The Rampant Growth of Cybercrime in Healthcare

February 08, 2017

Workgroup for Electronic Data Interchange
1984 Isaac Newton Square, Suite 304, Reston, VA. 20190
www.wedi.org

Sponsored By:

FORTINET®

Table Of Contents

Disclaimer

While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial or other professional advice or recommendations by WEDI. The listing of an organization does not imply any sort of endorsement and WEDI takes no responsibility for the products, tools and Internet sites listed.

The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by WEDI.

Document is for Education and Awareness Use Only

INTRODUCTION

Healthcare security breaches and criminal attacks are surging in frequency, scope and sophistication, making them increasingly difficult to detect, prevent and mitigate. The past two years have seen a record number of breaches and records exposed. In 2015, more than 120 million healthcare records were compromised in data breaches, and in 2016 more than 315 major breaches were reported among healthcare organizations.[1]

The widespread use and exchange of digital personal health information has created a hotbed for cyberattacks conducted by sophisticated threat adversaries. Despite heavy investment and implementation of health information technology (e.g. electronic health record systems, databases, registries, repositories, connected medical/personal devices and other software) organizations are increasingly vulnerable because they do not have sufficient cybersecurity resources, processes or encryption measures in place. In the healthcare industry, data breaches today are primarily the result of threats that are able to gain unauthorized access to records that would otherwise be preventable with appropriate measures deployed. It is therefore critical for healthcare stakeholders to elevate cybersecurity as a core asset that is integrated into care delivery, coordination, communication and management.

PURPOSE OF ISSUE BRIEF

This issue brief summarizes cybersecurity topics that were discussed at multi-stakeholder cybersecurity roundtables convened in November, 2015 and April, 2016 by the Workgroup for Electronic Data Interchange (WEDI). In follow-up to a primer published on the anatomy of a cyberattack,[2] this issue brief explores some of the common vulnerabilities of healthcare organizations that are typically exploited by threat adversaries in today's environment as well as best practices to mitigate these vulnerabilities.

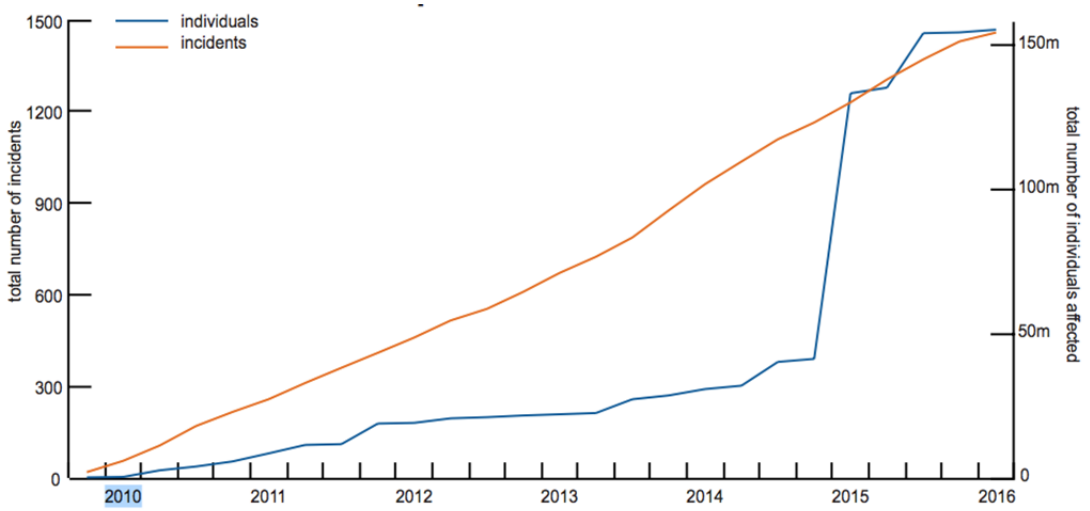
LANDSCAPE OF CYBERATTACKS

Compared with data from other industries, medical records are far more valuable to steal given the wealth of information (e.g. social security number, address or claims data) that can be used and re-used for identity fraud. While credit cards can be quickly cancelled and replaced, there is often no straightforward contingency plan for healthcare records once they have been breached. As a result, a medical record can fetch as much as $20 on the black market – more than ten times as much as a credit card number. The high value of digital healthcare records has attracted organized crime and government-sponsored entities that in turn are capable of launching sophisticated attacks to disrupt, disable, destroy or maliciously control digital technology and data of organizations. As cybercrimes have become more prevalent and complex in healthcare,

