ASA Research Note

Operational Risks in Healthcare IT

Author: Elizabeth Crooks

Published: July, 2019

Written: May, 2018

Keywords: Healthcare; Public Health; Critical Infrastructure; Protected Health Information; Healthcare IT

Abstract: This paper discusses the operational risks related to information technology (IT) within the Healthcare and Public Health sector. This critical infrastructure sector's faces particularly challenging risks due to its size, its diversity of organizations, and its inherently open-to-the-public nature. The analysis examines common operational risks that face both the public and private sides of the healthcare IT subsector across all dimensions of operational risk - people, processes, systems, and external events.

The Healthcare and Public Health Sector

The U.S. Department of Homeland Security (DHS) designates the Healthcare and Public Health (HPH) sector as one of the sixteen critical infrastructure sectors, charged with protecting "all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters" and ensuring the health of the general population.[1] Managing the operational risks inherent in the HPH sector are particularly challenging due to how large it is, how diverse its mandate is, and from its inherent need to be open to the public, all of which has to happen at federal, state, local, territorial, and tribal levels.[2] Included in this sector are direct care for patients, mass fatality services, health information technology, medical materials, health plans and payers, public health, federal programs and response, and laboratories, blood and pharmacies. The Health and Human Services - as the Sector-Specific Agency for this sector - must work to manage these subsectors alongside the numerous private sector partners, which include a wide range of organizations including private insurers, medical equipment and pharmacy manufacturers, funeral homes, medical record software publishers, and other organizations involved in providing, maintaining, and governing healthcare across the country.[3]

Healthcare Sector Information Technology

One of the biggest risks facing the HPH sector overall stems from the possibility of healthcare information technology (IT) systems being compromised, resulting in the exfiltration or exposure of protected health information (PHI) and electronic health records (EHR). This risk is extremely salient as there continues to be a constant stream of very public data breach events in

the healthcare sector, including 20 breach events in March of 2018 alone.[4] Verizon's 2018 *Data Breach Investigations Report* found that the healthcare sector had the largest number of breaches across all industries studied.[5] The steady pattern of healthcare organizations being a popular target for cybersecurity attacks shows no sign of slowing down. In 2017, the healthcare sector suffered 58 percent of all cyber-attacks that year, rising from 34 percent in 2016.[6]

The management of data in the healthcare industry is both a vast and complex job: data must be immediately available for timely service delivery while the majority of data is highly sensitive (and valuable). Additionally, there are strict legal requirements and regulations surrounding the protection of personal health data (HIPAA and HITECH, among others). This risk is faced by both the public and the private sides of the healthcare and public health sector and encompasses financial risk (through identity loss at an individual level and operational disruption) as well as loss of life risk if critical services are unavailable due to a lack of data. The risk of data breaches across the board in this sector is present across all dimensions of operational risk - people, processes, systems, and external event risks.

People Risks

Although people risks are present in every critical infrastructure sector to some degree, it is particularly salient in the healthcare sector. Healthcare was the only sector in the 2018 Verizon Data Breach Investigation report where there were more internal actors responsible for breaches than external actors.[7] The Verizon Report also noted that of the breaches that they received data on, the breaches most often happened due to error or misuse of privileges (although phishing is still certainly present as a risk as well).[8] A step away from outright error (which itself comes in many varieties, from disposal errors to publishing errors), even being careless about transmission methods also contributes to the risk of breaches. A 2018 survey of healthcare workers found that 87 percent admitted to using non-secure email to send PHI, and a majority said "when it comes to transferring data, documents, or information, they do whatever is easiest" – some even using cloud storage services like Dropbox.[9] The misuse of privileges is particularly egregious, as healthcare insiders were found to be "most likely to snoop on their family members" followed closely by looking up information about their co-workers and then VIPs.[10] The greater number of internal actors responsible for breaches, and misuse and error as the primary causes suggest that the internal controls around data security are not as strong as they could be in healthcare environments.

Some of the strongest internal controls to prevent employee ignorance or malfeasance (that would likely result in breaches) are strong codes of conduct and senior management 'tone at the top' to demonstrate ethical behaviors for the organization.[11] Without these two important components of governance, efforts to improve the number of breaches are likely to fail. The healthcare sector is no stranger to codes of conduct, but it is possible that they view the sanctity

of private healthcare records as paling in comparison to their duties under the Hippocratic Oath. A stronger code of conduct regarding how data should be handled and modeling that behavior from leaders within the organization is one possible way to mitigate the tendencies of those working in healthcare to send documents via an insecure method, or to sneak a look at a celebrity's medical records in their database.

