Business Horizons (2019) 62, 539—548

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

Muddling through cybersecurity: Insights from the U.S. healthcare industry

Chon Abraham [a], Dave Chatterjee [b,*], Ronald R. Sims [a]

[a] *Raymond A. Mason School of Business, College of William & Mary, Alan B. Miller Hall, 101 Ukrop Way, Williamsburg, VA 23185, U.S.A.*
[b] *Terry College of Business, The University of Georgia, C423 Benson Hall, Athens, GA 30602-6114, U.S.A.*

KEYWORDS
Cybersecurity;
Healthcare information technology;
Cyber resilience;
Cyberattacks;
Cybersecurity risk management

Abstract The U.S. healthcare sector is inadequately prepared to deal with the reality of cyber threats. The increasing use of smart medical equipment and mobile devices is making healthcare organizations more susceptible to ransomware and other types of malware. The size and complexity of operations, coupled with the presence of numerous legacy and incompatible systems, make it difficult to implement effective cybersecurity measures. The daunting nature of the problem often results in an if-it-ain't-broke-don't-fix-it stance among senior healthcare leaders. The preponderance of healthcare-related laws, compliance regulations, and security guidance frameworks serve to complicate the cybersecurity challenge further and too often results in senior leadership assuming a state of blissful ignorance. This study sheds light on the key factors contributing to the chaotic state of affairs and presents a roadmap to a more deliberate and proactive approach to cybersecurity risk management.

> *"Proactive planning, defining our risk tolerance, and then managing risk according to that tolerance will decrease the angst around cybersecurity, which is the smarter approach to take, compared to how most organizations are just muddling through today."*
> —Senior board member of a large U.S. health network

1. Is muddling through an acceptable approach to cyber risk management?

Muddling through is a dangerous approach to cybersecurity risk management. Yet, many organizations fall into this chaotic trap for reasons ranging from a lack of top management priority and commitment to organizational size and complexity, presence of numerous and incompatible legacy systems, inadequate budget, and more (Cram, Proudfoot, & D'Arcy, 2017; Kaminski, Rezek, Richter, & Sorel, 2017; Sweeney, 2016).

* Corresponding author
E-mail addresses: chon.abraham@mason.wm.edu (C. Abraham), dchatte@uga.edu (D. Chatterjee), ron.sims@mason.wm.edu (R.R. Sims)

https://doi.org/10.1016/j.bushor.2019.03.010
0007-6813/© 2019 Kelley School of Business, Indiana University. Published by Elsevier Inc. All rights reserved.

There is enough evidence to suggest that U.S. healthcare organizations lack a deliberate, organized, and comprehensive cyber-resilience strategy. To quote a recent survey report: “One-third of hospital executives have purchased cybersecurity solutions blindly without much vision or discernment” (Leventhal, 2018). Investments in establishing cyber resilience severely lag behind other regulated industries. Not only are cybersecurity budgets low and being cut but also many firms have neither a formal security program nor a dedicated leader assigned to security (Donovan, 2018a; Leventhal, 2018; Lord, 2018). Size and complexity of operations are some of the other factors contributing to an ineffective approach to cybersecurity risk management. The following quote reflects this unfortunate state of affairs:

> Healthcare rivals the public sector in our mission and complexity. Both industries tend to be too trusting that everyone (internal employees and information exchange partners) is doing their due diligence regarding cybersecurity. But the sectors are just too large to know for sure. We don’t truly understand our own risks until it’s made plain to us by the hackers.
> —Senior Executive Services (SES) in public health and cyber operations

Criminal cyberattacks on healthcare organizations have increased by 125% during the last 5 years. A hospital in Los Angeles paid a $17,000 Bitcoin ransom to a hacker that seized control of its systems (Kaminski et al., 2017). It is not uncommon for patients to receive bills for medical procedures they have not undergone. A particular victim’s stolen credentials were used to buy a mobility scooter and several pieces of medical equipment worth tens of thousands of dollars. Information security breaches cost healthcare companies close to $400 per lost or stolen record compared to costs of $215 and $165 faced by banks and retail organizations, respectively (Symantec, 2017).

Ransomware attacks, such as WannaCry and NotPetya, have awakened corporate boards and executive leadership to the need for a more deliberate and comprehensive approach to cybersecurity risk management (Kitchen & Reiss, 2018). Considering the many challenges and hurdles that must be overcome when transitioning to a cyber-reliable state, it is easier said than done.