[1] http://www.hipaajournal.com/largest-healthcare-data-breaches-of-2016-8631/
[2] www.wedi.org/knowledge-center/resource-view/resources/2015/06/19/perspectives-on-cybersecurity-in-healthcare

they are also causing greater damage. Data breaches cost the healthcare industry approximately $6.2 billion each year, with the average breach incurring damages of $2.2 million and compromising 3,128 records per incident.[3] According to one study, 90 percent of healthcare organizations responding to a recent survey reported having a data breach within the past two years; and as shown in the figure below, the number of breaches and individuals affected shows no signs of abating[4]. Although more records were breached in 2015 than 2016 due to several massive cyberattacks targeting health plans, 2016 actually saw a greater number of breaches, the largest of which predominantly impacted provider organizations.[5]

Figure 1: Number of Breaches and Affected Individuals in the U.S.[4]



While the scale of publicly reported data breaches has certainly called attention to cybersecurity, only 40 percent of healthcare organizations express concern about cyberattacks or report that their cybersecurity budget has increased in response to threats.[6] Nonetheless, the true risk, cost and prevalence of cyberattacks in healthcare is likely far greater than most are aware. Chronic underinvestment in cybersecurity has left many so exposed that they are unable to even detect cyberattacks when they occur. While attackers may compromise an organization within a matter of seconds or minutes, it often takes many more weeks – if not months – before the breach is detected, damage is contained and defensive resources are deployed to prevent the same attack from happening again. Indeed, a breach typically goes undetected for an average of 229 days. In the case of organized crime, the delay may be much longer if a comprehensive campaign is conducted to covertly achieve command and control. Once an organization has been compromised, the damage and cost of a breach can

[3] http://www.ponemon.org/blog/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1

[4] https://www.brookings.edu/research/hackers-phishers-and-disappearing-thumb-drives-lessons-learned-from-major-health-care-data-breaches

[5] http://www.hipaajournal.com/largest-healthcare-data-breaches-of-2016-8631

[6] http://www.ponemon.org/news-2/66

significantly increase with every minute that passes as information is harvested or systems are disrupted and damaged. Without an effective means of detecting threats that have entered or tried to enter a system in a timely manner, organizations are fundamentally handicapped in their ability to respond appropriately.

In addition to their data being more valuable than in other industries, healthcare organizations - particularly providers – are also more vulnerable across multiple attack surfaces and vectors. As patients journey across the healthcare continuum of primary, acute and post-acute care, each touchpoint increases the risk of a cyberattack due to the amount of information stored and exchanged between organizations that operate within an interconnected network which, once breached, can put them all at risk. Hospitals in particular have become incredibly vulnerable to cyberattacks due to the number of systems, devices and staff that cybercriminals can target as a beachhead or launch point into the network. In the past, risk and vulnerabilities were far more easily contained to specific systems, networks and operations. Over time, however, attack surfaces have multiplied as organizations cobbled together a health information technology (health IT) infrastructure comprised of new components, legacy hardware and antiquated software from multiple vendors. Furthermore, the decentralization and fragmentation of healthcare services has not only expanded care delivery and data exchange into new settings that need to be managed, but also introduced new virtual care modalities (e.g. telemedicine and mobile health) that are further complicating cybersecurity efforts.

Today, provider organizations rely on a limited portfolio of basic security tools focused on antivirus, malware and firewall vulnerabilities, but lack a deeper set of prevention, encryption, detection, authentication and protection strategies.[7] While a defensive patchwork of interfaces, policies, procedures, services, staff and resources can be implemented, it is all but impossible to safeguard every physical (e.g. easily accessible computers), technical (e.g. unaudited technology), application (e.g. unpatched software) and organizational (e.g. lack of breach notification) weakness. As health data becomes more liquid and less easily controlled in mobile and cloud environments, security vulnerabilities and attack surfaces are expected to increase exponentially. Indeed, many experts expect that the ubiquity and usability of medical devices and wearables will lead them to emerge as the primary cyberattack surface and threat.

With these trends in mind, it is critical for organizations to assess their current approach to cybersecurity, understand potential adversaries that they may encounter and identify the vulnerabilities that may be targeted before developing a comprehensive and robust strategy to effectively detect, mitigate and prevent cyberthreats across multiple fronts.