Process Risks

Inadequate processes create significant risks for protected health information on both the public and private sides of the sector. Those inadequate processes range from not having procedures in place at all, processes not being followed correctly (as seen with the risks created when employees chose to not use secure file transmission tools at their disposal), and either the lack of individuals managing these cybersecurity risks in the organization or those individuals are without appropriate authority to enact controls. In the private sector, organizational processes are still fluid in terms of reporting structure – the Chief Information Security Officer (CISO) does not necessarily report straight to the Board or the CEO, giving them less authority to work with. These process failures are larger indicators of internal controls not being in place that would otherwise "help ensure that actions identified to address risks are carried out."[12]

On the public-sector side, the risk stems more often from processes being either ineffective or not being reliably in place across different agencies. The Inspector General for the Department of Defense found in a 2018 report that "officials from DHA [Defense Health Agency], Navy, and Air Force did not consistently implement security protocols to protect systems that stored, processed and transmitted EHRs and PHI at the locations tested."[13] The report even warned that the locations visited by the Inspector General, which had HIPAA violations due to their lax security protocols "could cost up to 1.5 million dollars in penalties for each category of violation."[14] At the facilities the Inspector General visited, there were not reliable protocols in place for, among other things, compliance with password complexity requirements, multifactor authentication, access control based on duties, standard operating procedures for system access, and privacy impact assessments were not updated or did not exist at all.[15] The Office of Management and Budget (OMB) also found that across the federal agencies it looked at, "only 16 percent of agencies achieved the target for encrypting data at rest" – this problem of process is certainly not unique to healthcare.[16]

It is impossible to fully manage risks that are not well understood, and in the case of health record data, risk is introduced because those charged with its care are not fully aware of the assets they held. The audit by the Inspector General found that there was no requirement for the identification of systems that contained patient health information, so officials did not know about all the systems with that kind of vulnerable information.[17] Even when there are appropriate hierarchical structures in place and individuals within those pivotal roles, risk is still present if

leadership does not prioritize the implementation of changes. The DHS and OMB's report *Federal Cybersecurity Risk Determination Report and Action Plan* found that across federal agencies "assessments show that CIOs and CISOs often lack the authority necessary to make organization-wide decisions despite direction to centralize authority in statutes such as FITARA and FISMA."[18] As Moeller adeptly says, the tone set at the top matters a great deal to the overall effectiveness of a control environment, and right now at the highest level of our government the position of cybersecurity coordinator has been eliminated from the National Security Council by the White House. This move signals that the current administration does not rank cybersecurity as a high priority, slowing momentum for government agencies to implement cyber directives.[19,20] The OMB report emphasizes how crucial senior leadership is to mitigating risk, as "OMB and the Inspector General have repeatedly found that senior-level visibility and authority is necessary to drive consistent improvement in agency cybersecurity."[21]

On the private-sector side, the exact same risks are present, both from a lack of adequate processes and from a lack of people that can put those processes in place and enforce them. As Moeller points out, "The control environment is greatly influenced by the extent to which individuals recognize they will be held accountable."[22] Many private healthcare organizations lack an authority that can drive policy around information technology risk and push for greater accountability. The Ponemon Institute's 2018 *Impact of Cyber Insecurity on Healthcare Organizations* study found that of the organizations surveyed, only 51 percent had a dedicated CISO, and a large percentage felt that their in-house cybersecurity skills were lacking.[23] The insufficient number of personnel overseeing data security increases the likelihood of risks stemming from little oversight and even a lack of processes. That same report found that only half of those surveyed had incident response plans in place.[24]

System Risks

The healthcare sector experiences increased systems risk when aging IT infrastructures are not updated in a timely fashion, third-party vendors have access to systems, and organizations introduce new medical devices without adequate security measures built in. Any of these circumstances increases operational risks and the vulnerability of personal health data. Aging IT infrastructure (of all kinds) inherently increases systems risk, particularly if an organization is not actively planning to update and replace this infrastructure in a timely manner. However, if an organization does not address known, existing vulnerabilities in their systems, this introduces a far higher degree of risk, as those systems then become 'low-hanging fruit' ready to be exploited.[25] This IT infrastructure may include x-rays or MRI machines running legacy software that has been overlooked for patching or may not be included in the process of systems being actively monitored. Legacy systems often have "hardcoded passwords that can be found with a simple Google search."[26] A hospital bed will have on average between 10 and 15

devices connected to it, which means the risk quickly multiplies, especially with different manufacturers and standards.[27] Even if all of the systems are relatively up to date, the healthcare sector must grapple with an enormous volume of devices connected to their networks and systems.

