Case: Cyber Hygiene in Health Systems: Turning (Supply Chain) Cybersecurity into a Corporate Capability

“We’ve got the right skills and capabilities. We have relevant tools and techniques informed by sound philosophical principles — and just as importantly, reflecting the engagement of frontline team members. We’re already seeing direct, outcome-based evidence of success across the supply chain, and we expect that to continue over the next fiscal year.”

– Dean Gunther, Chief Supply Chain Officer, Mountainwest Health System

Overview of the United States Healthcare System

Health services in the United States (U.S.) are provided by a loosely structured delivery system organized at the local level [1]. There is no health planning at the Federal level, and State planning efforts vary from minor to stringent reviews of hospitals and other health care
delivery organizations [1]. Also, physicians are free to establish their practice(s) where they choose, and hospitals can open or close according to community resources, preferences, and the dictates of an open market for hospital services [1]. Municipal and county public health departments provide limited primary care services through public health clinics and regulate sanitation, water supply, and environmental hazards.

The U.S. spends more on health care services than does any other nation, but the U.S. does not achieve better health outcomes [1-3]. The U.S. spends more on a general practitioners, pharmaceuticals, and healthcare administration [2]. More specifically, the U.S. spends 8 percent of its total national health expenditures on activities related to planning, regulating, and managing health systems and services, compared to an average 3 percent spent among all high-income countries [2]. From a service offering and utilization perspective, experts argue that the U.S. has similar levels of spending for social services (including both public and private spending) and similar use of health care services [2]. So, these two areas are not believed to be major causes of the spending gap [2, 3]. In light of this, some researchers argue that the U.S. should focus on lowering prices and administrative costs to control healthcare expenditures, rather than just reducing the use or availability of health care services [2, 3].

U.S. hospitals and its healthcare industry are experiencing major transformations that are expected to affect the costs in its health care system. One such example is a federal regulation known as the Value-based Purchasing (VBP) program [4]. VBP is Centers for Medicare & Medicaid Services (CMS) initiative that rewards acute-care hospitals with incentive payments for the quality care provided to Medicare beneficiaries [4]. The spirit and intent of VBP is to tie a larger percentage of hospitals’ reimbursements to the value (i.e., quality and associated outcomes) of care delivered rather than the volume of patient
encounters accounted for [4]. This paradigm change from a fee-for-service model to a value-based model requires hospitals to more accurately track and document resources/assets utilized in the delivery of care, in addition to appropriate health outcomes [4].

**About Mountainwest Health System (MHS)**

Mountainwest Health System (MHS) is a USA-based, not-for-profit, healthcare system of over 20 hospitals, multiple large physician groups and practices, and nearly 200 clinics. As such, MHS is made-up of 2,400 physicians and specialists and nearly 40,000 employees. MHS serves a large geographical area and diverse population, with each population requiring varying levels of healthcare. MHS’s aim is to improve healthcare quality, safety and patient experience with a large focus on new innovation and growth to improve healthcare.

The MHS medical group, made up of all its clinicians, focuses on personalized primary care and patient identification and safety. Personalized care to MHS means a collaborative approach with patients and clinicians to share decision-making and actively engage patients in the health management and their own treatment plans. MHS is working towards a National Patient Identifier to correctly identify patients every time, which should help reduce medical error and adverse events. MHS prides itself on being community driven with over 400 community representatives serving on governing boards, helping guide MHS strategies and charitable foundations. The aim to improve community needs is a part of the MHS strategy, including their focus on the social determinants of health: examining the impact of housing, utility needs, food security, transportation, and interpersonal violence on patient’s health.

MHS has a variety of collaborations and partnerships that they use to advance healthcare technology and find innovation for some of healthcare’s larger problems. Some of
the collaborations involve business partnerships, investments in pilot projects, and strategic investments that support the advancement of health. Additionally, MHS has been known to create its own initiatives to fill gaps in the healthcare market. One such example is the “virtual hospital” initiative.

MHS partners with different healthcare systems, outpatient clinics, government, and rural hospitals to provide a virtual hospital aimed at reducing patient and increasing their access to high quality health care. Through the use of virtual care, patients are able to access specialists while staying in their local hospital, saving money as well as undue patient stress from travel.