[7] http://www.himss.org/sites/himssorg/files/2016-cybersecurity-report.pdf

Types of Threat Adversaries

Threat adversaries strive to identify and exploit weaknesses in an organization. As the value of digital healthcare records and vulnerability of healthcare organizations have grown, the primary threat adversaries responsible for cyberattacks have evolved from opportunistic individuals to highly sophisticated, organized entities that are redefining the scope and complexity of cyberattacks. In the early days, cyberattacks were often focused on primitive means of gaining unauthorized access to information or private sections of a facility. Today, however, campaigns are highly coordinated to systematically exploit human, software, hardware and network weaknesses. The table below summarizes some of the threat adversaries that are commonly encountered.

Table 1: Common Types of Threat Adversaries

Level of Threat	Type of Threat Adversary	Characteristics of Adversary
Low	**Internal user errors/negligence**	Human error (e.g. system configuration) and negligence can cause widespread damages, cause outages or bring down critical resources such as firewalls, routers and servers across a department or organization
	Opportunistic hackers	Typically "script kiddies" driven by notoriety or profit-driven security researchers and hackers
Medium	**Insider threats**	Often disgruntled employees or ex-employees looking for revenge and/or financial gain that can be exploited at a relatively low cost for a high reward
	Hacktivists	Attacks are conducted to achieve a political agenda or raise awareness through propaganda and/or damage
High	**Organized crime**	Profit-driven attacks target breaches that can pull personally identifiable information at a massive scale
	Government-sponsored entity	Targeted, well-funded attacks that are motivated by political, economic or military reasons

As cyberattacks become more expansive, adversaries often farm out phases of a campaign to different specialized operatives, affiliates and partners. The diffusion of actors can make attacks not only more difficult to detect but also prevent and mitigate. Generally speaking, roles can be divided in two parties: **crimeware producers** develop source codes that can be weaponized to target vulnerabilities in hardware and software, while **crime service enablers** can assist the delivery of an attack by transferring money, renting out services (e.g. botnets for malware installs, spam and distributed denial-of-service attacks), hosting infections, installing skimmers or providing quality assurance for packers, scanners and crypters. In 2016, the leading causes of reported data

breaches in healthcare were unauthorized access (40 percent) and hacking (33 percent), while theft and loss of data actually saw a decrease in the number of incidents.[4] These causes reflect growing concerns among healthcare organizations around the insider threat of employee negligence in handling personal health information, devices and communication.

Types of Vulnerabilities and Attacks

Vulnerabilities in an organization's security policies, procedures and resources (e.g. identification, authentication, patch management, encryption and antivirus, firewall and intrusion protection) can open the door to an attack. External vulnerabilities may include those that may emerge during a natural disaster, terrorist attack or other event that distracts organizations from responding quickly. Internal vulnerabilities include **zero-day vulnerabilities** that can be attacked the same day that they are discovered before there is time to fix code, distribute a patch or install an update. Despite technical vulnerabilities in hardware and software, criminals often seek to exploit human behavior because it is the easiest factor to manipulate – and the most difficult for organizations to consistently change or control.

A wide range of **social engineering** tactics can be employed by criminals to manipulate individuals into providing confidential information that can bypass security protocols and enable further access to an organization's software, systems and networks. In 2015, phishing attacks were the most common social engineering tactic utilized and were featured in more than two-thirds of cyberattacks.[8] In a typical phishing scam, criminals present themselves as a trustworthy entity to unsuspecting victims through electronic communication that describes a spoofed scenario and urges recipients to click on a link to a website that appears authentic but is in fact malicious. For example, users may be asked to verify and update their account information online within a short timeframe to encourage them to act quickly without thinking too carefully about the request. Typically sent en masse to large numbers of targets, phishing attacks yield a high rate of success for criminals. An average phishing attack is able to compromise an organization within approximately 80 seconds. Moreover, people are increasingly susceptible to opening and clicking on phishing bait; more than 23 percent of email recipients open phishing messages and 11 percent click on malicious links or attachments.[5] Phishing attacks can also be delivered at a smaller scale to achieve certain objectives. **Spear phishing** schemes feature tactics that are targeted to a specific organization or department with elaborately tailored content, sender impersonation or access-control bypass techniques. Similarly, **whaling** is even more specifically personalized to executive management, often with the intent of obtaining confidential corporate information.