The purpose of this study is to develop a deeper understanding of the cybersecurity challenges in the healthcare sector and offer a roadmap to a more deliberate and proactive approach to information security risk management and resilience. It also provides generalizable insights that are likely to benefit all industries. Data were gathered from 47 interviews with professionals and experts who serve in the healthcare industry in various capacities, from senior-level business and technology leaders to security consultants. The research methodology is reviewed briefly in the Appendix.

2. What is causing the ‘muddling through’ approach?

Many healthcare organizations are underprepared to deal with the reality of cyber threats. The overwhelming nature of the problem causes senior healthcare leadership to look the other way and adopt an if-it-ain’t-broke-don’t-fix-it stance. Some of the key contributing factors are discussed in Sections 2.1.—2.6.

2.1. The vast and vulnerable attack surface

The growing use of Internet of Things (IoT) devices in the healthcare sector is significantly increasing the potential attack surface for hackers. These devices are used for a variety of purposes, including the remote monitoring of patients, tracking hospital bed occupancy, alerting hospital staff members about device malfunction, the timely and proper administration of medication, health education, and preventive care (Matthews, 2018). They are connected to health organization networks and a plethora of data sources, such as electronic medical records (EMR) and health information systems (HIS).

Compared to regular computers, IoT devices tend to have weaker security protections and not all devices are easily patched or updatable. When these medical IoT devices are left unpatched, the entire network is exposed and becomes extremely vulnerable to potential attacks. To exacerbate matters further, IoT vendors are notorious for implementing poor security measures, such as weak encryption protocols that barely meet compliance standards (Lord, 2018). As a result, these devices are easy and attractive targets for hackers. The following quote from the chief information security officer (CISO) of a large healthcare system captures the reality of an unwieldy and vulnerable healthcare network:

> The healthcare landscape is a honey pot for hackers as an unbound enterprise sharing electronic personal health information across devices in multiple locations . . . this digital transformation with EMRs may be more productive but it opens us up to more vulnerabilities.

> Also, every open port allowing data to be transmitted from our network across the web—whether it be an infusion pump; a heart monitor; a patient-engagement app, like View from the EMR; or the vendor-monitored HVAC system across all facilities—increases our chances of being breached.
> —CISO of a large healthcare system

Criminals break into these IoT devices to launch distributed denial-of-service (DDoS) attacks, eavesdrop on network traffic, and steal passwords and confidential data. Not surprisingly, in a recent report, the National Institute of Standards and Technology (NIST) warned about the IoT-related vulnerabilities and encouraged healthcare organizations to take steps to enhance device and data security. The Federal Bureau of Investigation (FBI) advises organizations to look for indicators of compromised devices, such as a major spike in internet use or the devices running slowly (Donovan, 2018b).

The growing use of mobile devices to deliver healthcare has also increased the attack surface. The human element continues to be the weakest security link in any organization; healthcare firms are no exception. A review of the largest healthcare data breaches found that hackers were able to exploit human vulnerabilities to compromise systems and access data (Lord, 2018; Winnefeld et al., 2015).

A significant percentage of Electronic Medical Records (EMR) systems are cloud-based and this further enhances the attack surface and creates additional security challenges. Despite the necessary due diligence and vetting, it is difficult for healthcare organizations to ensure that third-party service providers will take necessary precautions to secure the data.

2.2. A plethora of security guidance frameworks

There are numerous security governance frameworks with overlapping goals and recommendations. While some of them—such as NIST, ISO, and SABSA—are focused primarily on effective management of information security, others have more overarching goals of guiding every aspect of information technology management. Which framework to adopt or not to adopt and to what extent is often the cause of much confusion and dilemma.

