Florida Society for Healthcare Risk Management & Patient Safety

RESEARCH INTERNSHIP

Cybersecurity Risk Management in Health Care

Purpose: As we become more accustomed to our reliance on digital technologies it is essential to understand the core cybersecurity risk exposures that health care organizations are constantly facing. As Health care systems become more dependent on the internet like electronic health records, online medical devices, or the movement of patient data these services become much more vulnerable to cybersecurity threats. Understanding these risks is essential for healthcare organizations to ensure that data breaches, ransomware and phishing attacks are minimized as much as possible.

Background and Relevancy

HealthCare records are constantly under fire from bad actors and minimizing any risk associated with keeping patient files safe is becoming harder and harder. The Office for Civil Rights began openly documenting HealthCare data breaches in 2009, and we have seen a massive increase in the number of data breaches per year. These data breaches have led to compromised access of over one billion instances of patient data, and it's been steadily increasing since. In 2024 the average data breach resulted in 400,000 patient's information being accessed without authorization, the sheer increase that we've seen over the years prompts the need for awareness on different types of risks that are present in HealthCare.

Risks can come from anywhere, whether that be exposed credentials, unattended hardware, or individuals clicking malicious links, they are apparent everywhere. These are all things that individuals working in the HealthCare field must be informed about. In this day and age of technology majority of healthcare organizations have switched to electronic healthcare records (EHR) or cloud-based systems, recognizing these apparent threats are crucial. Cyberattacks like ransomware, phishing, insider threats, and third-party vendor vulnerabilities will always be aimed at HealthCare systems because of all the sensitive patient information stored. Due to constantly being under threat of bad actors HealthCare systems require strong technical security controls for managing risks so that patient data is safely stored and all possible risks are lessened.

Research Objectives

- Identify major cybersecurity risks affecting healthcare organizations.
- Assess the best current practices for integrating cybersecurity into Enterprise Risk Management.
- Analyze why data breaches are continuing to rise in occurrence year by year and assess potential risk mitigation tactics.

Core Cybersecurity Risk Exposures in Health Care

Cybersecurity risks exist wherever technology is used. Understanding these risks and creating mitigation techniques are essential to ensuring patient safety and regulatory compliance. One of the most significant threats for health care organizations is ransomware, ransomware is a type of cyberattack which attackers encrypt certain systems such as health records and demands payment for their release. These attacks can occur in many different ways, including social engineering, phishing, compromised credentials, or insider threats. Although no organization can fully eliminate cyber risk entirely, limiting your exposure to harmful actors along with proactive risk management is imperative to keeping your network safe.

Phishing scams are one of the most notable attacks as they are relatively easy to perform and employees often accidentally fall for them. A phishing attack is when bad actors attempt to trick people into giving away sensitive information or allowing access to computers or networks, most of the time this is done by emails, text messages or phone calls. These phishing emails often are sent by fake websites that appear to be trusted organizations but are false. In most email phishing links, it will send you to a legit looking website and prompt you for your credentials, once the user inputs said credentials the bad actor then given those credentials. These harmful actors will use phishing to gain user credentials to then access systems, patient records, or other sensitive information then either sell said information or encrypt it leading to ransomware. Sadly, phishing is one of the most successful cyber-attacks as it focuses on targeting people instead of technology, even with training you cannot guarantee that all employees can identify phishing links.

Data Breaches Throughout the Years

Healthcare risk managers must understand that cyber threats will continue to increase in both frequency and impact. Each year, there has been a rise in the number of reported healthcare data breaches which further increases the need for active risk management. The table below shows the current trend of healthcare data breaches and showcases why cybersecurity will remain a critical part of enterprise risk management.