True to its innovative spirit, MHS launched a health platform company that focuses on elevating value-based care capabilities with providers, payers, and accountable care organizations. The new venture will enable other organizations to accelerate their transition from volume to value-based systems of care, while keeping care more affordable and accessible. The platform offers a suite of tools and services to support healthcare transformation and improvement. Some of those tools and services include digital tools to address virtual care, a value-based clinical care model, analytics, and access to MHS innovations.

**MHS Supply Chain Background Overview**

MHS views its supply chain as a strategic asset and core capability. The MHS supply chain organization focuses on technological advancements and innovative solutions to help reduce costs while improving value. MHS is not conservative when it comes to leveraging existing and emerging technologies to ensure that quality products and services are sourced,
purchased, and delivered to their healthcare organizations. In addition to directly handling the procurement products, devices, and supplies directly from suppliers, MHS, similar to 97 percent of US health systems, also leverages the collective purchasing power of GPOs to negotiate savings on purchased goods and services [5].

The MHS supply chain organization has four areas of operations: (1) category management, (2) purchasing, (3) logistics and materials management, and (4) business programs and support services. Category management is responsible for ensuring sustainable procurement practices, while sourcing and contracting the best items that meet the procurement strategy. Purchasing function is responsible for executing orders for goods and services. Logistics and materials management orchestrates the movement of goods from supplier to site and oversees inventory management to ensure clinicians have access to the right products when needed. The business programs and support services function is responsible for the operational effectiveness of the MHS supply chain to ensure seamless functionality of system-wide programs.

MHS has been successful in supply chain due to its support from senior and clinical leadership and having the right people in the right place. Through hiring the right people and gaining the right support, MHS has been able to use best practices in healthcare and global supply chain to support its organization. MHS has created significant savings through supply chain practices of reducing variation and physician preference, improving specimen-handling protocols, and better clinical alignment. These changes have led to over $550 million USD over the past decade.
Cybersecurity

Generally speaking, cybersecurity is the ability to protect or defend the use of one’s interdependent network of information systems infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers from internal and external threats. Cyber hygiene, in response to cybersecurity threats, is the promotion of the commonly accepted objectives of confidentiality, integrity, and availability of information and assets and is essential to the overall safety and soundness of an institution. The consistent practice of good cyber hygiene provides layers of protection from malicious and non-malicious actions that increase the risk of adverse effects on patient trust and confidence, healthcare delivery, monitoring, and management, revenues, assets, and enterprise value and reputation.

It is important to recognize that cybersecurity is not merely one thing. Rather, it is inclusive of information security (commonly referred to as InfoSec), IT security, operational technology (OT) security, and offensive security (see Figure 1) [6]. InfoSec pertains to preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information to provide confidentiality, integrity, and availability. IT security entails implementing measures and systems designed to securely protect and safeguard information. OT consists of hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, industrial equipment, assets, processes, and events. Hence, OT security is the practices and technologies used to protect people, assets and information involved in the monitoring and/or control of physical devices, processes and events [6]. Lastly, offensive security is a proactive and adversarial approach to protecting computer systems that consists of legal countermeasures and
counterstrike actions taken against an attacker outside of friendly systems for the purpose of self-defense [7].

**Figure 1: Cybersecurity in Relation to Other Forms of Security**

Offensive security mechanisms are usually categorized as the “3 A’s”: annoyance, attribution, and attack [8]. Annoyance is frustrating the attacker's attempt through tools that establish false ports, services and directories. Once lured into the false system, the attacker ends up looping endlessly through it. This approach creates time for appropriate attribution. Attribution is where the organization under attack works to accurately identify the attacker, even while the attack is ongoing. For example, embedding a “web bug” in a document, such that if the document is accessed, the web bug sends back information about the system that accessed it. Lastly, attack is an enhancement of the annoyance and attribution capabilities, rather than a truly malicious (and illegal) assault on the attacker. Potential adverse events from cyber breaches can include the following:
• Disclosure of information;
• Operational loss;
• Fines;
• Lawsuits;
• Productivity loss;
• Misappropriation or theft of information;
• Loss of control over medical equipment and devices;
• Modification or destruction of systems or information;
• Theft of intellectual property; and
• Exploitation of medical device vulnerabilities that lead to disruption of functionality or patient harm [9].