Once an organization has been breached, unauthorized access can lead to significant losses in data availability, confidentiality, integrity and privacy. Today, phishing is often used as a vehicle to covertly conduct additional reconnaissance, maintain a foothold

[8] http://news.verizonenterprise.com/2015/04/2015-data-breach-report-info/

inside the network and gather as much as data as possible. In more than 25 percent of data breaches, criminals were able to harvest and exfiltrate data within minutes of a user clicking on phishing bait.[5] Typically, malicious links and attachments deliver **spyware** to monitor information about user habits, activity and applications, or **malware** to damage and disable devices and systems. The table below displays several broad categories of malware that are employed to achieve different objectives. Malware is extremely difficult to detect and defend against given that it is polymorphic in nature and constantly evolving. Roundtable participants estimated that 70 to 90 percent of malware samples are unique to each organization, and that malware can mutate into as many as 120 different variants within the first hour of detection.

Table 2: Common Types of Malware Delivered to Healthcare Organizations

Type of Malware	Example	Characteristics
Contagious	**Virus**	Infects software and spreads copies of itself once software is opened and/or used
	Worm	Infects software and spreads copies without requiring user action
Masked	**Trojan**	Software appears to be benign but contains concealed malware that is released upon download and installation
	Rootkit	Conceals malware from antivirus detection and removal programs (but doesn't cause any damage directly)
	Keystroke logger	Programs or hardware that allow user strokes to be covertly monitored and recorded (usually to harvest passwords)
	RAM Scraping	Software steals plaintext data from credit and debit cards during transactions before they are encrypted on point of sale (POS) machines
Other	**Adware**	Embedded script or code that can automatically display or download malware
	Rogue security software	Software that misleads users into believing a virus is on their system and manipulates them into installing a fake malware removal tool – which instead often releases a Trojan or a form of ransomware
	Ransomware	Malware that prevents or limits users from accessing their system or device, or encrypt specific files until a ransom has been paid.

As cyberattack strategies and techniques have evolved, a cottage industry has rapidly emerged in the wake of **ransomware** and crypto-currency. Until several years ago, cybercriminals may have limited themselves to "scareware" that threatened or intimidated users into paying a ransom at a drop location or to a bank account before a certain date to avoid losing data forever. Today, however, operators can cause significantly more disruption to an organization by encrypting and blocking access to a target's systems, devices or specific files that can only be unlocked with a decryption key

once payment is received. Leverage can be applied to further cripple a target organization by using infection routines that spread across networks or servers. If and when payments are made under agreed conditions, access to systems may not be fully restored and cybercriminals can disappear back into anonymity thanks to digital currencies like Bitcoin that make it difficult to trace payment. Over the past several years, adversaries have moved from targeting individual devices and systems to more global networks with Distributed Denial of Service (DDoS) attacks that cause far greater damage and disruption to an organization. By attacking multiple computers and Internet connections, DDoS flood a targeted resource with incoming traffic until online service becomes unavailable. As malicious software is spread through emails, social media and websites, adversaries can remotely leverage massive networks of infected computers or botnets, to launch a distributed attack on TCP connections, bandwidth and applications from hundreds of thousands of different points of origin, making it exceptionally difficult to defend against.

Of the current cyber threats that compromise data today, healthcare organizations are most concerned by ransomware (69 percent), phishing attacks (61 percent) and negligent insiders (55 perdent).[7] Notably, these are often the most difficult to prevent and protect, given the human elements involved. Indeed, no matter how strong the firewall, antivirus, encryption and intrusion protection deployed, criminals with sufficient resources, patience and coordination can consistently find a way to compromise a system or network through the weakest link – people. Few healthcare organizations rigorously monitor or enforce adherence with security protocols among employees. Providers consistently display low levels of cybersecurity literacy, and IT teams are often understaffed and underfunded to appropriately train staff. More worrisome, a recent study found that 78 percent of IT security professionals had plugged in a USB flash drive that was found abandoned or lying around – and 90 percent would insert a flash drive imprinted with their company's logo despite the potential risks of malware and loss of information.[9] Given the number of devices, software, systems networks and modalities through which confidential data is regularly accessed, stored and exchanged between healthcare organizations, these statistics are particularly sobering given that the most basic of security protocols are not being followed by the very employees who are the most literate in security and aware of the risk of cyberattacks. In the few cases of healthcare organizations that are able to successfully implement a strong culture of cybersecurity and adhere to best practices, they are still vulnerable to threats across their greater network of partners and third party organizations that may not protect personal health information or employ skilled security professionals to the same set or degree of standards.

