organization's current IT budget is allocated to cybersecurity?

Most organizations are conducting security risk assessments at least once a year

We asked respondents how frequently security risk assessments are conducted at their organizations. The majority of respondents (45.5%) indicated that their organizations conduct security risk assessments once every year, as noted in Table 10. (Compared to the results of our 2017 HIMSS Cybersecurity Survey, we did not see significant improvement from last year to this year.) Other respondents indicated other time frames such as daily (9.6%), once a month (9.0%), once a quarter (10.7%), and once every six months (5.6%).

Table 10: Frequency of security risk assessments

Frequency	N	percent
Daily	17	9.6%
Once a month	16	9.0%
Once every six months	10	5.6%
Once every year	**81**	**45.5%**
Once every 2 years	6	3.4%
Once every 3 years	2	1.1%
My organization does not conduct security risk assessments	9	5.1%
Don't know	18	10.1%

Q. How frequently are security risk assessments conducted at your organization?

Security risk assessments have some uniformity across healthcare organizations

We asked respondents what their security risk assessments include when their organizations conduct security risk assessments. The top five responses were as follows: (1) cybersecurity policies and procedures (and documentation) (81.3%), (2) network (74.7%), (3) security awareness and training program(s) (73.5%), (4)

physical security (71.1%), and (5) inventory of assets (69.3%), as noted in Table 11. Thus, there is some degree of uniformity in terms of components included in security risk assessments.[7]

Table 11: Components of security risk assessments

Components	N	percent
Cybersecurity policies and procedures (and documentation)	**135**	**81.3%**
Network	**124**	**74.7%**
Security awareness and training program(s)	**122**	**73.5%**
Physical security	**118**	**71.1%**
Inventory of assets	**115**	**69.3%**
Cybersecurity roles and responsibilities	108	65.1%
Clinical information systems (including electronic health record systems)	102	61.4%
Business and financial systems	97	58.4%
Communications plan	90	54.2%
Third party risks	86	51.8%
Organizational website	68	41.0%
Medical devices	57	34.3%
Comprehensive (i.e., end-to-end)	43	25.9%
Don't know	9	5.4%
Other	7	4.2%

Q. When conducting a security risk assessment, what does your security risk assessment include? Please select all that apply.

Risk assessment results guide risk management activities

Risk assessments are done for a purpose—namely, managing risk (not just merely identifying and assessing risks, with nothing more). New or improved security measures may be adopted, security solutions may be upgraded or replaced, and hardware, software, and devices may be replaced. The results of risk assessments may even indicate a need to test things further (e.g., penetration testing).

We asked respondents about the actions taken by organizations as a result of conducting a security risk assessment. The vast majority of respondents (83.1%) stated that their organizations adopted new or improved security measures, as noted in Table 12. Yet others replaced or upgraded security solutions (65.1%). Still others replaced hardware, software, devices, etc. that are end-of-life or that have been deprecated (56.6%). Still others conducted a penetration test (39.8%).

Only 2.4% of respondents concluded that no additional actions were deemed necessary in light of the security risk assessment having been conducted at their organization. Thus, the vast majority of organizations are doing something proactive in response to conducting security risk assessments (e.g., managing risk) and not merely letting the results of such assessments merely sit on the shelf.

[7] While comprehensive (i.e., end-to-end) security risk assessments are the ideal, there are many components of security risk assessments that are typically included (as noted in Table 10). Thus, healthcare organizations are moving in the right direction in regard to security risk assessments.

Table 12: Post-risk assessment actions

Actions	N	percent
Adopted new or improved security measures (e.g., processes)	**138**	**83.1%**
Replaced or upgraded security solutions	**108**	**65.1%**
Replaced hardware, software, devices, etc. that are end-of-life or that have been deprecated (other than those related directly to IT security – e.g., firewalls, IDS, etc.)	94	56.6%
Conducted a penetration test	66	39.8%
Other	12	7.2%
Don't know	6	3.6%
No additional actions deemed necessary	4	2.4%

Q. Which of the following actions has your organization taken after conducting a security risk assessment? Please check all that apply.

Supply chain integrity and security are important to healthcare organizations

Supply chain security and integrity are an important part of the procurement process. The majority of respondents include a cybersecurity assessment as part of their due diligence analysis when acquiring a product or service at their respective organizations. Cybersecurity matters and the acquisition of products and services is not arbitrary, nor is it necessarily based on the "lowest bidder."