Despite a recent increase in the adoption of security frameworks, the healthcare industry is found predominantly to use frameworks and tools that are not risk-based (Lord, 2018). One respondent spoke to this concern:

> If you don't have a risk-based security framework (like NIST's CSF) in place to identify all your cyber risks and prioritize them for remediation, do that now! You can't just look at the security risk; you must also look at the risk to the business. Ransomware doesn't shut down IT; it shuts down patient care. That is the business of healthcare.
> —Senior Business and Technology Leader of a primary care innovation center

2.3. Numerous laws and compliance obligations

U.S. cybersecurity-related laws and regulations include the Cyber Disclosure Act of 2015, the Omnibus Rule, the 1999 Gramm-Leach-Bliley Act, the 2002 Homeland Security Act, and the Health Insurance Portability and Accountability (HIPAA) Act of 1996. These regulations are often ambiguous in laying down information security expectations and mechanisms. For instance, HIPAA (based on the NIST guidance) currently does not require a gold standard certification or anything beyond requiring organizations to comply with a list of security controls. Only health entities that are considered part of the federal government are mandated to apply HIPAA guidance, while others are more at liberty to adopt controls that may or may not match a particular cybersecurity framework.

There is no cybersecurity certification process mandated by law in the healthcare sector that would trigger industry-wide compliance. While NIST is supposed to promote industry-wide compliance in government, the complexity in its implementation exhausts organizational resources just in achieving 'secure enough' compliance. Experienced professionals know that secure enough is not secure, as evidenced by continued breaches of government bodies such as the Office of Personnel Management and the National Security Agency. Even staying abreast of these national laws and regulations can be quite challenging, as one senior compliance officer stated:

> Compliance navigation is a nightmare and exhausting so this is where organizations tend to stop, but it's only the baseline for beginning. Ascribing to a framework like NIST for compliance standards is complex. We need auto-generated tools or pick and choose components of less onerous frameworks to help make the process easier. This has driven a culture of compliance, only not fostering proactive cybersecurity risk management. Compliance alone does not guarantee you are impenetrable or

> more importantly resilient. Compliance means we've checked the box, which can breed complacency.
> —Senior Executive Services Compliance Officer for a large government organization

Furthermore, these laws and regulations are often misguided and thereby do not serve the intended purpose. One interviewee noted:

> The breach laws or requirements under HIPAA seem to incentivize the wrong approach. You only have to report when 500 or more patients are affected by a data breach of private health information, [but even] if it's just one patient then it's still a breach. We get fined and there is less emphasis on how the breach gets remediated. We need CERT teams like the government . . . or cyber protection teams to be deployed and do some forensics to help identify what happened and institute fixes. DHHS should help supply that.
> —Corporate Compliance Officer of a large health organization

2.4. Lack of an effective and mature information technology (IT) function

A lack of maturity and effectiveness of the IT function is evident when healthcare organizations fail to maintain a current inventory of sensitive and valuable data and where those data reside. There is also a lack of awareness of which ports are open on the network. Accounts that should have been terminated—for example, when an employee or vendor is no longer associated with the company—are still in existence. Such organizations are not organized to monitor and track network traffic in their own IT environment, let alone know how secure the networks of the information exchange partners is. Proactive measures such as penetration testing and advanced encryption and obfuscation techniques are not systematically used to mitigate security risks.

A capability-rich and mature IT organization can be a significant strength as firms strive to become *cyber resilient*: able to prevent attacks, proactively prevent an attack, and quickly recover from an attack. The IT function can play a significant role in determining and implementing the different forms of preventative, detective, and recovery-control measures.

Building an effective technology and security infrastructure takes time and resources. Unfortunately, in the healthcare sector, information technology and security have not been a priority. The technology budget has declined from a high of 3.1% in 2014 to 2.8% of gross revenue in 2018 (Kass & Bazzoli, 2017). The average spend on cybersecurity is around 3% of total annual IT spend (Donovan, 2018a).

Cybersecurity budgets are low and being cut, and many firms have neither a formal security program nor a dedicated leader assigned to security. In several hospitals and large healthcare systems, CISOs are lower in the reporting chain than desirable and only 4% of the organizations have steering committees in place to evaluate cybersecurity investments. Decisions about cybersecurity spending are being made at the C-level without consulting users (Donovan, 2018a; Leventhal, 2018; Lord, 2018).

2.5. Lack of senior management awareness of cybersecurity risk tolerance level

The consequences of a cyberattack can be far reaching, from disruption of operations to loss of sensitive data, lawsuits, regulatory inquiries and penalties, loss of reputation, bankruptcy, and business closure. Thus, being fully cognizant of the operational and strategic impacts of cybersecurity risk is key to a deliberate and thorough approach to cyber resilience preparedness. Senior management must be engaged in this activity of immense strategic significance (Rothrock, Kaplan, & Van der Oord, 2017).