[9] http://www.marketwired.com/press-release/ahnlab-survey-78-it-professionals-admit-picking-up-plugging-in-abandoned-usb-drives-1769319.htm

Key Mitigation Best Practices

In light of the cybersecurity challenges identified, roundtable participants identified the following best practices for mitigation to the industry:

1. **Drive a cultural change in how cybersecurity is approached in healthcare, beginning with raising awareness to educate stakeholders around the risk and cost of cyberattacks.** Currently, cybersecurity is too often perceived as an issue that only concerns IT support staff, rather than a core business asset that critically impacts every department of an organization. The implementation and management of robust cybersecurity strategies must go beyond technical aspects to embrace the process of tackling human factors and driving culture change. Similar to the call to action spearheaded by the Institute of Medicine in the early 2000s to improve the quality of care, a paradigm shift is needed to fundamentally reframe cybersecurity as a national priority that concerns the value of care and patient health and safety. While culture change must begin from within each healthcare organization to be more aggressively defensive, it must also extend beyond to the greater landscape of health and life sciences at large to encourage a more collective mindset. Currently, cybercrime is often a tragedy of the commons where fragmented self-interests encourage organizations to circle their wagons, rather than transparently communicate and effectively coordinate a response to limit collateral damage to the broader healthcare community. In today's environment of insider threats targeting human vulnerabilities through social engineering, raising awareness among employees of the need to handle health data and devices with care is woefully insufficient – organizations must actively train and retrain staff at all levels with best practices in how to appropriately prevent, detect, respond, report, manage, mitigate and recover from cyber crimes.

2. **Build the business case for cybersecurity and move it into the executive suite.** Healthcare organizations, particularly providers, are in desperate need of training and resources to achieve basic levels of protection. However, cybersecurity strategies are often perceived as cost-prohibitive because organizations are not fully aware of their liability, risk or cost of cyberattacks. Without an accurate understanding of return-on-investment, executives may be unwilling to invest appropriate resources into building a secure IT infrastructure or hiring and retaining security professionals if they perceive greater value in other assets. Accordingly, cybersecurity must be moved off the IT desk and into the C-Suite so that strategies can be more effectively planned, executed and integrated by a Chief Security Officer (CSO). Given how many cyberattacks continue to be attributable to human error and behavior, employees at most healthcare organizations need a CSO whose department can oversee compliance with protocols, drive user training around how health data should be securely accessed, used, stored and

shared according to best practices, and continuously monitor vulnerabilities that threat adversaries may seek to exploit.

3. **Develop cybersecurity frameworks that provide a robust, forward-facing roadmap to protect organizations in a changing environment.** To date, frameworks such as the National Institute of Standards and Technology (NIST) Framework for Critical Infrastructure Cybersecurity[10] and the Health Information Trust Alliance (HITRUST) Risk Management Framework[11] have provided an initial blueprint for existing standards, policies, procedures and principles to assess, establish, manage and improve cybersecurity programs. However, the majority of healthcare organizations are vulnerable to cyberattack methodologies conducted today – and largely unprepared for the threats that may arise in the future. NIST and HITRUST frameworks are helpful in providing the initial groundwork for a strategic roadmap to address vulnerabilities, but organizations must execute additional tactical steps such as proactive patch management, legacy decommissioning and realignment of systems. As mobile and cloud-based technologies become more pervasive in healthcare, it will be increasingly important for organizations to adopt a multi-layer network security approach that ensures that data is protected, segmented and monitored.

   In the current environment, organizations need a common set of best practices and standards for data to be safely and securely shared. On the one hand, the decentralization of care delivery and the growing liquidity of health data between different settings are redefining the arena that must be protected with more robust, end-to-end solutions. Organizations must expand beyond control of how data is received, used and stored internally to also address how data is managed externally across different endpoints and devices. On the other hand, frameworks must also provide cost-effective measures for organizations to adopt at scale. Regardless of the buy-in from leadership, many small to mid-size organizations do not have the budget to implement comprehensive cybersecurity solutions or retain enough trained staff when security professionals may be better compensated in other industries. It is therefore all the more important that organizations raise awareness around the importance and value of keeping health information safe, and to train employees around best practices in cybersecurity. Ultimately, if cybersecurity practices are to be as commonplace and routine as handwashing and hygiene in healthcare, it is likely that processes will need to be incorporated into a common checklist for teams to rigorously follow. As one roundtable participant noted, developing a basic protocol can be as