Virtually any piece of technology may have vulnerabilities that may be exploitable now or at some point in the future. Thus, the acquisition of any product or service could potentially have consequences and impacts for the organization. Simply buying a product or service without conducting such an assessment may introduce unnecessary or potentially unreasonable risks to the organization.

Accordingly, we asked respondents whether cybersecurity assessments were conducted as part of their due diligence analysis when acquiring a product or service for their organizations. The vast majority of respondents (70.0%) stated "yes." But, 26.5% of respondents indicated "no." (While this is a positive trend, we believe that more healthcare organizations should be doing such cybersecurity assessments.) Only 3.5% of respondents did not know whether a cybersecurity assessment of a potential product or service was conducted prior to acquiring the same.

Table 13: Cybersecurity due diligence prior to acquisition of product/service

Cybersecurity assessment	N	percent
Yes	**119**	**70.0%**
No	45	26.5%
Don't know	6	3.5%

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

Observation 2: Healthcare Cybersecurity Programs Could Be Improved in Multiple Areas

While healthcare organizations have notably made some progress with their cybersecurity programs, there is still room for improvement. Many healthcare organizations have been focused on compliance and security has not necessarily been top of mind—until recently.

Other critical infrastructure sectors, such as electrical, chemical, and manufacturing, have had decades to mature their cybersecurity programs. However, many healthcare organizations have only been focusing on improving their cybersecurity programs in the last five years or so (especially since cyber-attacks started to become the norm).

Indeed, many cybersecurity professionals are still getting used to the idea that there are bad actors out there that are directly or indirectly targeting healthcare organizations (including externally and from within). Furthermore, many healthcare organizations are used to the "old way" of doing business. More organizations are focusing on cybersecurity as a priority. But, as the following results will show, there is still the need to significantly advance the state of healthcare cybersecurity in multiple areas, such as the ones described below.

Biggest barriers for remediation and mitigation of cybersecurity incidents: Personnel and financial resources

The biggest barriers for remediating and mitigating cybersecurity incidents are a lack of appropriate cybersecurity personnel and a lack of financial resources. This finding was also echoed in the 2015 HIMSS Cybersecurity Survey.

We asked respondents to identify the biggest barriers to remediating and mitigating security incidents. The top five barriers identified were lack of appropriate cybersecurity personnel (52.4%), lack of financial resources (46.6%), too many application vulnerabilities (28.6%), too many endpoints (27.5%), and too many emerging and new threats (27.0%), as noted below in Table 14.[8]

[8] These results are fairly similar to those of the 2015 HIMSS Cybersecurity Survey with 64% of respondents (n=190) indicating lack of appropriate cybersecurity personnel, 60.3% of respondents (n=179) indicating lack of financial resources, 41.8% of respondents (n=124) indicating too many emerging and new threats, and 32.0% of respondents indicating too many endpoints (n=95).

Table 14: Biggest barriers for remediating & mitigating cybersecurity incidents

Actions	N	percent
Lack of appropriate cybersecurity personnel	**99**	**52.4%**
Lack of financial resources	**88**	**46.6%**
Too many application vulnerabilities	54	28.6%
Too many endpoints (e.g., user devices, computers, etc., connected to the network)	52	27.5%
Too many new and emerging threats	51	27.0%
Not enough cyber threat intelligence to stay ahead of threats	44	23.3%
Network infrastructure too complex to secure	39	20.6%
Sufficient cyber threat intelligence, but lack of technologies/tools for effective use and deployment	32	16.9%
Sufficient cyber threat intelligence, but lack of know-how for effective use and deployment	27	14.3%
Too many users for timely and effective provisioning and de-provisioning of accounts	26	13.8%
Other	20	10.6%
Don't know	3	1.6%
None of the above	9	4.8%

Q. What are the biggest barriers your organization faces to remediating and mitigating cybersecurity incidents? Please select all that apply.

