2019 HIMSS Cybersecurity Survey

Contents

1. Executive Summary

The **2019 HIMSS Cybersecurity Survey** provides insight into the information security experiences and practices of US healthcare organizations in light of increasing cyber-attacks and compromises. Reflecting the feedback from **166** US based health information security professionals, the findings of this study distill as follows:

- A pattern of cybersecurity threats and experiences is discernable across US healthcare organizations
    - Significant security incidents are a near universal experience in US healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their targets.
- Many positive advances are occurring in healthcare cybersecurity practices
    - Healthcare organizations appear to be allocating more of their information technology ("IT") budgets to cybersecurity.
- Complacency with cybersecurity practices can put cybersecurity programs at risk
    - There are certain responses that are not necessarily "bad" cybersecurity practices, but may be an "early warning signal" about potential complacency seeping into the organization's information security practices.
- Notable cybersecurity gaps exist in key areas of the healthcare ecosystem
    - The lack of phishing tests in certain organizations and the pervasiveness of legacy systems raise grave concerns regarding the vulnerability of the healthcare ecosystem.

2. Methodology and Demographics

This study offers a robust insight into the cybersecurity experiences and practices of security leaders in US healthcare organizations.

Findings from the **2019 HIMSS Cybersecurity Survey** reflect the responses of **166** qualified[1] **information security leaders** from an array of healthcare organizations, participating in a web survey commissioned by HIMSS, November through December 2018. As respondents with no information security responsibilities were excluded from the study, the findings in this report skew towards those with some degree of concern about cybersecurity issues in their respective organizations. Readers are encouraged to exercise caution in extrapolating the findings to broader audiences outside those represented in this report.

Organization Profile:

When presented with an array of work environments, **the majority of respondents (N=107; 65%) reported working at healthcare provider organizations**, with a full two-thirds of this group (N=71) working in a hospital environment (Table 1).

Table 1: Organization Type

Organization Type	N	%
Provider Organization	**107**	**65%**
Hospital	*71*	*43%*
Non-acute	*36*	*22%*
Vendor	**34**	**20%**
Other	**25**	**15%**
All Respondents	**166**	**100%**

Leadership Profile:

After noting their current employer's type of organization, respondents then indicated their managerial responsibilities within their current work setting. As detailed in Table 2, **the vast majority of all respondents (83%) reported have some level of managerial responsibilities**.

Table 2: Roles

Roles	Hospital	Non-Acute	Vendor	Other	TOTAL
Management	**75%**	**92%**	**91%**	**80%**	**83%**
Executive Management	*31%*	*53%*	*68%*	*36%*	*44%*
Non-Executive Management	*44%*	*39%*	*24%*	*44%*	*39%*
Non-Management	**25%**	**8%**	**9%**	**20%**	**17%**

[1] 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 202 individuals responding to the survey invite, 36 individuals indicated they had "no responsibility at all." These 36 individuals were therefore excluded from this survey.

3. Findings

Observation 1: A pattern of cybersecurity threats and experiences is discernable across US healthcare organizations.

Significant security incidents[2] continue to plague US healthcare organizations of all types and sizes. While respondents in the present study report a myriad of cybersecurity threats and experiences, there is a pattern that is discernable; *significant security incidents are a near universal experience in US healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their targets.*

Healthcare organizations continue to deal with challenges on the inside of their organizations as well. Securing healthcare data and managing a cybersecurity program are both complex feats. Healthcare data is widely used internally and must be exchanged with a wide variety of entities in order to facilitate the coordination and delivery of care—something that is complex in and of itself, but securing this data, too, adds on an additional layer of complexity. It is therefore incumbent on healthcare leaders to ensure internal personnel have the training and resources needed to ensure robust internal information security practices are in fact practiced.

1.1 Healthcare organizations continue to experience significant security incidents

When asked a question relating to *significant security incidents* their organization experienced during the past twelve months, 22% of respondents reported they did not experience a significant security incident (Table 3). These findings are in line with the 2018 HIMSS Cybersecurity Survey where 21% of respondents reported that their organization had not experience a significant security incident during the previous 12 months. While the types of significant security incidents appeared to vary by organization type, this variation may be due to differences in levels of awareness about security incidents that may be affecting their respective organizations.

DISCUSSION:
That the majority of respondents acknowledged that their organizations experienced a significant security incident aligns with the historical pattern of healthcare organizations being targeted by bad actors, including cyber adversaries and others.[3] Hospital breaches, especially, have made the headlines. This does not diminish the fact that non-acute and vendor organizations should be less concerned about security challenges than their hospital peers.

---

[2] Respondents were asked a series of questions relating to "significant security incidents" without any definitional direction of this phrase. 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.

[3] See, e.g., https://www.forbes.com/sites/danmunro/2014/08/18/cyber-attack-nets-4-5-million-records-from-large-hospital-system/#1ca34e717f07. However, healthcare is not the only industry targeted (*See, e.g.,* https://outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks).

With approximately two-thirds of non-acute and vendor organizations reportedly experiencing a security incident in the past 12 months, security challenges are very real concerns for leaders in these types of settings too. Indeed, according to the Office for Civil Rights at the US Department of Health and Human Services, approximately fifteen percent of healthcare providers that reported a breach due to a hacking/IT incident in the past 24 months were from hospital systems.[4] The remainder were other types of healthcare organizations, such as physician practices, ambulatory surgical centers, mental health facilities, rehabilitation facilities, and others. However, not all security incidents necessarily rise to the level of a breach and not all breaches are reported.