The systems risk that comes along with the sheer size of healthcare's mandate, as well as infrastructure not being updated, the risk is compounded by the addition of Internet of Things (IOT) capabilities being added to medical devices. In recent years, there has been movement towards imposing standards on IOT systems, but the market is currently being flooded with devices that do not always come with security built in mind. Without strong incentives, vendors have little reason to take the time and expense to build in the necessary security that would mitigate system risks from connecting these devices to healthcare environments. The FDA has starting issuing non-binding guidance and recommendations with regard to medical device security, but there are not yet mandatory requirements that would allow for security reliability and interoperability.[28] It is also possible (however unlikely it may currently seem) that legislation addressing the standards for IOT devices and systems could be passed by Congress. In the fall of 2017, Senators Warner, Gardner, Wyden, and Daines proposed the Cybersecurity Improvement Act, which would require "minimum security standards for federal procurements of connected devices."[29] Imposing federal standards would greatly simplify things on the public sector side, as there would be a consistent baseline to follow, and the private sector would soon follow, having incentives to be compliant for federal contracts, and because ensuring the interoperability of systems would also reduce risk.

External Event Risks

Risks from external events in the healthcare IT sub-sector stem from the public facing nature of most organizations, the crucial nature of services provided by operations, and the profitable nature of personal healthcare data which incentivizes bad actors to try obtaining it. The DHS's Sector-Specific Plan for healthcare that the "HPH sector is inherently more vulnerable than many of the other critical infrastructure sectors" due to their community focus, service ethos, and public access.[30] The risks created by the inherent nature of the sector will never be able to be fully mitigated, but the risks created are in fact exacerbated by other external factors. The incentive to target healthcare information technology with malware and phishing attacks is in fact doubled. There is the higher profit to be had from healthcare records. One estimate from The Ponemon Institute puts a healthcare record (including name, date of birth, and social security number) as worth about fifty dollars on the black market, compared to a credit card being worth about three dollars.[31] No matter which type of malicious actor is at work, from criminal syndicates to foreign nation-states, there is a strong financial motivation to target healthcare IT on both the public and private sides.

Additionally, the reality is that within the healthcare sector, critical systems support the delivery of emergency (acute) as well as persistent medical care to people. Hospitals and other organizations within the sector are far more likely to pay a ransom to get sensitive data back, and quickly, because that information may be needed in order to provide treatment. In January 2018, a hospital in Indiana paid a ransom of $55,000 (in bitcoin) to bad actors holding their IT system hostage, even though they had backups in place.[32] The administration of the hospital felt that restoring from the backup would have been too expensive and taken too long, in comparison to paying the ransom. In that particular case, no patient information appeared to have been compromised, but there is little guarantee of that in other circumstances.[33] These incentives for bad actors creates lots of external risk, and which is reflected in the amount of malware present in the healthcare industry – Verizon's 2018 *Data Breach Investigation Report* estimates that ransomware to get personal health data accounts for 85 percent of all the malware in the healthcare sector.[34] The sector is hard pressed to keep up with the volume of attacks, as even a single strain of malware can wreak havoc. The Department of Health and Humans Services issued a warning in March of this year that as of that time, there had been "at least eight separate cyber-attacks on healthcare and government organizations utilizing a form of ransomware known as SamSam."[35]

Recommendations

In order for there to be greater alignment and partnership between the public and private sectors, there should be better user experience design in healthcare tools and products, facilitated information sharing within the sector regarding emerging cyber threats, and legislation passed with cybersecurity requirements for both medical devices and IOT devices. To strengthen these efforts, organizations should provide regular training for those working with PHI and EHR data to increase awareness of the multiple areas of risks. Ultimately, senior leadership positions in healthcare and public health organizations will need to clearly and regularly communicate the high priority of implementing these risk mitigation efforts.