Unfortunately, that is not the case with many of the healthcare organizations in which information security is an afterthought, with minimal resources devoted to combat and thwart different forms of attacks. Such organizations have little or no awareness of their risk tolerance levels, operating in a state of ignorance that can turn to fear once vulnerabilities are laid bare by attacks (Donovan, 2018b; Lord, 2018).

2.6. Lack of senior management awareness of cybersecurity threats and defense mechanisms

For cybersecurity governance to be truly effective, top management needs to be very hands-on, from making every effort to learn about the organization's vulnerability points and defense mechanisms to participating in security-review discussions and proactively engaging with and serving on different security governance committees. One survey revealed that only 40% of C-level executives have an in-depth understanding of cybersecurity protocols (Sweeney, 2016). This finding is consistent with anecdotal evidence and other research reports that suggest top management is not taking the lead, ownership, or responsibility in ensuring strong cybersecurity governance (Visner, 2016).

Studies have found significant variance in the extent and level of senior management awareness of cybersecurity and threats. For instance, an HIMSS Analytics study found interactions between the CISO and the senior leadership of healthcare organizations were very infrequent. The study also found a small resource commitment (0%—3% of the total IT budget) toward information security management. This lack of resource commitment indicates a failure of senior healthcare management to appreciate the risks and potential consequences of cyberattacks. Organizations in which such top management mindset prevails are bound to flounder when it comes to cybersecurity preparedness (Rothrock et al., 2017).

The CFOs we interviewed indicated that investments in cybersecurity are increasing in the wake of recent attacks, but not particularly with a deliberate strategy. Investments are often blind or made out of fear, lacking data-driven decision making (Rothrock et al., 2017).

3. Cybersecurity risk management roadmap

Managing cybersecurity risk is a balancing act between security and resilience. A firm can never be completely secure but can develop the capability to recover quickly from an attack. The roadmap depicted in Figure 1 is anchored on this balancing act and presents a systematic and holistic approach to understanding, valuing, and mitigating cybersecurity risks.