Table 3: Significant Security Incidents in the Past 12 Months

	2019					2018
Recent Significant Security Incident	Hospital	Non-Acute	Vendor	Other	Total	Total
Yes	82%	64%	68%	76%	**74%**	**76%**
No	14%	33%	30%	20%	**22%**	**21%**
Don't Know	4%	3%	3%	4%	**4%**	**3%**

1.2 Bad actors continue to play a dominant role in significant security incidents

Respondents were presented with an extensive listing of "threat actors" frequently associated with significant security incidents and asked to characterize the sources responsible for their organizations' significant security incidents over the past 12 months. Almost half (48%) of all respondents cited two primary threat actors; *Online scam artists* (28%) and *Negligent insiders* (20%). Similar to 2018 findings, *Online scam artists* continue to be the most frequently cited threat actor (28% in 2019; 30% in 2018). The majority of threat actors involved in security incidents can be characterized as bad actors (e.g., cybercriminals and others with malicious intent) (56%) (Table 4).

DISCUSSION:
The majority of threat actors responsible for a significant security incident were reported to be bad actors (e.g., cybercriminals and others). However, approximately one-third of incidents were reported to be associated with negligent insiders and others, actors reflecting benign motivations. As such, there is a significant need to educate key stakeholders on information security best practices and ensure adoption of the same. In other words, the significant security incidents were not caused intentionally by this latter group but rather were due to lapses in security practices and/or protocol.

[4] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed January 30, 2019).

Table 4: Significant Security Incident in the Past 12 Months – Threat Actors

	2019					2018
	Hospital	Non-Acute	Vendor	Other	Total	Total
Bad Actors	**57%**	**53%**	**54%**	**64%**	**56%**	**59%**
Online scam artist (e.g., phishing, spear phishing, whaling, business email compromise)	27%	31%	26%	30%	**28%**	**30%**
Hacker (e.g. cybercriminal, bug bounty hunter, hobbyist, etc.)	13%	3%	14%	12%	**11%**	**16%**
Social engineer (e.g., vishing or otherwise) (not via online means)	7%	5%	4%	9%	**6%**	**4%**
Malicious insider (bad actors with trusted access who seek to steal information or damage IT infrastructure)	6%	11%	2%	4%	**6%**	**4%**
Nation state actor	2%	3%	4%	5%	**3%**	**2%**
Hacktivist (hacking for a politically or socially motivated purpose; not a nation state actor)	2%	0%	4%	4%	**2%**	**3%**
Benign Actors	**35%**	**25%**	**29%**	**26%**	**31%**	**16%**
Negligent insider (well-meaning but negligent individuals with trusted access who may facilitate or cause a data breach or other cyber incident)	21%	19%	25%	14%	**20%**	**16%**
Vendor or consultant	5%	3%	2%	5%	**4%**	**-**
Third party partner (not a vendor or consultant)	4%	3%	0%	7%	**4%**	**-**
Researcher	5%	0%	2%	0%	**3%**	**-**
Other/Don't Know/No incidents	**8%**	**21%**	**20%**	**11%**	**13%**	**25%**
Other	0%	0%	0%	0%	**0%**	**1%**
Don't Know	6%	2%	2%	2%	**2%**	**3%**
No recent significant incident	2%	19%	18%	9%	**11%**	**21%**

1.3 E-mail is the most common initial point of compromise for significant security incidents

Continuing on with the line of questioning surrounding significant security incidents at their organizations during the past twelve months, respondents were asked to describe the initial point(s) of compromise. The most commonly cited point of compromise was via *e-mail (e.g., phishing e-mail)* (59%), followed by *human error* (25%) (Table 5).

DISCUSSION:
That e-mail (e.g., phishing email) continues to be the most frequently reported initial point of compromise is not surprising as phishing e-mails are inexpensive to generate and can be quite accurate in targeting recipients.[5] E-mail can contain a wealth of information, ranging from sensitive patient information, financial

[5] For more information on phishing, please see the following reference by the US Department of Homeland Security Analytic Exchange Program Vulnerabilities of Healthcare Information Technology Systems team https://www.himss.org/library/phishing-dont-be-phooled.

information, business information, and technical information. Online scam artists using phishing e-mails are known to masquerade themselves as a senior leader within the email recipient's organization (e.g. CEO or CFO) and request sensitive information (e.g., credentials) or even the transfer of funds to an account accessible to the scammer. While phishing continues to be a very effective approach for compromising the integrity of an organization, advances in information security defensive efforts may push bad actors to look to exploit other points of compromises. Information security leaders therefore need to diligently watch other areas of compromise.

Human error is also a significant initial point of compromise. Whether it is accidentally posting patient information to a public-facing website, inadvertently leaking or breaching data, or otherwise, mistakes often happen, resulting in potentially significant consequences for the organization.