Year	Data Breaches Affecting Fewer than 500 individuals.	Percentage Annual Change
2024	74,299	9% increase
2023	68,315	7% increase
2022	63,966	1% increase
2021	63,571	4% decrease
2020	66,509	-

Cybersecurity Training for Health Care Risk Managers

Health Care Risk Managers are not expected to be cybersecurity experts; however, they should possess a strong understanding of common cyber threats and the threat against health care organizations. They should be able to identify emerging threats, assess organizational risk, and collaborate effectively with information security professionals to ensure smooth compliance.

To help develop these skills there are many professional certifications and training programs. One of the most recognized certifications on health care risk management is the Certified Professional in Health Care Risk Management (CPHRM) certificate organized by the American Hospital Association. The CPHRM provides a strong foundation enterprise risk management, regulatory compliance, patient safety, and cyber risk within health care.

Blending Cybersecurity into an Enterprise Risk Management Program

Cybersecurity should be incorporated into every organization's enterprise risk management program as it affects anything connected to technology. With Healthcare organizations relying so heavily on Electronic health records, connected medical devices, and online communication systems, cybersecurity risks must be addressed. If you want a successful ERM program there should be a key inclusion of cybersecurity as there are so many risks which include operational, financial, regulatory, and patient safety risk.

Health Care Risk Managers play a crucial role in integrating cybersecurity into an organization's broader risk management process. These steps would include identifying critical information systems and data, assessing any potential cyber threats, analyzing the likelihood of an attack, determining the potential impact of incidents and working with information security personnel to create proper controls.

Collaboration and communication between risk management, IT, executive leadership, and key stakeholders is essential for allowing cybersecurity risks to be evaluated from all different points of view. Cybersecurity risks affecting many different areas in different ways often require different sets of eyes to determine potential impact/severity. Enterprise Risk Management Programs should require regular employee cybersecurity training, incident response planning, vendor risk assessments, vulnerability management, and data backup strategies.

Every year we grow more and more attached to technology and begin to implement it in new ways, especially in our healthcare systems. Cyberattacks affect more than just data and systems, patient safety, public health, intellectual property and reputation are all at risk from cyberattacks. Cyber risk and enterprise risk are too closely interconnected to address one without considering the other. Both are essential components of protecting an organization and ensuring its overall safety and security.

Integrating Cybersecurity Risk into an ERM Case Study

Case Study Overview

The integration of cybersecurity risk into enterprise risk management has become more apparent as cyber threats continue to affect organizations in many different parts. Sasha Romanosky and Elizabeth L. Petrun Sayers throughout this case study examined how organizations are able to incorporate cyber risk into their ERM programs and found that many organizations have actually used very different approaches. This research performed shows that cyber security does not have to be treated as just an isolated concern for risk, rather, it should be incorporated throughout the organization's broader risk management framework.

Merging Cyber Risk into Enterprise Risk

One key point from this case study is that organizations can incorporate cyber risk into already established ERM processes, so this process is possible without the need of creating an entirely separate risk management structure. Cybersecurity risks include such a wide range of areas including financial, operational, legal, regulatory, and reputational risk which also stem from general organizational risk. Merging the two types allows leadership to evaluate cyber risk based on its potential impact on the organizations overall objectives rather than approaching each risk individually as an issue.

Organizational Leadership

Communication is key. This case study cements that by highlighting the importance of communication between cyber security professionals, risk managers, board of directors, and executive leadership. The collaboration between cyber professionals and enterprise risk managers is required as cybersecurity professionals understand the technical aspects of threats meanwhile the enterprise risk managers and leadership understand how the threats can affect overall business operations. The communication would allow cyber risks to be translated into business risks that can be compared with any other current risks that the organization is facing to determine urgency.

Implications for Healthcare Organizations

Integrating cybersecurity risks into already established enterprise risk management programs is very relevant for healthcare organizations as cybersecurity incidents can affect patient safety, regulatory compliance, financial stability, and continuity of care. The IT department should not be solely responsible for cyber risks and should be a team effort to ensure that all risks are being properly identified and delt with. Completely combining an ERM program and cyber risk can help organizations identify connections between cybersecurity vulnerabilities and other enterprise risks which allows for more robust controls and mitigation strategies to be made.