In aggregate, the effects of a cyber incident or disruption leads to loss of stakeholder trust in MHS.

The frequency of cyberattacks are increasing at a fast pace. The impact of a failure in cybersecurity can result in financial and reputational damage, especially when you consider that a breach has a relatively “long tail”. That long tail suggests that the costs associated with a breach can, and likely will, be felt for years after the incident [10]. For example, the breach lifecycle\(^1\) grew noticeably between 2018 and 2019. The average breach lifecycle in 2019 was 279 days (i.e., 206 days to identify a breach and 73 days to contain it) as compared to 266 days in 2018 (4.9 percent increase) [10]. As one might imagine, speed in this case is of extreme importance for obvious reasons. What can, but shouldn’t, go unnoticed is the financial implication of how fast/slow an organization is in identifying and containing a breach. IBM

---

1 The time between when a data breach incident occurs and when it is finally contained.
Security [10] found that breaches with a lifecycle less than 200 days were on average $1.22 million USD less costly than breaches with a lifecycle of more than 200 days ($3.34 million USD vs. $4.56 million USD respectively); that is a substantial difference of 37 percent.

Organizations in a high data protection regulatory environment, such as healthcare, saw 53 percent of breach costs in the first year, 32 percent in the second year, and the remaining 16 percent occurred more than two years after a breach [10].

Similar to the rise in attacks, there has been a relatively steady increase in the cost per breach (see Figure 2) [11]. In 2019, the global average total cost of a data breach is nearly $4 million USD (see Figure 3) [10]. By comparison, the US has the highest country average total cost of a data breach at slightly over $8 million USD [10].

Figure 2: Average Cost Per Cybersecurity Breach Trends

<table>
<thead>
<tr>
<th>Year</th>
<th>Cost in millions USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>3.54</td>
</tr>
<tr>
<td>2007</td>
<td>4.79</td>
</tr>
<tr>
<td>2008</td>
<td>6.36</td>
</tr>
<tr>
<td>2009</td>
<td>6.66</td>
</tr>
<tr>
<td>2010</td>
<td>6.75</td>
</tr>
<tr>
<td>2011</td>
<td>7.24</td>
</tr>
<tr>
<td>2012</td>
<td>5.5</td>
</tr>
<tr>
<td>2013</td>
<td>5.4</td>
</tr>
<tr>
<td>2014</td>
<td>5.85</td>
</tr>
<tr>
<td>2015</td>
<td>6.53</td>
</tr>
<tr>
<td>2016</td>
<td>7.01</td>
</tr>
<tr>
<td>2017</td>
<td>7.35</td>
</tr>
</tbody>
</table>

Source: IBM [11]

---

2 Total breach costs include lost business resulting from diminished trust or confidence of those affected; costs related to detection, escalation, and notification of the breach; and ex-post response activities, such as credit report monitoring.
Malicious actors including cyber-criminals, hacktivists, Nation States, and malicious insiders are motivated by monetary gain, protest, revenge, and desire to disrupt operations. Malicious actors employ various techniques (see Figure 4) such as the exploitation of hardware and software vulnerabilities, exploitation of third-party connections, social engineering, and DDoS define attacks. KnowBe4, Inc. [12] reports that executives find data breaches and user credential compromise as the most concerning attack vectors (see Figure 4). As it pertains specifically to medical devices (see Figure 5), the most common attack vector is exploit-kit, which targets specific vulnerabilities/OS accounts [13].
These aren’t isolated cases. According to a Ponemon Institute cyber risk report [14], 56 percent of organizations have had a breach that was caused by one of their vendors.
Meanwhile, the average number of third parties with access to sensitive information at each organization has increased from 378 to 471. That number might be a little low, especially since only 35 percent of companies had a list of all the third parties with whom they were sharing sensitive information [14]. Forty-one percent said they had third party-related incidents in the past 24 months [14]. Further, misuse or unauthorized sharing of confidential data by third parties was the second biggest security worry for 2019 among IT professionals with 64 percent of the tally [14]. For these reasons, companies are paying more attention to third-party risk.