Compromise of vendor, consultant, or client credentials are also commonly identified as an initial point of compromise. At least as early as 2014, healthcare organizations and other types of entities have been compromised through vendors.[6] Many healthcare providers report breaches of healthcare data due to a compromise of a business associate, according to data on reported breaches by the Office for Civil Rights at the US Department of Health and Human Services.[7]

Table 5: Significant Security Incident in the Past 12 Months – Initial Point of Compromise

	2019					2018
Initial Point of Compromise	**Hospital**	**Non-Acute**	**Vendor**	**Other**	**Total**	**Total**
E-mail (e.g., phishing e-mail)	69%	56%	35%	68%	**59%**	**70%**
Human error	30%	25%	21%	16%	**25%**	**-**
Compromise of vendor, consultant, client, or other party	20%	3%	0%	8%	**10%**	**3%**
Hardware or software infected with malware "off the shelf" (e.g., pre-loaded malicious software)	7%	8%	9%	8%	**8%**	**3%**
Compromise of mobile device (e.g., malware infection or otherwise)	11%	0%	12%	0%	**7%**	**3%**
Compromise of our organization's website and/or web server (e.g., SQL injection, XSS, etc.)	6%	3%	9%	4%	**5%**	**4%**
Compromise of remote access server (e.g., RDP, VNC, remote access gateway, etc.)	3%	8%	9%	4%	**5%**	**-**
Compromise of medical device (e.g., malware infection or otherwise)	10%	0%	6%	0%	**5%**	**3%**
Compromise of third party website (not a vendor, consultant, or third party partner)	7%	0%	3%	8%	**5%**	**2%**
Compromise of our cloud provider/service	3%	3%	0%	0%	**2%**	**2%**
Other	1%	3%	3%	4%	**2%**	**10%**

[6] Specifically, this technique (i.e. compromising a vendor to get to the primary company) was quite prolific after the compromise of a major retailer in December 2013. *See, e.g.,* https://arxiv.org/pdf/1701.04940.pdf.
[7] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

1.4 Internal resources play a significant role in uncovering significant security incidents

When asked to identify the various individuals responsible for uncovering significant security incidents within their organization during the last 12 months, the majority of respondents cited internal resources; *internal security team* (46%) or *internal personnel* (37%). As with the 2018 HIMSS Cybersecurity Survey, external resources continue to play a secondary role in the detection of information security incidents.

DISCUSSION:
The predominance of internal staff involved in the discovery of significant security incidents suggests organizations would be wise to devote the resources necessary to bolster this line of defense. Suggestions include providing additional security awareness training and education for all staff (not just those involved in day-to-day information security operations and management). Additionally, those involved in day-to-day information security operations and management should receive additional education and training to understand the latest threats and how prevent and/or mitigate them. This includes giving healthcare cybersecurity professionals time off to take training classes and education and paying for them as well. Regular education and training is necessary to arm healthcare cybersecurity professionals with the knowledge and know-how to handle a variety of security incidents and know how to prevent, mitigate, and/or remediate them.

Table 6: Significant Security Incident in the Past 12 Months – Initially Learned About Incidents

	2019					2018
Initially Learned about Incidents	**Hospital**	**Non-Acute**	**Vendor**	**Other**	**Total**	**Total**
Internal Resources						
Internal security team	54%	33%	38%	56%	**46%**	**41%**
Internal personnel (other than internal security team) (e.g., employee)	46%	33%	18%	40%	**37%**	**28%**
External Resources						
Business associate or subcontractor	14%	11%	9%	24%	**14%**	**-**
Retained third party vendor, consultant, or other (e.g., risk assessment results, penetration test results, auditor report, etc.) (but not a business associate or subcontractor)	11%	11%	6%	8%	**10%**	**5%**
Patient whose information was compromised (e.g., identity theft – medical, financial, or otherwise)	11%	3%	0%	0%	**5%**	**3%**
Unsolicited third party vendor, consultant, or other (e.g., report from researcher or consulting firm or vendor, etc.)	3%	0%	9%	0%	**3%**	**4%**
Law enforcement	1%	6%	0%	0%	**2%**	**-**

Observation 2: Many positive advances are occurring in healthcare cybersecurity practices.

Despite significant information security challenges healthcare organizations face, many positive steps are being taken by healthcare organizations. Healthcare organizations of all types and sizes have had to quickly learn and adapt to a rapidly changing cybersecurity landscape. The first major cyber-attack that was reported against a hospital system was in August 2014.[8] This unfortunate event was a wake-up call for the healthcare industry. The notion of "Who would attack a hospital?" has slowly faded away as a new reality presented itself. We are all now targets of cyber adversaries and other bad actors. There are no exceptions. Fortunately, healthcare cybersecurity is a primary concern at many organizations. As a result, healthcare cybersecurity professionals have more resources and budget available to help ensure that their organizations stay ahead of the threats.

2.1 Cybersecurity professionals feel empowered to drive change in healthcare organizations

When asked to rate the extent to which they agreed that cybersecurity professionals were empowered to drive change throughout their organizations, the majority of respondents (59%) indicated some level of agreement with the statement (44% agree and 15% strongly agree) (Table 7). While this finding is encouraging, it is notable that 41% of the respondents stated that they did not feel empowered to drive significant change throughout their organizations.

DISCUSSION:
Cybersecurity professionals in healthcare organizations should be empowered to drive change throughout the system within which they operate. Rather than being "hermetically sealed off" from the rest of the organization they serve, cybersecurity professionals should be both a visible and integral part of the strategic planning and operational infrastructure of their organizations.