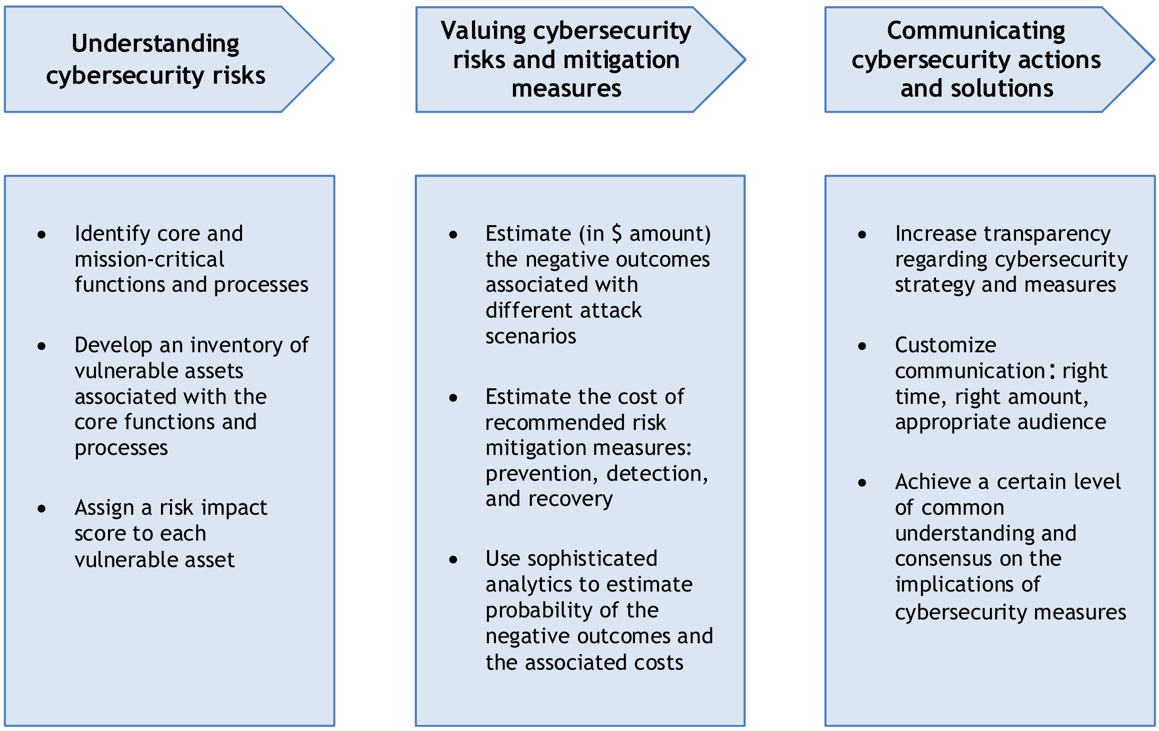
3.1. Understanding cybersecurity risk

Whether treating patients or securing patient data, healthcare organizations must recognize their risk tolerance levels. For instance, treating ER patients within 90 minutes of admission and critically ill patients within 10 minutes could be the risk tolerance levels set for healthcare activities. Similarly, cybersecurity risk tolerance levels could be set along the lines of zero tolerance for nonreporting of breach incidents, shutting down the network within 5 minutes of becoming aware of the attack and reverting to failover procedures, and dispatching forensic analysts within 5 hours to discern the type and severity of the loss.

It is imperative that risk appetites and tolerance levels are determined and defined as part of the cybersecurity strategic planning process. These assessments reflect clarity of purpose and pave the way for a thoughtful and deliberate method of securing the enterprise effectively.

The first step in understanding cybersecurity risk entails profiling the core business functions, identifying all processes and operational units that are

Figure 1. Cybersecurity risk management roadmap



Understanding cybersecurity risks

- Identify core and mission-critical functions and processes
- Develop an inventory of vulnerable assets associated with the core functions and processes
- Assign a risk impact score to each vulnerable asset

Valuing cybersecurity risks and mitigation measures

- Estimate (in $ amount) the negative outcomes associated with different attack scenarios
- Estimate the cost of recommended risk mitigation measures: prevention, detection, and recovery
- Use sophisticated analytics to estimate probability of the negative outcomes and the associated costs

Communicating cybersecurity actions and solutions

- Increase transparency regarding cybersecurity strategy and measures
- Customize communication: right time, right amount, appropriate audience
- Achieve a certain level of common understanding and consensus on the implications of cybersecurity measures

mission-critical. The next step involves developing an inventory of vulnerable assets for the core processes/functions and locating the personnel responsible for these assets. The third and final step entails assigning a risk impact score to each vulnerable asset/process based on the severity of threat impact. Attaining this risk impact score can be challenging but realistically needs to be based on what the organization deems the most to least critical data sources, systems, and processes to safeguard.

3.2. Valuing cybersecurity risk and mitigation measures

At a generic and high level, valuing cybersecurity risk involves estimating the negative cost associated with different attack and breach scenarios. From a healthcare organization's standpoint, cyber risk valuation must take into consideration negative consequences such as ransomware payment; sending patients/customers to alternative sites for care services; reputation damage; government penalties and sanctions; and the costs of recovering data, replacing equipment, and implementing additional security measures. The assessment must also factor in the cost of investing in various preventive, detective, and recovery mitigation measures such as:

- Having reliable and frequent backups;
- Customized cybersecurity training for all organizational levels and roles;
- Thorough vetting of cloud service providers (e.g., the extent to which their services are in compliance with auditing standards such as SAS 70 and FIPS 200);
- Implementing strong endpoint protection solutions to thwart attacks from insider threats or external hacking;
- Continuous monitoring of networks and systems by internal IT staff or by managed security service providers;
- Maintaining a highly trained and experienced incident response team;
- Implementing high-end encryption software for protecting data at rest and in transit; and
- Deploying artificial intelligence-enabled automated systems that proactively detect and thwart attacks on networks and devices.

Such estimation will entail the use of sophisticated and advanced analytics to determine the probability of the different types of risks and the costs of recommended mitigation action plans.

3.3. Communicating cybersecurity actions and solutions

Effective communication is centric to any implementation success, including cybersecurity preparedness. Whether to make top management aware of the seriousness of the threats and resources needed to combat them or inform the relevant user community why a certain control (such as dual-factor authentication) should be in place despite the apparent inconveniences, communication must be clear, candid, and customized.