**Cybersecurity in Healthcare**

The Health Insurance Portability and Accountability Act (HIPAA) is the primary governing regulation for the protection of patient information. HIPAA underscores the fact that cybersecurity is not simply an IT issue, rather it is an organizational and health sector issue [9]. Additionally, the U.S. Food & Drug Administration (FDA), the U.S. Department of Health and Human Services (HHS), and HHS Centers for Medicare and Medicaid Services (CMS) are increasing requirements for healthcare organizations and their suppliers to improve cybersecurity [9].

According the Identity Theft Resource Center (ITRC), healthcare had the second largest amount of data breaches in 2018, but the highest rate of exposure per breach [15]. Further, Verizon’s 2018 Protected Health Information Data Breach Report cites healthcare as the only industry in which internal actors are the biggest threat to an organization [16]. In fact, the study found that 58 percent of the nearly 1,400 healthcare incidents analyzed in involved insiders [16]. From a cost standpoint, healthcare has the highest industry average total cost of
a data breach at $6.45 million USD (see Figure 6) [10]. This point is not an isolated occurrence. In fact, healthcare reportedly has been atop the list for nine consecutive years [10].

**Figure 6: Average Total Cost of a Data Breach by Industry**

Measured in USD millions

<table>
<thead>
<tr>
<th>Industry</th>
<th>Cost (USD millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health</td>
<td>$6.45</td>
</tr>
<tr>
<td>Financial</td>
<td>$5.86</td>
</tr>
<tr>
<td>Energy</td>
<td>$5.60</td>
</tr>
<tr>
<td>Industrial</td>
<td>$5.20</td>
</tr>
<tr>
<td>Pharma</td>
<td>$5.20</td>
</tr>
<tr>
<td>Technology</td>
<td>$5.05</td>
</tr>
<tr>
<td>Education</td>
<td>$4.77</td>
</tr>
<tr>
<td>Services</td>
<td>$4.62</td>
</tr>
<tr>
<td>Entertainment</td>
<td>$4.32</td>
</tr>
<tr>
<td>Transportation</td>
<td>$3.77</td>
</tr>
<tr>
<td>Communication</td>
<td>$3.45</td>
</tr>
<tr>
<td>Consumer</td>
<td>$2.59</td>
</tr>
<tr>
<td>Media</td>
<td>$2.24</td>
</tr>
<tr>
<td>Hospitality</td>
<td>$1.99</td>
</tr>
<tr>
<td>Retail</td>
<td>$1.84</td>
</tr>
<tr>
<td>Research</td>
<td>$1.65</td>
</tr>
<tr>
<td>Public</td>
<td>$1.29</td>
</tr>
</tbody>
</table>

Source: IBM [10]

**Why Healthcare and Why So Frequently?**

Part of what's driving the uptick in cyber breaches in healthcare is the multitude of valuable information that can be aggregated from a single breach source. Healthcare systems (both clinical and non-clinical systems) and medical devices contains or is the pathway to: (i) social security number, (ii) your name(s), (iii) the names and ages of your relatives, (iii) historical information of where you live(d), (iv) where you work(ed), (v) diagnoses, (vi) prescriptions, and (vii) financial information (e.g. credit card information, bank account numbers) [15, 16]. When you consider this potential honeypot it's no surprise that the
medical record is considered the most comprehensive record about the identity of a person that exists today [16].

Health systems around the world are negatively affected by the continued growth of ransomware attacks. Recently, three hospitals in Alabama (U.S.) and seven in Victoria (Australia) were targets of ransomware attacks that inhibited their ability to accept new patients and provide care to existing patients in their facilities [17]. In response to such pervasive issues, the U.S. Senate approved a new legislation, *DHS Cyber Hunt and Incident Response Teams Act of 2019* [18]. The legislation is aimed at helping government agencies and private-sector companies combat ransomware attacks. In fact, it calls for the creation of cyber hunt and incident response teams for the “purpose of leading Federal asset response activities and providing timely technical assistance to Federal and non-Federal entities, including across all critical infrastructure sectors, regarding actual or potential security incidents, as appropriate and upon request” [18]. In addition to restoring infrastructure hit by ransomware attacks, the incident response teams would also seek to proactively mitigate against cyber threats along with identifying cybersecurity risks, developing mitigation strategies and providing guidance to infrastructure owners. The recognized need and positive momentum spurring the legislation lends some credence to the belief that some of the contribute to health systems being top victim organizations has to do with ineffective disaster recovery and business continuity programs.