Table 7: Cybersecurity Professionals Empowered to Drive Change Throughout Entire Organization

Empowered to Drive Change	N	percent
Strongly Agree	**28**	**15%**
Agree	**81**	**44%**
Neither Agree nor Disagree	38	21%
Disagree	30	16%
Strongly Disagree	7	4%

2.2 IT budgets increasingly reflect cybersecurity allocations

This year's survey asked several questions related to cybersecurity budgeting practices to include what percentage of respondents current organizational IT budgets were allocated to cybersecurity. As noted in Table 8, the majority of respondents (55%) reported that some designated amount of their current IT budget

[8] *See* https://www.modernhealthcare.com/article/20140818/NEWS/308189946.

is allocated for cybersecurity purposes. With allocated amounts varying greatly, it is instructive to note that over one-quarter of respondents (26%) operate within a system that spends money on cybersecurity activities/resources, even though there is no specific cybersecurity "carve out" within the IT budget.

DISCUSSION:
Securing a modern healthcare organization is a complex endeavor. The pervasiveness of cyberattacks as well as the continual emergence of new and evolving threats can stretch an organization's financial and human resources. Healthcare organizations, in general, appear to be responding to this challenge by dedicating more financial resources toward their cybersecurity programs.

In terms of the significance for no specific cybersecurity carve out, the jury is still out on whether this is a benefit or a detriment to an organization's cybersecurity progression; this can be positive, negative, or neutral. For example, a cybersecurity program may be well funded in that the Chief Financial Officer at an organization may grant the cybersecurity program monies as requested. However, in yet other cases, it may be challenging to ask for monies to fund a cybersecurity program, since a business case may need to be made each time. In still other cases, cybersecurity programs may not receive any funds until and if there is a major significant security incident, such as a breach or a ransomware attack that cripples mission critical systems.

Table 8: Percentage of Organization's Current IT Budget Allocated to Cybersecurity

Budget Allocation	N	percent
1 to 2 percent	17	9%
3 to 6 percent	45	25%
7 to 10 percent	20	11%
More than 10 percent	19	10%
No specific carve out	47	26%
No money is spent on cybersecurity	1	1%
Don't Know	34	19%

2.3 The amounts allocated within IT budgets for cybersecurity are increasing

Compared to last year's results, the percent of an organization's IT budget allocated to cybersecurity appears to be increasing. In the 2018 HIMSS Cybersecurity Survey, 21% of respondents indicated their organization allocated 1 to 2 percent of their IT budget to cybersecurity, whereas this year the percentage dedicating the same amount dropped to just under 10% (Table 9). When asked specifically how their organizations' cybersecurity budgets compares to the previous year, 72% of respondents indicated their budgets increased by 5% or more (38%) or remained essentially the same (34%) (Table 10).

DISCUSSION:
Taken together, leadership at healthcare organizations seem to be giving cybersecurity a higher priority and dedicating more financial resources to support their security programs.

Table 9: Percentage of Organization's Current IT Budget Allocated to Cybersecurity 2018 and 2019

Budget Allocation	2018	2019	Change
No money is spent on cybersecurity	3%	1%	-2%
1 to 2 percent	21%	9%	-12%
3 to 6 percent	21%	25%	4%
7 to 10 percent	7%	11%	4%
More than 10 percent	7%	10%	3%

Table 10: Change in Cybersecurity Budget Allocation Compared to Last Year

Change in Cybersecurity Budget	N	%
Increased by 25% or more	13	7.1%
Increased by 10% to 24%	20	10.9%
Increased by 5 to 9%	37	20.2%
Did not substantially change	63	34.4%
Decreased by 5 to 9%	2	1.1%
Decreased by 10 to 24%	2	1.1%

2.4 Security risk assessments are universal practices and have a good degree of uniformity across healthcare organizations

Respondents were presented with a list of 13 components common to organizations and were asked to identify all those components included in their organization's security risk assessment efforts. Virtually all respondents indicated their respective organizations conducted risk assessments, with only 4% reporting their organization did not conduct security risk assessments (Table 11). Notably, eight of the 13 components listed are included in a security risk assessment by approximately 70% or more of the respondents: *workstations and servers* (84%), *networks* (78%), *cybersecurity policies and procedures (and documentation)* (75%), *inventory of assets* (74%), *physical security* (73%), *clinical information systems* (71%), *business and financial information systems* (69%), and *cybersecurity roles and responsibilities* (69%). A substantially similar question was posed in the 2018 HIMSS Cybersecurity Survey. However, there was less uniformity as only 5 components were typically included in a security risk assessment by approximately 70% or more of the respondents; *inventory of assets* (69%), *cybersecurity policies and procedures (and documentation)* (81%), *physical security* (71%), *security awareness and training program(s)* (74%), and *network* (74%).

Note too that 37% of respondents in the 2019 survey indicated their organization conducts comprehensive, end-to-end security risk assessments. These findings are a notable increase over the 2018 survey results where just 26% of respondents reported the same.[9]

[9] 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 14). Thus, healthcare organizations are moving in the right direction in regard to security risk assessments.