Without such awareness and understanding, it will be difficult to mobilize organization-wide support to create and sustain a proactive cybersecurity culture. A certain level of common understanding and consensus is essential to achieve the desired buy-in (Iveroth, 2010). One cybersecurity consultant spoke of the need for salient communication at each organizational level:

> The board wants to know the cost of keeping the organization from being the next Target (literally). Middle managers or operational leads want to know how they can effectively keep working without impediment from tighter cybersecurity measures like two-factor authentication, which takes time away from the process of care. Technical leads want to know what controls and how to implement controls to inflict less pain but ensure protection for the organization. This entails communicating different messages at each level of the organization.
> —Cybersecurity consultant

4. What are some generalizable insights?

While this research has focused on how U.S. health sector organizations understand and manage cybersecurity risk, the insights gained from expert interviews are applicable to other industries.

4.1. Business and technology leaders must partner up

Securing sensitive data, mission-critical applications, systems, and the overall network is not just a technology or security matter; rather, it is a business challenge of strategic significance. The negative consequences of information security breaches can be severe and threaten the very existence of the business. Therefore, it is imperative that senior management actively partner with technology and security personnel regarding information security governance planning, implementation, and monitoring activities (Dang-Pham et al., 2016; Manworren et al., 2016; Sweeney, 2016; Visner, 2016). It is only through a hands-on approach that top management will have a good feel for organizational vulnerabilities and how best to address them. As one expert opined: "engage business and clinical leaders in information governance and in implementing security practices. Security and IT can't do it alone."

4.2. Do not leave suppliers and other value chain partners behind

The collaborative approach to dealing with cybersecurity matters should not stop at the organizational level. All value chain partners—from customers to suppliers, shippers, and technology service providers—must be engaged and informed. After all, the cybersecurity chain is only as strong as its weakest link (Lord, 2018). Organizations must ensure primary, secondary, and tertiary third-party vendors that provide devices and/or services or that have access to the infrastructure are involved in comprehensive risk evaluation and mitigation plans. While this extensive collaboration and engagement model might be difficult to implement, it is good practice from the standpoint of enhancing cybersecurity preparedness.

4.3. Adopt a proactive and holistic approach to cybersecurity readiness

While it is impossible to ensure foolproof security and a zero-incident guarantee, organizations can ill afford to look the other way. Too much is at stake, and every organization must adopt a proactive and holistic cybersecurity posture that seeks to strike a balance between security and resilience by investing in preventive, detective, and recovery measures. The overall goal is to do the very best to avoid a security breach, but at the same time be prepared to quickly and effectively recover from an incident.

4.4. A layered approach to cybersecurity

A layered approach to security is a commonly espoused recommendation from experts, and this point of view was reinforced by the primary and secondary data gathered for this study. It is essentially about securing the data, the network on which data travels, the devices on which data is stored, and the location(s) in which data resides. Using a combination of software, hardware, and administrative controls, organizations should secure sensitive data and systems. The term *defense in depth* is often used to describe this layered defense mechanism.

According to one expert, the layered approach would include: (1) installing a robust antivirus and antimalware program on all computers and servers, (2) having a cloud-based service provider scan website and email traffic before it can enter the organization's network, and (3) train personnel to recognize different types of threats and how to deal with them (Donovan, 2018b).

4.5. Have a well-tested backup and recovery plan

An organization must always be prepared for the worst and have a robust backup and recovery plan if/when it is a victim of an attack. The plan should include clearly laid out and documented roles and responsibilities for personnel to take action in the event of different attack scenarios. The organization should also have one or two safe sites at different locations. These sites provide the firm the luxury and flexibility of being up and running while main site—that is, the subject of the attack—is switched off for investigation. Data must be backed up to servers located at these sites as often as is feasible.

4.6. Broaden the skillset of decision makers: Strategize like a hacker

Organizations actively hire consultants to perform attacks on the network to expose vulnerabilities (i.e., penetration tests). Healthcare organizations utilize hackathon challenges to aid their security operation personnel in identifying vulnerabilities. As a one-time penetration test this is an effective tactic, but the logic also serves the organization well if applied at the strategic level: recruit team members who think like a hacker or, better yet, hire ethical hacker strategists and not just ethical hacker technologist to better understand the business strategy perspective. Akin to red teaming in business intelligence and other formal intelligence analysis methods, these hacker strategists can form task forces and collaborate with operational managers as needed to think through cyber implications of different business scenarios.