**Cybersecurity and the Supply Chain**

“The supply chain in the healthcare industry is a complex ecosystem of interdependent organizations of all sizes, spanning patient care, payment and data management systems,
pharmaceutical and technology research and manufacturing, and public health administration” [9, p. 4]. From a supply chain perspective, approximately 75% of supplies that come into a health system in the US are purchased on group purchasing organization (GPO) initiated contracts [19]. This dynamic creates a vital intermediary between buyer and supplier organizations. According to MHS security analysts, Eleanor Rathbone and Sam Johnson, some of the challenges facing many health systems could be attributed to too much reliance (whether implicit or explicit) on implementation/system integration partners to help gather product, system, or device information from the manufacturer or service provider that could potentially serve as security vulnerabilities.

As supply chain attacks continue to surge, an alternative method of attack is to “island hop”. Island hopping is when hackers use a business partner or other vendor to infect a primary organization. The interdependencies between various healthcare and supply chain stakeholders mean that a cybersecurity event in one organization is likely to have ripple-effects on multiple other links within the supply chain [9]. Hackers continue to take advantage of new vulnerabilities and native operating system tools to proliferate across a victim organizations’ networks [13, 20]. In fact, reportedly 70 percent of all attacks involve attempts to laterally move across the network; this concept is referred to as lateral movement [21].

Yet another supply chain tactic used by attackers is to incorporate a compromised component into a legitimate application or update package, which then is distributed to the users via the software [22]. These attacks can be very difficult to detect because they take advantage of the trust that users have in their software vendors [21, 22]. Supply chain attacks can affect the integrity and security of goods and services that organizations provide by way of the “poisoned” software and undermining delivery or update infrastructures [22].
MHS and Cyber Hygiene

Given its desire to reduce geographic and economic barriers to high quality healthcare, MHS embodies and entrepreneurial spirit and is viewed as an innovator. For example, MHS continues to innovate in medical science and health information technology (HIT). Despite the desire and need to continually innovate and push the envelope of what’s possible, MHS is well aware that the frontier of connected health is riddled with cyber landmines. As a result of island hopping and lateral movement by attackers, vulnerabilities that nonclinical applications and non-medical devices, procured by the supply chain function, can create are also of grave importance. For instance, operational technology (e.g., HVAC systems, hand hygiene monitoring systems, aquariums, building automation systems) doesn't have direct implications for service delivery, but at the same time could very well create a potential vulnerability [23-25]. Points of vulnerability have the potential to manifest as a result of cyber hygiene practices of partners or providers with access to mission critical and non-mission critical systems that may or may not be within the purview of the chief supply chain officer or chief information security officer [26]. These vulnerabilities tend to not be on the watchlist of Chief Supply Chain or Chief Security Officers in healthcare organizations, unless they are informed of the connectedness of such operational technology [26].

MHS is better than most in this area, but their security and supply chain professionals both acknowledge the importance of having good processes and tools in place to handle and mitigate risks posed by operational technology prior to them arriving at their facilities. Although MHS is used to operating from a position of strength, cyber hygiene in the health system is one area that still serves as a place for continual improvement. This sentiment is echoed by MHS’s CEO, who stated, “For those who might ask why a highly successful health
system continues to strive to be better...the answer is twofold: 1) because we can, and 2) because we must.”

**Problem Statement**

The primary objective of MHS’s cybersecurity is to protect the creation, collection, storage, use, transmission, and disposal of sensitive information, including the protection of hardware, operational technology, and medical devices and components that store and/or transmit such information. The Chief Supply Chain Officer (CSCO), Dean Gunther, along with the Chief Information Security Officer (CISO), Hicks Monroe, are well aware that MHS is in the business of saving lives. As such, the organization’s budget prioritizes staff, programs, and equipment that are directly related to that goal.