Cybersecurity staffing ratios vary widely across the board

We asked respondents about the approximate ratio of cybersecurity staff to IT users at their organizations. The top three responses were 1:100 (22.1%), more than 1:1000 (17.7%), 1:1000 (14.4%), and 1:10 (n16.0%), as noted in Table 15. Interestingly, 13.3% of respondents indicated that they had no cybersecurity staff at all. Staffing ratios tended to widely vary across various healthcare organization types (e.g., hospitals, vendors, government, etc.).

Table 15: Cybersecurity staffing ratios

Ratios	N	percent
No cybersecurity staff	24	13.3%
1:10	**29**	**16.0%**
1:100	**40**	**22.1%**
1:500	20	11.1%
1:1000	**26**	**14.4%**
More than 1:1000	**32**	**17.7%**
Don't Know	10	5.5%

Q. What is the approximate ratio of cybersecurity staff to IT users in your organization? Please choose the best answer.

Most organizations spend 6 percent or less of the current IT budget on cybersecurity

We asked respondents about what percentage of the organization's current IT budget is allocated to cybersecurity. Of those respondents who indicated that their organizations have a specific allocation for cybersecurity within the current IT budget, the top three responses were 1-2 percent (21.0%), 3-6 percent (21.0%), and 7-10 percent (7.2%), as noted in Table 16. However, 26.7 percent of respondents indicated that

there is no specific carve out within the IT budget, but money is spent on cybersecurity. 2.8 percent of respondents indicated that no money is spent on cybersecurity at all.

Based upon these numbers and the previous finding in this survey that there is a lack of financial resources to appropriately remediate and mitigate cybersecurity incidents, it is clear that healthcare organizations across the board need to allocate more of their respective IT budgets to cybersecurity.

Table 16: Cybersecurity budget

Percentage of Current IT Budget	N	percent
1-2 percent	**38**	**21.0%**
3-6 percent	**38**	**21.0%**
7-10 percent	13	7.2%
11-13 percent	7	3.9%
14-17 percent	3	1.7%
More than 17 percent	2	1.1%
No specific carve out of cybersecurity within IT budget (but, money is spent on cybersecurity)	48	26.7%
No money is spent on cybersecurity	5	2.8%
Don't know	27	14.9%

Q. What percentage of your organization's current IT budget is allocated to cybersecurity?

No Universally Adopted Security Framework

Before healthcare cybersecurity can improve, all healthcare organizations need to get on the same page. One of the ways to achieve this is through the adoption of a universal security framework. Unfortunately, we are not there yet.

As noted in Table 17, the majority of respondents (57.9%) indicated that they used NIST (57.9% of respondents). This was followed by HITRUST (26.4%), Critical Security Controls 24.7%), and ISO (18.5%). (Please note: Respondents were able to select one or more security frameworks as response options.) Furthermore, 16.9 percent of respondents indicated that no security framework has been implemented at their respective organizations at all.

Table 17: Security Frameworks

Framework	N	percent
NIST	**103**	**57.9%**
HITRUST	47	26.4%
Critical Security Controls	44	24.7%
ISO	7	18.5%
COBIT	13	7.3%
Other	9	5.1%
No security framework has been implemented at my organization	30	16.9%
Don't know	15	8.4%

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

No Uniform Sources of Cyber Threat Intelligence

In order to stay ahead of cyber threats, healthcare organizations must have reliable and trustworthy cyber threat intelligence. Ideally, healthcare organizations are able to push and pull cyber threat intelligence from their sources. And, ideally too, such sources will be used by virtually everyone in the healthcare and public health sector. Unfortunately, this is not the case today.

We asked respondents about which cyber threat intelligence sources their organizations use to stay informed about cyber threats. Based upon these responses, there was no clear cut winner in terms of a single, dominant source. However, the top three sources included peers (word of mouth) (68.6%), US CERT alerts and bulletins (60.0%), and HIMSS resources (e.g., monthly healthcare and cross-sector cybersecurity reports, etc.) (53.8%), as noted in Table 18. Respondents could choose one or more cyber threat intelligence sources, as appropriate.