DISCUSSION:
We are encouraged by these findings, as the trajectory for risk assessments appears to be moving in a positive direction. While the best type of a security risk assessment is end-to-end (as it is comprehensive in nature), it is good to see a more cohesive, holistic approach to conducting security risk assessments (based upon 8 of the 13 components being typically incorporated into security risk assessments, as reported by the majority of respondents). It appears that the industry continues to move toward a level of uniformity and adopting voluntary, consensus-based, industry-led practices in regard to security risk assessments.[10] That all said, the Office for Civil Rights at the US Department of Health and Human Services recommends that the security risk assessment should be conducted accurately and thoroughly for the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the healthcare organization. [11]

Table 11: Security Risk Assessment Components

Security Risk Assessment Components	N	%
Workstations and servers	**155**	**84%**
Organization's network	**143**	**78%**
Cybersecurity policies and procedures (and documentation)	**138**	**75%**
Inventory of assets	**136**	**74%**
Physical security	**134**	**73%**
Clinical information systems (including electronic health record systems)	**130**	**71%**
Business and financial information systems	**126**	**69%**
Cybersecurity roles and responsibilities	**126**	**69%**
Organization's website	107	58%
Communications plan	104	57%
Other Third party risks	91	50%
Medical devices	86	47%
Comprehensive (i.e., end-to-end)	68	37%
Other	3	1.6%
Does not apply – no security risk assessment conducted	8	4%
Don't know	9	5%

2.5 Security risk assessment results guide risk management activities

Respondents were asked to identify those actions their organization took as a result of conducting a security risk assessment. As noted in Table 12, only 5% of respondents indicated *no additional actions were deemed necessary*, suggesting risk assessments are being used to guide risk management activities. This is a step in the right direction as the vast majority of organizations are using security risk assessment results to take actions (e.g. manage risks) and further enhance their cybersecurity efforts. The following actions were performed following a risk assessment, according to two-thirds or more of the respondents: *adopt new or improved security*

[10] *See* Section 405(d) of the Cybersecurity Act of 2015, codified at 6 USC §1533.
[11] *See* https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

measures (72%), *drafted, revised, and/or tested policies and procedures* (69%) and *replaced or upgraded security solutions* (68%).

DISCUSSION:
Conducting a security risk assessment is best practice that enables organizations to identify and assess risks in a repeatable and structured way. However, it is not enough to conduct security risk assessments if organizations do not use the results of the security risk assessment to help manage risks and improve their security posture. In other words, the results of security risk assessments should not just simply sit on the shelf. Rather, the majority of respondents are using the results of security risk assessments in an effort to improve their cybersecurity programs in some way.

Table 12: Actions Taken after a Security Risk Assessment

Actions Taken after a Security Risk Assessment	N	%
Adopted new or improved security measures (e.g., processes)	**127**	**72%**
Drafted, revised, and/or tested policies and procedures	**122**	**69%**
Replaced or upgraded security solutions	**119**	**68%**
Conducted new or additional training of personnel	105	60%
Replaced hardware, software, devices, etc. that are end-of-life or that have been deprecated (other than those directly related to IT security – e.g., firewalls, IDS, etc.)	98	56%
Conducted a penetration test	80	46%
Switched from one vendor or consultant to another	37	21%
Other	9	5%
No additional actions deemed necessary	8	5%

2.6 Most organizations conduct phishing tests

As noted in a previous section, online scam artists were the most frequently identified type of threat actor for significant security incidents (Table 4), and that email (e.g., phishing email) was, by far, the most frequently identified initial point of compromise for significant security incidents (Table 5), similar to the findings of the 2018 HIMSS Cybersecurity Survey. In light of this, we elected to ask respondents this year about their phishing testing efforts and in particular, their phishing click rate. The majority of respondents (58%) were able to report the phishing click rate at their healthcare organizations, although this did vary by organization type (Table 13).

For organizations conducting phishing tests, most respondents (40%) indicated that the phishing click rate was 10% or less, in line with what has been reported in the healthcare industry.[12] Interestingly, though, a remarkable number of respondents reported phishing click rates of 1 to 5% (16%) and 6 to 10% (24%). Hospitals seem to be performing a bit better than the other organizations surveyed with 45% reporting click rates of 10% or less.

[12] *See https://www.netsec.news/wombat-security-2018-state-of-the-phish-report/.*

DISCUSSION:
Achieving a phishing click rate of less than 10% is desirable for many healthcare organizations. Healthcare organizations of all types and sizes struggle with this and this trend is a significant, positive achievement for the healthcare industry.[13] However, since phishing is still a significant, initial point of compromise, additional work needs to be done to further lower the click rate. This can be done through more frequent security awareness training, phishing simulation, and better monitoring of metrics pertaining to phishing (including whether there are any particular repeat offenders).

Table 13: Conduct Phishing Tests

Status	Hospital	Non-Acute	Vendor	Other	TOTAL
Known "click rate"	**70%**	**50%**	**45%**	**52%**	**58%**
1 to 5%	*15%*	*8%*	*24%*	*20%*	*16%*
6 to 10%	*30%*	*28%*	*15%*	*16%*	*24%*
11 to 15%	*8%*	*6%*	*0%*	*4%*	*5%*
16 to 20%	*6%*	*0%*	*6%*	*4%*	*4%*
21 to 25%	*8%*	*0%*	*0%*	*0%*	*4%*
26 to 30%	*3%*	*8%*	*0%*	*4%*	*4%*
Over 30%	*0%*	*0%*	*0%*	*4%*	*1%*
Unknown "click rate"	**20%**	**14%**	**35%**	**36%**	**24%**
Do not conduct phishing tests	**10%**	**36%**	**21%**	**12%**	**18%**

[13] This would place the healthcare industry in line with other sectors with lower click rates, such as the defense and transportation sectors. *See* https://www.wombatsecurity.com/state-of-the-phish (2018 State of the Phish report).