Why is this Case Study Important

This case study explains that cybersecurity risks and enterprise risk are so closely related that if you treat them as separate entities, vulnerabilities become much harder to combat without proper communication between teams. Treating cyber risk as part of an ERM allows organizations to evaluate cyber threats based on their potential impact on the entire organization. Primarily for healthcare risk management, the combining of cyber risk and enterprise risk reinforces the importance of communicating with cybersecurity professionals to ensure that cyber threats are incorporated into broader organizational risk assessments. Overall, integrating cybersecurity into ERM helps to create a stronger approach to protecting organizational operations, safeguarding information, financial resources, and patient care.

Cybersecurity Threats Across Health Care Environments

Physician Office Practice: Often times physician office practices are frequent targets of several cybersecurity attacks including phishing, ransomware, and email compromise attacks. This is often due to them having limited cybersecurity resources and smaller IT teams. These smaller IT teams may be behind on updates to critical software, employee training, or reliance on other third-party vendors.

Outpatient Clinic: This is another area of healthcare that is very vulnerable to cyberthreats due to the lack of cybersecurity resources and smaller IT staff. Outpatient Clinics face cyberthreats to their cloud based electronic health records, along with human focused attacks. With such a high patient turnover rate there is a reliance on mobile devices and online systems which increase the risk of unauthorized access through phishing or data breaches.

Hospital: The pinnacle of high-risk environments, hospitals often times are so vast it makes them vulnerable, having a large attack surface with complex networks and constant operations leaves room for bad actors to infiltrate. There are many cyber threats that plague hospitals like Ransomware, insider threats, Distributed denial of service attacks (DDoS), and supply chain vulnerabilities just to name a few. These vectors are so important to always be secure as any of these attacks that can disrupt patient care directly threatens patient safety.

Long Term Care Facility: This type of facility is very vulnerable to cybersecurity threat mostly due to the limited cybersecurity resources they have along with outdated technology. These weak points make them a huge target for any bad actors and increases their risk of ransomware, phishing, or unauthorized access. The amount of risk carried can also be influenced by proper training of staff and how well they can identify cybersecurity threats.

References:

U.S Department of Health and Human Services, Office for Civil Rights. “Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information”. U.S. Department of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report_hip.jsf.

Alder, Steve. “Healthcare Data Breach Statistics.” Healthcare Data Breach Statistics - Updated for 2026, The HIPAA Journal, 18 June 2026, www.hipaajournal.com/healthcare-data-breach-statistics/.

Clarke, Matthew. “Managing Cybersecurity Risk in Healthcare Settings - PMC.” Managing Cybersecurity Risk in Healthcare Settings, Dalhousie University, 25 Aug. 2023, pmc.ncbi.nlm.nih.gov/articles/PMC10725101/.

Southwick, Ron. “Cyberattackers Target Physician Practices, Specialty Groups | Chief Healthcare Executive.” Chief Healthcare Executive, 14 July 2025, www.chiefhealthcareexecutive.com/view/cyberattackers-target-physician-practices-specialty-groups.

Riggi, John. “Why & How to Incorporate Cyber Risk Management into Enterprise Risk Management: Cybersecurity: Center: AHA.” American Hospital Association, American Hospital Association, www.aha.org/center/cybersecurity-and-risk-advisory-services/why-how-incorporate-cyber-risk-management-enterprise-risk-management.

Romanosky, Sasha, and Elizabeth L Petrun Sayers. “Enterprise Risk Management: How DO Firms Integrate Cyber Risk? | Management Research Review | Emerald Publishing.” Enterprise Risk Management: How Do Firms Integrate Cyber Risk?, Emerald Publishing, 30 Oct. 2021, www.emerald.com/mrr/article/47/1/1/1232191/Enterprise-risk-management-how-do-firms-integrate.