Table 18: Cyber Threat Intelligence Sources

Sources	N	percent
Peers (word of mouth)	**144**	**68.6%**
US CERT alerts and bulletins	**126**	**60.0%**
HIMSS resources (e.g., monthly healthcare and cross-sector cybersecurity reports, etc.)	**113**	**53.8%**
Third party vendor (non-healthcare specific)	100	47.6%
NIST National Vulnerability Database	92	43.8%
SANS resources	90	42.9%
Third party vendor (healthcare specific)	89	42.4%
InfraGard	61	29.0%
FBI-DHS Joint Indicator Bulletins (JIBs)	60	28.6%
US DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)	60	28.6%
HITRUST	58	27.6%
US DHS National Cybersecurity and Communications Integration Center (NCCIC)	55	26.2%
US HHS Health Cybersecurity and Communications Integration Center (HCCIC)	54	25.7%
National Health Information Sharing and Analysis Center (NH-ISAC)	53	25.2%
Other cross-sector information sources (outside of healthcare)	15	7.1%
Other	6	2.9%
None of the above	2	1.0%
Don't know	7	3.3%

Q. To stay informed about cyber threats, which of the following cyber threat intelligence sources does your organization use? Please check all that apply.

Formalized Insider Threat Management Programs Need to Be Established

The insider threat exists within every organization. As a result, many organizations have started to turn their attention towards developing insider threat management programs. But, more organizations need to develop and mature their insider threat management programs to the level where such formal programs are in place and clearly and consistently applied.

As stated in the survey, an "insider threat management program" is designed to reduce an organization's exposure to insider threat activity. The program may include policies, controls, and the involvement of management within an organization to address and mitigation the threat. An informal program, however, addresses insider threat activity on an *ad hoc* basis.

Most respondents (44.9%) indicated that their organizations do have insider threat management programs and that policies are in place. Yet other respondents (27.0%) indicated that their insider threat management programs are informal. But, a fair number of respondents (24.2%) indicated that their organizations had no insider threat management program at all. Both negligent and malicious insider threat activity[9] can be extremely damaging to any organization. Undesirable consequences, such as data leakage, breaches, sabotage, and fraud, may occur and could go unnoticed for a significant period of time until the damage is significant to the organization.

Table 19: Insider Threat

Insider Threat Management Program	N	percent
Yes, and there are policies in place	**80**	**44.9%**
Yes, but it is informal	**48**	**27.0%**
No	**43**	**24.2%**
Don't know	7	3.9%

Q. Does your organization have an insider threat management program?

More Penetration Testing, Not Less

A fair number of respondents indicated that they conduct penetration testing on a regular basis. A penetration test may uncover vulnerabilities, the exploitability of such vulnerabilities, and potential impact to the organization, through simulated attacks and mock exercises (e.g., phishing, incident response, etc.). Thus, penetration tests may illuminate certain issues which risk assessments may not.

However, penetration testing should ideally be done at frequent and regular intervals, as well as when major changes occur relevant to people, processes and technology, which may have an impact on the organization's cybersecurity program.

The majority of respondents (37.1%) are only conducting penetration testing once a year, as shown in Table 20. A minority of respondents (8.2%) conduct penetration testing more frequently than once a year. Still others conduct penetration testing either less frequently or sporadically (8.8%).

[9] *See* http://www.himss.org/sites/himssorg/files/The%20Enemy%20Within%20Dealing%20with%20Insider%20Threats%20_0-carmine-nigro-9-8-14.pdf.

Table 20: Penetration Testing: Frequency

Frequency	N	percent
Daily	6	3.4%
Weekly	4	2.4%
Quarterly	1	0.6%
Monthly	20	11.8%
Biannually	3	1.8%
Yearly	**63**	**37.1%**
Other	15	8.8%
Don't know	23	13.5%
My organization does not conduct penetration testing	35	20.6%

Q. How frequently does your organization conduct a penetration test of your IT system?

More Comprehensive Penetration Testing

Penetration testing can vary from organization to organization. Ideally, however, penetration testing should include the testing of people, processes, and technology (e.g., network, applications, websites, physical security, social engineering, incident response, etc.).

We asked respondents what parts of their IT system is subject to a penetration test (for those who conduct penetration tests at their organization). The top four responses were as follows: (1) network infrastructure (5.3%), (2) servers (15.0%), (3) websites (13.9%), (4) databases (11.7%), and (5) workstations (11.1%), as noted in Table 21. At the bottom of the list was physical security (6.8%), mobile devices (4.3%), and medical devices (3.8%).