Observation 3: Complacency with cybersecurity practices can put cybersecurity programs at risk.

While the results of the previous section highlight the positive advances organizations are making with respect to their information security practices, our report would be remiss for not identifying those findings that raise questions about select cybersecurity practices. In this section then, we isolate responses that are not necessarily "bad" cybersecurity practices, but may be an "early warning signal" about potential complacency seeping into the organization's information security practices. Though significant security incidents will continue to occur and the weakest links will be exposed, it is incumbent or security leaders to remain vigilant and advance their cybersecurity practices, know-how, and acumen. Otherwise, our critical infrastructure will inevitably crumble and fall. This is not something we want, especially with patient lives on the line. Healthcare cybersecurity, indeed, is mission critical work.

3.1 Confidence surrounding remediation and mitigation of security incidents

Respondents were presented with a list of ten common factors healthcare organizations face in *remediating and mitigating* security incidents and asked to rate the challenge each issue posed their organization. Using a five-point scale (where 1 = "*no challenge at all*"; 5 = "*extreme challenge*"), the findings displayed in Table 14 are striking in terms of the "lack of passion" expressed by the respondents. To illustrate, the most challenging factor cited by all respondents (*Too many emerging and new threats*) registered an average score of 3.13, meaning it is only "*somewhat of a challenge*" to the respondents. While hospital respondents were slightly more passionate about the listed factors than all other respondents groups, their rating of the various challenges are "muted" at best. That said, there were two factors which percolated as top challenges for all groups; *Too many emerging and new threats* and *Lack of personnel with the appropriate cybersecurity knowledge and expertise*.

DISCUSSION:
The lack of concern expressed about challenges in remediating and mitigating security incidents on the one hand is very encouraging. This finding suggests there are few barriers respondents see as limiting their ability to ensure the integrity of health information. The confidence these findings convey may be reflective of the skewed sample of respondents selected for this study: *health information leaders with a strong understanding of their organization's cybersecurity vulnerabilities and assets*. On the other hand, the lack of passion exhibited raises concerns regarding the information security vigilance these leaders may practice. Over-confident leaders may be "lulled" into believing there are few challenges they face in managing the confidentiality, integrity, and availability of their organization's information and technology infrastructure, and may be susceptible to "dropping their guard. It is also very possible that respondents to this year's survey were overwhelmed by financial-constraints and understaffing (consistent with the findings of the 2018 HIMSS Cybersecurity Survey). If true, there may be a bit of "numbness" in discerning those factors that are truly significant barriers.[14] In any event, it is clear that more attention and focus needs to be paid to remediating and mitigating security incidents to ensure better information security and, in turn, patient safety.

[14] *Cf.,* Table 24 of the 2018 HIMSS Cybersecurity Survey. Pretty much all kinds of potential threats are perceived threats to the organization.

Table 14: Barriers for Remediation and Mitigation of Security Incidents

Challenges	Hospital	Non-Acute	Vendor	Other	TOTAL
Too many emerging and new threats	3.23	3.33	3.03	2.68	**3.13**
Lack of personnel with the appropriate cybersecurity knowledge and expertise	3.11	3.19	3.21	2.92	**3.12**
Lack of financial resources	2.90	2.69	3.09	2.84	**2.89**
Too many application vulnerabilities	3.17	2.47	2.76	2.48	**2.83**
Too many endpoints (e.g., user devices, computers, etc., connected to the network)	3.11	2.47	2.74	2.44	**2.80**
Lack of security awareness training	2.79	2.58	2.59	2.28	**2.63**
Lack of information sharing of threats, mitigation, and know-how with external parties (e.g., other providers, payers, etc.)	2.52	2.36	2.50	2.16	**2.43**
Network infrastructure too complex to secure	2.79	2.00	2.26	2.16	**2.42**
Lack of organizational will (e.g., executive buy-in, corporate culture, etc.)	2.37	2.61	2.44	1.96	**2.37**
Too many users for timely and effective provisioning and de-provisioning of accounts	2.52	2.33	2.24	1.92	**2.33**

3.2 Adoption and application of policies and procedures

Respondents were presented with two statements regarding information security practices at their organization and asked to rate the extent to which they agreed with each statement (where 1 = "Strongly disagree"; 5 = "Strongly agree"). The findings suggest respondents are somewhat more positive about their employees' understanding about what actions to take per the organization's policies and procedures (average score = 3.54) than they are about employees putting those policies and procedures into practice (3.28)(Table 15).

DISCUSSION:
The apparent disconnect between "knowing what to do" and "doing what needs to be done" is a dilemma managers face on an array of issues. It is possible that the policies and procedures may be outdated, may not necessarily be clear, and/or the policies and procedures may have been written by administrative staff who may not be involved in day-to-day security operations. It is also not uncommon for many exceptions to be granted to policies and procedures that are in place and/or for employees to ignore the policies and procedures (with good security practices being perceived as a barrier or a hindrance to getting work done). Additionally, even if staff may know what to do, they may choose to ignore the policies and procedures that are in place.