4.7. Move toward a data-driven approach to cybersecurity management

A data-driven approach is key to the development and sustainability of a robust cybersecurity governance program. Whether determining the threshold for reporting potential threats to senior management, quantifying the risks associated with different threat scenarios, deciding the amount of cyber insurance to carry, or estimating the implementation costs of security measures, organizations need to find ways of gathering quality data and running sophisticated analyses.

CIOs and CISOs can also benefit from data-driven insights when developing situational awareness of the enterprise, deciding on training programs, establishing structural mechanisms to facilitate cyber defenders and engineers working together, monitoring and defending systems and networks, pitching for cybersecurity investments, and assessing the effectiveness of existing cybersecurity programs (Hooper & McKissack, 2016). In essence, quantify as much as possible to remove subjectivity from prioritization of cybersecurity initiatives, investments, or actions.

4.8. Have an internal and external cybersecurity risk communication plan

Whether convincing top management to invest in certain cybersecurity initiatives, making organizational members at all levels aware of various threat scenarios and how to respond to them, or gaining trust of the user community by providing greater transparency of security plans and measures, effective communication can go a long way toward creating and sustaining a supportive security culture.

One CISO shared her don't-cry-wolf communication approach with her C-level peers. She is always very realistic and pragmatic in her evaluation and assessment of potential cybersecurity risk scenarios and never oversells the need to take immediate action or spend a certain amount of time. Over the years, this conservative approach has earned her the respect and trust of her peers and they are ready to back her up when needed.

Another CIO facilitated a board-level learning workshop by recruiting board members to serve as problem ambassadors and raise awareness of a certain breach incident at a competing organization. Participants discussed the scenario and reflected on how the organization would protect itself from such an attack or quickly recover from it. It is also imperative that organizations follow regulatory guidelines and are candid and honest in their external communications with victims of cyberattacks and the media.

5. Summary

Cybersecurity is a global phenomenon that is here to stay. No organization can ever be fully secure or immune from every type of cyberattack. Healthcare's rapidly expanding attack surfaces, coupled with the highly sensitive and valuable nature of its data, makes the field particularly vulnerable and appealing to hackers. The consequences of such attacks go far beyond financial impacts or operational disruption; quality of care can be affected and patients can die. Any medical device that is connected to a network can be hacked, from MRI machines to heart defibrillators and electric wheelchairs. The implanted heart defibrillator of a prominent public figure had to be suitably modified to prevent 'death by hacking' (Morris, 2018). Therefore, healthcare organizations have a responsibility to leave no stone unturned and to take a proactive and holistic approach to cybersecurity preparedness.

A comprehensive and robust information security plan entails investing in preventive, detective, and recovery measures. A combination of physical, technological, and administrative controls must be used to shore up data, devices, the network, and storage areas. A cybersecurity chain is only as strong as its weakest link. Considering that humans are most susceptible and vulnerable to attacks in any industry, including healthcare, an organization must raise the level of awareness and competency of all its members through regular and effective training programs.

Finally, senior management must be actively engaged in all aspects of cyber governance, from planning to implementation. They must treat cybersecurity investments as strategic investments and closely guide the development of this unique and distinctive competency.

Appendix. Methods

This qualitative study draws upon grounded theory to interpret the interview data. The Straussian version of grounded theory is used, as it encourages the researchers to take into consideration the literature as well as their professional and personal experiences when reflecting on the collected data. A total of 45 in-depth interviews were conducted

Table 1. List of study participants

Representative Official Titles	Representative Organizations
• Board Member	• Cybersecurity Consulting Firms focusing on Health Sector
• Chief Compliance Officer	• Department of Health and Human Services
• Chief Data Privacy Officer	• Department of Veteran Health Administration
• Chief Financial Officer	• Federal Bureau of Investigations
• Chief Information Officer	• Large Health System in the Southeast
• Chief Information Security Officer	• Medium Health System in the Northeast
• Chief Marketing Officer	• Small Health System in the Northwest
• Director of Compliance and Risk Management	
• Director of Risk Management	
• General Counsel	
• Security Operations Center Manager	
• Representative from National Intelligence and Cyber Infrastructure for Health Sector	
• Cybersecurity Consultants	

with professionals and experts who serve the healthcare industry in various capacities, from senior-level business and technology leaders to security consultants. A full list of participants is included in Table 1.