An interesting finding, too, is that while the majority of respondents indicated that their security risk assessments include physical security (71.1%) (Table 11), relatively few respondents indicated that physical security is included in the penetration test.

Table 21: Penetration Testing: IT

IT Components	N	percent
Network infrastructure	**93**	**15.3%**
Servers	**91**	**15.0%**
Websites	**84**	**13.9%**
Databases	**71**	**11.7%**
Workstations	67	11.1%
Applications	62	10.2%
Physical Security	41	6.8%
Mobile devices	26	4.3%
Medical devices	23	3.8%
Other	3	0.5%
Don't know	45	7.4%

Q. What parts of your IT system does your organization subject to a penetration test? Please check all that apply.

Test the Human More

We asked respondents which human elements are penetration tested. The top three components were as follows: phishing awareness of workforce members (32.9%), incident response (20.6%), and communications

(17.6%), as noted in Table 22. Unfortunately, there is no general consensus around which human components are tested.

Further, it is important to regularly penetration test your incident response team and/or incident response functions (if you do not have a team, *per se*). The penetration test can help determine weaknesses in a simulated scenario (as opposed to an actual scenario, such as a cyber-attack). Communications is also very important to penetration test, as information sharing both internally and externally are critically important during a suspected or actual incident. Delays in communication may result in harm and other undesirable consequences for healthcare organizations. Vishing (i.e., voice phishing) is also very important to test. A successful vishing attack may result in leakage of sensitive information, fraud, and other consequences. In summary, humans often are the weakest link for any cybersecurity program and it is important to educate, inform, and test.

Table 22: Penetration Testing: Human

Components	N	percent
Phishing awareness of workforce members	**99**	**32.9%**
Incident response	**62**	**20.6%**
Communications	**53**	**17.6%**
Vishing awareness of workforce members	**37**	**12.3%**
Other	5	1.7%
Don't know	45	15.0%

Q. Which elements of human security does your organization penetration test? Please check all that apply.

Human Safeguards: Security Awareness

An effective security awareness program help improve the security posture of an organization. Many healthcare organizations struggle with problems stemming from a lack of security awareness. For instance, end users (and poor security decisions and actions) may have the largest impact and consequences for a healthcare organization's cybersecurity program. Thus, security awareness training of workforce members and others (e.g., contractors, consultants, temporary personnel, etc.) plays a critical role.[10]

We asked respondents how frequently security awareness training was conducted at their organization. By far, the majority of respondents indicated that their organizations conduct security awareness training at least yearly, if not more frequently, as noted in Table 23. Most respondents stated that their organizations conduct security awareness training yearly (51.8%). However, a fair number of respondents indicated that they conduct such training monthly (22.9%).

While it is good news that many healthcare organizations are conducting security awareness training on a regular basis, conducting security awareness training only once a year may not be enough. Individuals attending the training may not necessarily retain the knowledge during the rest of the year. Thus, more frequent security awareness training may be desirable.

[10] Workforce members and others are essentially gatekeepers of good and evil into and out of an organization. As an example, a workforce member may choose wisely and decide not to open a suspicious attachment (which may contain embedded malicious code). Another example is that a hospital's call center representative may receive a call from someone masquerading as a patient (or family member of a patient) in order to elicit potentially sensitive information.

Table 23: Security Awareness Training

Frequency	N	percent
Daily	**7**	**4.2%**
Weekly	**5**	**3.0%**
Bimonthly	**1**	**0.6%**
Monthly	**38**	**22.9%**
Quarterly	**5**	**3.0%**
Yearly	**86**	**51.8%**
Biannually	1	0.6%
Other	2	1.2%
My organization does not have a security awareness training program	14	8.4%
Don't know	7	4.2%

Q. How frequently is security awareness training conducted at your organization?

Observation 3: What's Next for Healthcare Cybersecurity: Concerns and Priorities

Concerns and priorities will help shape the future of healthcare cybersecurity. Without a doubt, healthcare cybersecurity will become more of a priority (if it is not a priority already). It is not likely that the cybersecurity problem will "go away." If anything, being proactive about cybersecurity will be the wave of the future.

Breaches, ransomware, and credential stealing malware are top perceived threats

Many potential threats exist. However, some are perceived as a greater threat than others. We asked respondents to rate various potential threats vis-à-vis their perception of these threats to their respective organizations. Respondents could select one of the following options: No threat at all, slight threat, somewhat of a threat, moderate threat, and extreme threat.