[10] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[11] https://hitrustalliance.net/documents/csf_rmf_related/HITRUST-RMF-Whitepaper-2015.pdf

simple as adapting the emergency response first-aid checklist developed by the American Red Cross to keep a victim alive, prevent the condition from worsening, apply aid until help arrives, and ensure the victim receives appropriate care:

a. Assess the scene: Is it safe to access the network, system or device? What happened? Who was involved? What is the initial impression of the incident? What is the appropriate course of action? Is additional help needed to safely respond without causing additional damage?
b. If systems are responsive and there is no severe damage: conduct end-to-end assessment for signs of a cyberattack, evaluate the extent to which systems may be compromised, and deploy response consistent with knowledge and training according to the conditions encountered.
c. If systems are unresponsive and/or there is severe damage: send for help, conduct end-to-end assessment, limit contact with devices, systems and/or network, and prevent additional damage or exposure.

Looking ahead, security frameworks must also provide flexibility to address emerging threats. Today, many organizations develop cybersecurity strategies based on previous attacks or intrusion techniques. As a result, organizations may be focused on the privacy, confidentiality and fraud issues stemming from a data breach, while being wholly unprepared for the possibility of new threats such as data integrity loss. The FBI expects that organized crime and government-sponsored entities will exploit data-poisoning to threaten the system integrity of an organization and severely harm patient safety and health outcomes by disabling software or altering data fields (e.g. medication dosage and expiration date). With such threats on the horizon, it is critical for organizations to war-game how to not only defend against new cyberattack methodologies, but also recover from them. While these efforts may have been limited to simply backing up data in years past, organizations today must develop, document, test and implement a Disaster Recovery Plan (DRP) to be able to effectively restore availability of critical applications and access to information in a timely, organized and efficient manner. DRP procedures can be particularly useful for cyberattacks (such as ransomware incidents where data or systems are being held hostage) because of the discrete steps developed to limit the magnitude of loss, minimize the duration of service interruptions, control and repair the damage, recover data, relocate and migrate information, and prepare personnel to respond appropriately.

4. **Apply lessons learned from other industries.** To date, the healthcare industry has not been able to address cybersecurity as successfully as in other sectors. Roundtable participants observed that the financial industry was able to effectively mitigate threats in part because stakeholders worked together to develop a universal response in compliance with federal and

state regulators. Although the financial environment is not necessarily as complex as healthcare in terms of the processes, technologies, systems, transactions or actors that must be assessed and audited, roundtable participants advised that the federal and state government play a more aggressive, strict and active role in certifying, regulating and enforcing security. Under the current approach, many healthcare organizations fail to perform comprehensive risk assessments of security incidents despite the federal mandate. Risk assessments are a key first step to an effective cybersecurity strategy. After establishing the types of data accessed, stored and exchanged by different users, software and hardware, assessments help identify vulnerabilities and information that can be potentially manipulated. In turn, these insights inform the implementation of appropriate security and authentication protocols for personnel and systems, as well as the development of written incident response plans and recommended data governance agreements with other organizations.

CONCLUSION

Over the past several years, cybersecurity has come into acute focus for healthcare stakeholders in the wake of record data breaches. However, the industry at large has been unable to adequately respond defensively or sufficiently invest in resources to mitigate risk and reduce vulnerabilities resulting from hardware, software and human factors. As the use of health IT becomes more widespread, cybersecurity must be more directly integrated into the fabric of healthcare and ultimately become an organizational asset that is perceived as commonplace and mission-critical as hygiene and patient safety procedures have become to quality care. No matter how high the walls that any one organization is able to erect against cybercriminals, the healthcare industry at large must coalesce as a united front to more collectively address how to implement a universal culture of cyberdefense and train a more resilient workforce to mitigate threats.

Next Steps

Many of the topics and best practices that were discussed at the roundtables were reflected in the Cybersecurity Information Sharing Act (CISA) of 2015. In Section 405 of CISA, the law calls for the Secretary of Health and Human Services (HHS) to create a healthcare industry cybersecurity task force to assess emerging strategies, challenges and threats and to provide further recommendations. As a leading authority on health IT and an official advisor to the HHS Secretary since 1996, WEDI is uniquely qualified to leverage its multi-stakeholder coalition of member organizations in the public and private sectors and will provide ongoing support to help harmonize standards and develop best practices in cybersecurity.

ACKNOWLEDGEMENTS

On behalf of WEDI, we would like to acknowledge and thank the all of the individuals who participated in the roundtables and contributed to the development of this paper.