Improved user experience in healthcare tools and products would ease the burden of security fatigue on the end user and help to 'nudge' people in the right direction, mitigating the risk of internal actors causing breaches. Legislation putting cybersecurity standards in place for medical and IOT devices would not only show that our government is taking the risk presented by those devices seriously, it would also force the vendors creating those devices to incorporate security into their entire approach. Continuous training and tone at the top are the kinds of mitigations that seem obvious, but are still missing in too many places, where there is a lack of will or budget, or both in order to more effectively reduce data breach risks. Facilitated information sharing does already occur within the sector, due to DHS and ISAC coordination, and healthcare as a sector is still consistently facing threats to data that were not seen in other

environments, suggesting that there is far more work to be done for threat environment awareness and risk mitigation.

SOURCES

[1] Department of Homeland Security. "Healthcare and Public Health Sector." *Department of Homeland Security.* 11 Jul 2017. Accessed May 2018. <https://www.dhs.gov/healthcare-public-health-sector>

[2] *Healthcare and Public Health Sector-Specific Plan.* Department of Homeland Security. May 2016. Accessed May 2018. <https://www.dhs.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf>

[3] *Healthcare and Public Health Sector-Specific Plan.* Department of Homeland Security. May 2016. Accessed May 2018. <https://www.dhs.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf>

[4] Black, Ryan. " March's Reported Data Breaches: Another 120,000 Patients at Risk (So Far)." *Healthcare Analytics News.* 2 Apr 2018. Accessed May 2018. < http://www.hcanews.com/news/marchs-reported-data-breaches-another-120000-patients-at-risk-so-far>

[5] *2018 Data Breach Investigations Report, 11th Edition.* Verizon. Apr 2018. Accessed May 2018. <https://www.verizonenterprise.com/verizon-insights-lab/dbir/>

[6] Jay, Jay. "Healthcare sector suffered more than half of all cyber-attacks in 2017." *SC Media.* 4 May 2018. Accessed May 2018. <https://www.scmagazineuk.com/healthcare-sector-suffered-more-than-half-of-all-cyber-attacks-in-2017/article/763532>

[7] *2018 Data Breach Investigations Report, 11th Edition.* Verizon. Apr 2018. Accessed May 2018. <https://www.verizonenterprise.com/verizon-insights-lab/dbir/>

[8] *2018 Data Breach Investigations Report, 11th Edition.* Verizon. Apr 2018. Accessed May 2018. <https://www.verizonenterprise.com/verizon-insights-lab/dbir/>

[9] Donovan, Fred. "Most Healthcare Workers Admit to Non-Secure Healthcare Data Sharing." *Biscom.* 21 May 2018. Accessed May 2018. <https://www.biscom.com/most-healthcare-workers-admit-to-non-secure-healthcare-data-sharing/>

[10] *Protenus Breach Barometer Report.* Protenus. 3 May 2018. Accessed May 2018. <https://protenus.com/press/press-release/113m-patient-records-breached-from-january-to-march-2018>

[11] Moeller, Robert. *COSO Enterprise Risk Management.* John Wiley & Sons, Inc. 2011, p. 11.

[12] Moeller, Robert. *COSO Enterprise Risk Management.* John Wiley & Sons, Inc. 2011, p. 166.

[13] U.S. Department of Defense Inspector General. *Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities.* 2 May 2018. Accessed May 2018. <https://media.defense.gov/2018/May/07/2001913398/-1/-1/1/DODIG-2018-109.PDF>

[14] U.S. Department of Defense Inspector General. *Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities.* 2 May 2018. Accessed May 2018. <https://media.defense.gov/2018/May/07/2001913398/-1/-1/1/DODIG-2018-109.PDF>

[15] U.S. Department of Defense Inspector General. *Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities.* 2 May 2018. Accessed May 2018. <https://media.defense.gov/2018/May/07/2001913398/-1/-1/1/DODIG-2018-109.PDF>

[16] The Office of Management and Budget. *Federal Cybersecurity Risk Determination Report and Action Plan.* May 2018. Accessed May 2018. < https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf>

[17] U.S. Department of Defense Inspector General. *Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities.* 2 May 2018. Accessed May 2018. <https://media.defense.gov/2018/May/07/2001913398/-1/-1/1/DODIG-2018-109.PDF>

[18] The Office of Management and Budget. *Federal Cybersecurity Risk Determination Report and Action Plan.* May 2018. Accessed May 2018. < https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf>

[19] Moeller, Robert. *COSO Enterprise Risk Management.* John Wiley & Sons, Inc. 2011.