Breach or data leakage (11.8%), ransomware (11.3%), and credential stealing malware (11.0%) all were top perceived threats according to respondents, as noted in Table 24. (All respondents had to rate all of the listed potential threats.) However, there was relatively close clustering of responses in regard to the listed potential threats. Accordingly, healthcare organizations appear to be at least cognizant and concerned about a variety of potential threats which may impact their organizations.

Table 24: Perceived Threats

Potential Threat to Organization	N	percent
Breach or data leakage	**181**	**11.8%**
Ransomware	**181**	**11.3%**
Credential stealing malware	**181**	**11.0%**
Malicious insiders (employees or otherwise workforce members with trusted access)	181	10.1%
Wiper malware	181	10.0%
Denial of service attacks	181	9.6%
Website backdoors	181	9.5%
Theft of hardware, devices, etc. (physical theft)	181	9.4%
Supply chain integrity of software, hardware, devices, etc.	181	9.0%
Fire, flash flood, or natural hazard	181	8.3%

Q. Please rate the following in terms of the potential threat you believe they pose to your organization.

Patient Safety is the Top Medical Device Security Concern

Medical devices can be life-sustaining or life-saving. Thus, patient safety is a top concern. Furthermore, many of these medical devices are now "connected." Accordingly, there is the possibility of a compromise, such as a cyber-attack, which may affect the operations, configuration, and/or safety of the medical device itself.

We asked respondents about their greatest concern regarding medical device security at their respective organizations. As noted in Table 25, the top concerns were patient safety (35.3%), data breaches (23.5%), and spread of malware to other devices on the same network (12.4%).

Table 25: Medical Device Security

Concern	N	percent
Patient safety (e.g., patient harm or serious injury)	**60**	**39.0%**
Data breach	**40**	**26.0%**
Spread of malware to other devices on the same network	**21**	**13.6%**
Liability concerns	9	5.8%
Device loss or theft	7	4.5%
Intellectual property theft (e.g., clinical trials, research, etc.)	3	1.9%
Other	4	2.6%
Don't know	10	6.5%

Q. What is your greatest concern about medical device security at your organization? Please choose the best answer.

Concerns about Disruption or Failure of Other Critical Infrastructure Sectors

The healthcare and public health sector either depends upon or has a relationship with many other critical infrastructure sectors. Some sectors are closely aligned with the healthcare and public health sector, such as emergency services and water and wastewater. Given the international cyber-attacks of 2017 (including NotPetya and WannaCry) and other actual or attempted attacks and compromises on critical infrastructure sectors, we wanted to see whether and to what extent respondents were concerned about their reliance on the security of other critical infrastructure sectors.

We asked respondents to indicate to what extent they were concerned about the consequences or impacts on their respective organizations from a failure or disruption of other sectors (i.e., those outside of the healthcare and public health sector). By far, the greatest concerns appeared to be around information technology: business and clinical information systems, including developers, manufacturers, and distributors of IT-related hardware, software, and services (including Internet of Things) (12.9%) and information technology and communications ("ICT"): Internet and other computer networks (12.5%), as noted in Table 26. These top concerns make sense in view of all of the data and the commensurate amounts of electronic data which flows in and out of healthcare organizations daily. These top concerns also highlight the importance of other critical infrastructure sectors—i.e., those outside of the healthcare and public health sector.

Table 26: Critical Infrastructure

Concern about Disruption or Failure	N	percent
Information technology and communications ("ICT"): Internet and other computer networks	**166**	**12.9%**
Information technology: Business and clinical information systems, including developers, manufacturers, and distributors of IT-related hardware, software, systems, and services (including Internet of Things)	**166**	**12.5%**
Communications: Radio and telephone communications supporting a wide variety of business processes	166	9.5%
Emergency services: Coordination with first-responders and emergency medical services; includes local law enforcement for security for various emergencies	166	9.3%
Energy: Electric, natural gas, propane, and diesel fuel to power and run facility functions and vehicles	166	8.6%
Banking and finance: Depository institutions, providers of investment products, insurance companies, other credit and financing organizations	166	8.5%
Emergency services: Coordination with first-responders and emergency medical services; includes local law enforcement for security for various emergencies	166	9.3%
Transportation: Movement of supplies, raw materials, pharmaceuticals, personnel, emergency response units, patients, and fatalities	166	6.7%
Food and agriculture: Food production and distribution for healthcare and public health personnel and patients Postal and shipping: Movement of equipment and supplies	166	6.6%
Postal and shipping: Movement of equipment and supplies	166	6.5%
Chemical: Support to the pharmaceutical industry Manufacturing: Manufacturers of electrical equipment, components, and appliances, machinery, transportation equipment, metals, etc.	166	6.1%
Manufacturing: Manufacturers of electrical equipment, components, and appliances, machinery, transportation equipment, metals, etc.	166	5.5%