These findings suggest healthcare leaders would be wise to take "a step back" and determine what needs to be done to increase the effectiveness of the written cybersecurity policies and procedures. Such proactive steps may include ensuring that the written policies and procedures are up to date, accurate, updated on a regular basis, easy to read and understand, and to think about what can be done in terms of enforcement of policies and procedures (including coordination with IT, legal, and human resources departments). Policies and procedures with no "teeth" may not give employees much incentive to adhere to them. Furthermore, policies and procedures that are not necessarily enforceable may not be very effective.

Table 15: Policies and Procedures

Challenges	Hospital	Non-Acute	Vendor	Other	TOTAL
Employees knowledgeable about policies & procedures	3.46	3.53	3.56	3.76	**3.54**
Our organization's cybersecurity practices closely follow our written policies and procedures	3.06	3.08	3.65	3.68	**3.28**

Observation 4: Notable cybersecurity gaps exist in key areas of the healthcare ecosystem.

In the final section of the report, we highlight those responses that raise grave concerns regarding the cybersecurity practices in US organizations.

4.1 Some healthcare organizations do not conduct phishing tests

As previously reported, when asked about their organizations' email phishing test results, 18% of respondents stated their organization did not conduct phishing tests (Table 13). Whether or not phishing tests are conducted varies by organization type with a significant portion of non-acute care organizations not conducting phishing tests at all (36%) (Table 16).

DISCUSSION:
The percentage of organizations not conducting phishing tests is disconcerting. This is especially true for non-acute organizations. In light of evidence presented earlier in this report citing the pervasiveness of online scam artists using phishing emails to compromise healthcare organizations (Table 5), it is incredible that any organization in this environment would not be testing a known vulnerability. We are online and connected more than ever. Given that e-mail is a major form of communication and means for data exchange, it's not surprising that bad actors are becoming very sophisticated in developing well-crafted phishing e-mails designed to fool even the experts. Note too that social phishing (i.e., social media phishing) and vishing (i.e., phishing by voice calls), are also on the rise. Regardless of the form, the bottom line is that the weakest link in any cybersecurity program is the human, phishing seeks to exploit the human.

Healthcare organizations must know where they are in terms of a baseline risk vis-à-vis the phishing threat. Healthcare organizations should also be tracking the phishing click rate to gauge whether or not there is improvement in this regard. By failing to conduct phishing tests, organizations are in essence leaving the "door" open to attackers. Conducting phishing tests and monitoring associated metrics do not necessarily involve a significant amount of monetary spend or time. There are free tools available to conduct phishing tests (in addition to subscribing to paid services). Accordingly, all organizations, no matter how large or small and no matter what the budget, should be conducting phishing tests. As with any type of security incident, it is a best practice to take proactive measures instead of being reactive (i.e., waiting until a breach or other significant security incident actually occurs).

Table 16: Conduct Phishing Tests

Status	Hospital	Non-Acute	Vendor	Other	TOTAL
Known "click rate"	70%	50%	44%	52%	**58%**
Unknown "click rate"	20%	14%	35%	36%	**24%**
Do not conduct phishing tests	10%	36%	21%	12%	**18%**

4.2 Pervasiveness of legacy systems

Finally, respondents were asked to indicate the percentage of their systems running off legacy (unsupported) operating systems. As noted in Table 17, a majority of respondents (69%) indicated that they had at least some legacy systems in place at their healthcare organizations. Moreover, 14% of respondents claimed over 10% of their systems qualify as a legacy operating systems. When asked to identify the legacy system(s) in place at their organization, almost half of the respondents (48%) cited *Windows server* (Table 18) [15]. Other legacy commonly used include; *Windows XP* (35% of respondents),[16] *embedded legacy operating systems in medical devices* (33%),[17] and *embedded legacy operating systems in industrial control systems* (e.g., HVAC) (20%) (Table 18).[18]

DISCUSSION:
As current and patched operating systems are foundational to secure information environments, running a legacy operating system is an ill-advised practice. Operating systems that have been unsupported for five, ten, or more years (decades in some cases)[19] greatly increases a healthcare organization's risk of being compromised. This is particularly significant in light of recent international cyber-attacks such as WannaCry and NotPetya. Based upon these findings, healthcare organizations may still be vulnerable to future attacks using the same or similar exploits. Thus, the level of sophistication needed to compromise some healthcare organizations – especially if their systems may not be patched – may not need to be very high. Furthermore, a fair number of vendors, consultants, and others reported having such legacy systems in place. Even if a healthcare provider may not have such legacy systems in place, an attacker may compromise the vendor to get to the healthcare provider.

The problems of legacy systems do not stop there. Legacy medical devices and/or industrial control systems such as HVAC systems can serve as an entry point for cyber adversaries. While the security of medical devices and industrial control systems is an often discussed topic, many do not understand both sides of the equation. Inherently, medical devices and industrial control systems have their own respective and unique levels of complexity. Changing these devices and systems may be much more difficult, time consuming, and expensive than others may believe. Furthermore, securing medical devices is even more complex when one appreciates that the consumer is sometimes the healthcare provider and sometimes it is the patient itself. Thus, when there is a vulnerability affecting the medical devices, one set of individuals may be made aware while another set may not be (e.g., patients may be aware, but their hospitals may not be aware). Hence, there is a need for all stakeholders (including patients, as applicable) to come to the table and discuss how to help advance problems related to medical device security and the security of industrial control systems.