Most of these interviews were audio recorded and transcribed. The Atlas.ti tool was used to generate codes from analyzing the interview transcripts. Each of these codes represented a certain theme or factor relating to cybersecurity governance challenges and the recommended roadmap. We went through several reviews and iterations to ensure coding accuracy.

References

Cram, A., Proudfoot, J., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems, 26*(6), 605–641.

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2016). Impacts of security climate on employees' sharing of security advice and troubleshooting: Empirical networks. *Business Horizons, 59*(6), 571–584.

Donovan, F. (2018a, May 14). Healthcare data security programs get short shrift in IT budgets. *Health IT Security*. Available at https://healthitsecurity.com/news/healthcare-data-security-programs-get-short-shrift-in-it-budgets

Donovan, F. (2018b, October 1). NIST warns about cybersecurity vulnerabilities in healthcare IoT. *Health IT Security*. Available at https://healthitsecurity.com/news/nist-warns-about-cybersecurity-vulnerabilities-in-healthcare-iot

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons, 59*(6), 585–591.

Iveroth, E. (2010). Inside Ericsson: A framework for the practice of leading global IT-enabled change. *California Management Review, 53*(1), 136–153.

Kaminski, P., Rezek, C., Richter, W., & Sorel, M. (2017). Protecting your critical digital assets: Not all systems and data are created equal. In *McKinsey & Company*. Available at https://www.mckinsey.com/business-functions/risk/our-insights/protecting-your-critical-digital-assets-not-all-systems-and-data-are-created-equal

Kass, E. M., & Bazzoli, F. (2017, December 27). 2018 tech budget to rise about 8.8% for healthcare organizations. *Health Data Management*. Available at https://www.healthdatamanagement.com/news/2018-tech-budgets-to-rise-about-88-for-healthcare-organizations

Kitchen, K., & Reiss, M. (2018, May 7). Ransomware is coming; It'll make you wannacry. *Weekly Standard*. Available at https://www.weeklystandard.com/klon-kitchen/ransomware-like-wannacry-notpetya-and-samsam-threatens-global-finances-and-security

Leventhal, R. (2018, May 16). Cyber attacks increase as IT security budgeting remains static, report finds. *Healthcare Innovation*. Available at https://www.hcinnovationgroup.com/cybersecurity/news/13030218/cyber-attacks-increase-as-it-security-budgeting-remains-static-report-finds

Lord, N. (2018, June 25). Information security: The top INFOSEC considerations for healthcare organizations today. *Digital Guardian*. Available at https://digitalguardian.

com/blog/healthcare-information-security-top-infosec-considerations-healthcare-organizations-today

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons, 59*(3), 257—266.

Matthews, K. (2018, May 3). Exciting IoT use cases in healthcare. *IoT for all*. Available at https://www.iotforall.com/exciting-iot-use-cases-in-healthcare/

Morris, E. (2018, March 4). Can cyberattacks cause human fatalities? *The Doctor Weighs In*. Available at https://thedoctorweighsin.com/can-cyberattacks-cause-human-fatalities/

Rothrock, R. A., Kaplan, J., & Van der Oord, E. (2017, November 16). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*. Available at https://sloanreview.mit.edu/article/the-boards-role-in-managing-cybersecurity-risks/

Sweeney, B. (2016, September 13). Cybersecurity is every executive's job. *Harvard Business Review*. Available at https://hbr.org/2016/09/cybersecurity-is-every-executives-job

Symantec. (2017). *Addressing healthcare cybersecurity strategically* [White Paper]. Mountain View, CA: Symantec.

Visner, C. (2016, November 15). Cybersecurity is everyone's responsibility — And it starts at the top. *CSO*. Available at https://www.csoonline.com/article/3140924/security/cybersecurity-is-everyones-responsibility-and-it-starts-at-the-top.html

Winnefeld, J. A., Jr., Kirchoff, C., & Upton, D. M. (2015). Cybersecurity's human factor: Lessons from the Pentagon. *Harvard Business Review, 93*(9), 87—96.