[20] Perlroth, Nicole and Sanger, David E. "White House Eliminates Cybersecurity Coordinator Role." *The New York Times.* 15 May 2018. Accessed May 2018. < https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html>

[21] The Office of Management and Budget. *Federal Cybersecurity Risk Determination Report and Action Plan.* May 2018. Accessed May 2018. < https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf>

[22] Moeller, Robert. *COSO Enterprise Risk Management.* John Wiley & Sons, Inc. 2011.

[23] Dorch, Sheryl. " Merlin International & Ponemon Institute Cybersecurity Study Signals Dangerous Diagnosis for Healthcare Industry." *BusinessWire.* 12 Mar 2018. Accessed May 2018. <https://www.businesswire.com/news/home/20180312005302/en/Merlin-International-Ponemon-Institute-Cybersecurity-Study-Signals>

[24] Dorch, Sheryl. " Merlin International & Ponemon Institute Cybersecurity Study Signals Dangerous Diagnosis for Healthcare Industry." *BusinessWire.* 12 Mar 2018. Accessed May 2018. <https://www.businesswire.com/news/home/20180312005302/en/Merlin-International-Ponemon-Institute-Cybersecurity-Study-Signals>

[25] Jay, Jay. "Healthcare sector suffered more than half of all cyber-attacks in 2017." *SC Media.* 4 May 2018. Accessed May 2018. <https://www.scmagazineuk.com/healthcare-sector-suffered-more-than-half-of-all-cyber-attacks-in-2017/article/763532>

[26] Davis, Jessica. "When medical devices get hacked, hospitals often don't know it." *Healthcare IT News.* 11 May 2018. Accessed May 2018. < http://www.healthcareitnews.com/news/when-medical-devices-get-hacked-hospitals-often-dont-know-it >

[27] Snell, Elizabeth. "How IoT Impacts Medical Device Cybersecurity Considerations." *Health IT Security.* 29 Nov 2017. Accessed May 2018. < https://healthitsecurity.com/news/how-iot-impacts-medical-device-cybersecurity-considerations>

[28] Snell, Elizabeth. "How IoT Impacts Medical Device Cybersecurity Considerations." *Health IT Security.* 29 Nov 2017. Accessed May 2018. < https://healthitsecurity.com/news/how-iot-impacts-medical-device-cybersecurity-considerations>

[29] Warner, Mark, et al. *Internet of Things Cybersecurity Improvement Act of 2017. S. 1691.* U.S. Senate. 1 Aug 2017. Accessed May 2018. < https://www.congress.gov/bill/115th-congress/senate-bill/1691>

[30] *Healthcare and Public Health Sector-Specific Plan.* Department of Homeland Security. May 2016. Accessed May 2018. <https://www.dhs.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf>

[31] Fox, Bill. "How to protect patient data that's being shared widely." *Health Data Management.* 25 May 2018. Accessed May 2018. < https://www.healthdatamanagement.com/opinion/how-to-protect-patient-data-thats-being-shared-widely>

[32] Osborne, Charlie. "US hospital pays $55,000 to hackers after ransomware attack." *ZDNet.* 17 Jan 2018. Accessed May 2018. < https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/>

[33] Osborne, Charlie. "US hospital pays $55,000 to hackers after ransomware attack." *ZDNet.* 17 Jan 2018. Accessed May 2018. < https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/>

[34] *2018 Data Breach Investigations Report, 11th Edition.* Verizon. Apr 2018. Accessed May 2018. <https://www.verizonenterprise.com/verizon-insights-lab/dbir/>

[35] Healthcare Cybersecurity and Communications Integration Center. *Report on Ongoing SamSam Ransomware Campaigns.* 30 Mar 2018. Accessed May 2018. <https://www.aha.org/system/files/2018-04/corrected-HCCIC-2018-002W-SamSam-Ransomware-Campaign.pdf>