Q. To what extent are you concerned about the consequences or impacts on your organization from a failure or disruption of the following?

Multiple priorities in the future

Having insight into a healthcare organization's priorities may be indicative of where organizations will focus their resources (e.g., people, processes, and technology) and cybersecurity expenditures.

We asked respondents to rate to what extent certain issues are priority for their respective organizations' security program in the coming year. Interestingly, all of the issues we listed were regarded as a future priority for their respective organizations' security programs. Indeed, the numbers of responses were fairly evenly distributed across the listing of issues. Incident response (11.9%), risk assessment and management (11.9%), business continuity and disaster recovery (11.8%), and the awareness training programs (11.6%) were top

future priorities, as noted in Table 27. These top priorities align well with the top perceived threats (Table 24) (i.e., breach or data leakage, ransomware, and credential stealing malware).

Additional future priorities included cloud security (11.2%), website security (10.8%), physical security (10.7%), information sharing (10.4%), and medical device security (9.8%).

Table 27: Future Priorities

Issue	N	percent
Incident response	**181**	**11.9%**
Risk assessment and management	**181**	**11.9%**
Business continuity and disaster recovery	**181**	**11.8%**
Awareness training program	**181**	**11.6%**
Cloud security	**181**	**11.2%**
Website security	**181**	**10.8%**
Physical security	**181**	**10.7%**
Information sharing	**181**	**10.4%**
Medical device security	**181**	**9.8%**

Q. To what extent are the following issues a priority for your organization's security program in the coming year?

Use of Resources Expected to Increase for Next Year

As noted in Table 28, the majority of respondents (79.5%) indicated that they expect their respective organizations' use of resources to address cybersecurity concerns (e.g., people, assets, other resources) to increase in the next year. However, a minority of respondents (14.3%) stated that the organizations' use of resources is expected to decrease in the next year (2.9%). A significant number of respondents anticipated no change in the next year (14.3%).

Table 28: Use of Resources Next Year[11]

Use of Resources	N	percent
Yes – I expect it to increase	**167**	**79.5%**
Yes – I expect it to decrease	6	2.9%
No	**30**	**14.3%**
Don't know	7	3.3%

Q. Compared to this time next year, do you expect your organization's use of resources to address cybersecurity concerns (e.g. people, assets, other resources) to change?

[11] Please see Table 9 to see what respondents stated in terms of the use of resources to address cybersecurity concerns compared with the last year.

4. Conclusion

The findings of the **2018 HIMSS Cybersecurity Survey** reveal that healthcare cybersecurity is advancing with some noted improvements. However, there is always room for growth. But, cybersecurity programs cannot advance alone. Indeed, barriers such as lack of cybersecurity personnel and financial resources still persist. Accordingly, healthcare organizations (and their leaders) need to take proactive steps by instilling positive change and making cybersecurity a genuine priority. It is only then that we can move forward instead of taking one step forward and two steps back.

5. About HIMSS

HIMSS is a global voice, advisor and thought leader of health transformation through health information and technology with a unique breadth and depth of expertise and capabilities to improve the quality, safety, and efficiency of health, healthcare and care outcomes. HIMSS designs and leverages key data assets, predictive models and tools to advise global leaders, stakeholders and influencers of best practices in health information and technology, so they have the right information at the point of decision.

HIMSS drives innovative, forward thinking around best uses of information and technology in support of better connected care, improved population health and low cost of care. HIMSS is a not-for-profit, headquartered in Chicago, Illinois, with additional offices in North America, Europe, United Kingdom and Asia.

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 **2018 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