Although some in the organization may view cybersecurity as an information technology (IT) issue, Dean and Hicks are well aware that protected health information (PHI) and personally identifiable information (PII) data loss, and all of the pertinent regulations and disclosure requirements associated with it, are not solely the problem of the CISO or CIO in its organization. However, there is the tendency in healthcare organizations in general to not give cybersecurity as much of a priority on the steadily growing list of competing demands for resources. Hicks and Dean are adamant that MHS cannot afford to be one of those organizations that simply pay lip service to such a serious issue. In order to help MHS leadership understand the pervasiveness of cybersecurity, as it pertains to inhibiting achievement the organization’s overarching goals, Dean and Hicks are working to change this notion by linking supply chain activities and security goals with healthcare and health system priorities.
Dean and Hicks are creative problems solvers, who know that in order for them to win over other members of the MHS executive team, they have to work together and go beyond using the fear of internal and external threats and adversaries to make the case that cybersecurity is a business issue and not merely a supply chain or IT issue. As part of their approach they recognize the need to better educate the MHS executive team and Board about the financial, social, and medical liabilities of a cyber breach. They are in need of established effective practices to help foster better dialog about good cyber hygiene with non-security and IT professionals. They are very much open to, and would highly value, practices from other industries that appear to be as great of a target for cyber attacks as healthcare.

Another area of interest and concern for MHS is counterfeited and gray (AKA grey) market goods? Counterfeit goods refer to a non-genuine product traded with breach of brand and trademarks. Counterfeit goods are made or sold under another OEM’s brand name without that OEM’s authorization, and such goods tend to be of inferior quality. Counterfeiting is a deliberate attempt to deceive potential customers. Sometimes, the whole product is illegally manufactured, and sometimes a part of the original product is contaminated with non-genuine components. Conversations with key supply chain professionals within MHS acknowledge that lack of upstream visibility as it pertains to suppliers and prime contractors is a common issue for health systems.

Counterfeited goods are often confused with gray marketing, which is generally defined as products (very likely genuine) that are transacted through unauthorized distribution channels and/or markets. In essence, it is the purchasing of a goods through distribution channels that are legal, but unintended by the OEM. One of the more common ways in which gray market goods are introduced is when companies, which are not authorized by the OEM, sell imported products in an area or market that would otherwise be
either more expensive or unavailable in the country to which they are being imported. The challenge in combating gray market and counterfeited products is that they are sometimes found to be blended. Dean and Hicks recognize that gray market and counterfeit products could possibly be issues that can never be fully eliminated, but they agree it is vitally important that MHS identifies ways to contain the magnitude of exposure and reduce the likelihood of such products making it into MHS facilities.

**Consulting Assignment**

MHS’s executive team tasks you, as a consulting team, to advise it on the development of a cybersecurity strategy that is inclusive of its supply chain. MHS expects that your proposed strategy and implementation plan will demonstrate an understanding of emerging cybersecurity threats as they pertain to various forms of medical devices and equipment, operational technologies, as well as potential points of vulnerability as it pertains to outside partners or providers with access to mission critical and non-mission critical systems that may or may not be within the purview of the chief supply chain officer or chief information security officer. Your team’s strategy must address the growing threat of gray market and counterfeit products. Lastly, MHS is intrigued and desires to learn more about the means, and perception about a health system’s attempt, to monetize its newfound cyber hygiene capabilities.

**Case Prompt and Key Areas to Address:**

1. Develop a SWOT analysis that demonstrates an understanding of the emerging healthcare and cybersecurity landscape.
2. Recommend a value proposition for MHS to turn its cyber hygiene capabilities into a competitive advantage and deliver on the proposed value proposition.

3. What stances should MHS take or processes should it consider with respect to its desired level of cyber hygiene, particularly as it pertains to its supply chain operations, if any, to deliver on the identified value proposition?

4. If MHS were interested, whether in the short-term or long-term, how might it monetize its capabilities around cybersecurity and cyber hygiene?

5. How should MHS engage its suppliers and GPO(s) to ensure a shared risk model with respect to good cyber hygiene practices and addressing concerns around counterfeiting and gray market goods, while continuing to allow for aggressive innovation and supplier diversity?

6. How does your recommendation go beyond mere compliance with existing and impending regulations to maximize business profitability and supply chain excellence?
References


17. Goodin, D., *Ransomware forces 3 hospitals to turn away all but the most critical patients*, in Ars Technica. 2019.