Finally, it is significant to note that not all organizations can afford to upgrade legacy systems to supported versions of the operating systems. And for those that can, upgrading may not be a viable option. For

---

[15] The majority of the respondents with legacy *Windows Server* systems in place were from *hospitals, multi-hospital systems, integrated healthcare delivery networks* and *academic medical centers* (57% of respondents). An additional 10% of respondents were from *vendors*. This is an interesting trend, given the WannaCry cyber-attack that had happened previously and the associated EternalBlue SMB exploit. *See* https://www.us-cert.gov/ncas/alerts/TA17-132A.
[16] The majority of the respondents with *Windows XP* systems in place were from *hospitals, multi-hospital systems, and integrated healthcare delivery networks* (63% of respondents).
[17] The majority of the respondents with *embedded legacy operating systems in medical devices* in place were from *hospitals, multi-hospital systems, integrated healthcare delivery networks* and academic medical centers (74% of respondents.
[18] The majority of the respondents with *embedded legacy industry control systems* in place were from *hospitals, multi-hospital systems, and integrated healthcare delivery networks* (67%).
[19] *See, e.g.,* https://en.wikipedia.org/wiki/Timeline_of_Microsoft_Windows, https://www.informationweek.com/vms-operating-system-is-30-years-old-customers-believe-it-can-last-forever/d/d-id/1061051, https://en.wikipedia.org/wiki/MS-DOS, and https://en.wikipedia.org/wiki/OS/2.

example, a computer program may only run on an older operating system, such as Windows XP or MS-DOS. Industrial control systems such as HVAC and medical devices, too, quite often run on legacy operating systems, which are embedded. Again, there may be no viable option in upgrading these and/or the economics may not justify the upgrade. Furthermore, there may be pushback from administrators, clinicians, and others to not change systems since, from their perspective, everything works fine and some may argue that a significant change to patient care and workflow may result in the event of any such change.

Table 17: Percent of Legacy Systems

Percent of Legacy Systems	Hospital	Non-Acute	Vendor	Other	TOTAL
1 to 10%	72%	50%	38%	32%	**54%**
11 to 20%	6%	8%	12%	-	**7%**
21 to 30%	6%	3%	3%	4%	**4%**
31 to 40%	1%	3%	6%	-	**2%**
41 to 50%	-	-	-	4%	**1%**
More than 50%	1%	-	-	-	**1%**
Don't know	11%	11%	9%	24%	**13%**
Does not apply	3%	25%	32%	36%	**19%**

Table 18: Legacy (unsupported) operating systems in place

Legacy Operating System	N	%
Legacy Windows Server (e.g., 2003, 2008, 2012, 2016)	88	48%
Windows XP	64	35%
Embedded legacy operating system in medical device	61	33%
Embedded legacy operating system in industrial control system (e.g., HVAC)	36	20%
Legacy Linux system	24	13%
Windows 2000	10	5%
Windows NT	10	5%
Legacy VMS system	10	5%
Legacy Unix system	9	5%
Windows Vista	6	3%
MS DOS	4	2%
OS/2	3	2%
Windows 7	2	1%
Windows ME	2	1%
Other	3	2%
None of the Above	46	25%
Don't Know	18	10%

4. Conclusion

The findings of the **2019 HIMSS Cybersecurity Survey** suggest that healthcare cybersecurity practices are moving in the right direction with some degree of uniformity. The findings also suggest there is room for improvement. While there is positive progress, budgets allocated to cybersecurity are still quite small. The lack of knowledgeable cybersecurity personnel also continues to hinder progress. Legacy systems, too, present a problem in need of novel solutions. On the whole, however, it seems that healthcare organizations are indeed improving their cybersecurity programs in spite of these challenges.

5. About HIMSS

HIMSS is a global advisor and thought leader supporting the transformation of health through the application of information and technology. As a mission driven non-profit, HIMSS provides thought leadership, community building, public policy, professional/ workforce development and engaging events to bring forward the voice of our members. HIMSS encompasses more than 70,000 global individual members, 630 corporate members, and over 450 non-profit organizations. Thousands of volunteers work through HIMSS to leverage the innovation of digital health to improve both the health of individuals and populations, as well as the quality, cost-effectiveness and access of healthcare.

HIMSS innovation companies offer a unique breadth and depth of expertise and capabilities to support healthcare systems and market suppliers. HIMSS designs and leverages key data assets, guides operations and clinical practice through predictive analytics tools and maturity models 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.

Headquartered in Chicago, Illinois, HIMSS serves the global health information and technology communities with focused operations across North America, Europe, United Kingdom, Middle East and Asia Pacific.

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 **2019 HIMSS Cybersecurity Survey**.

7. For More Information

Karen D. Groppe
Senior Director, Strategic Communications
HIMSS
33 W. Monroe, Suite 1700
Chicago, IL 60603
312-965-7898
kgroppe@himss.org