Tampa General Hospital

Pieter de Swart

University of Charleston, West Virginia

CYBR-410-01N

Professor Bryan Bell

19 May 2024

Harmful cyber-attacks that target vulnerabilities in critical cyberinfrastructure (e.g., servers hosting confidential data) cost an average of $8.64 million per breach (Ampel, 2024). Risk assessment is a systematic process designed to identify, evaluate, and prioritize risks, followed by coordinated efforts to minimize, monitor, and control the probability and impact of unfortunate events. This process is crucial for organizations, especially in the healthcare sector, where the stakes involve not only financial losses but also the safety, confidentiality, and well-being of patients. Tampa General Hospital, a leading healthcare provider, faces a myriad of risks that could significantly impact its operations and reputation. This paper will apply the concepts of risk assessment, risk analysis, data classification, and security awareness to Tampa General Hospital. It will provide an overview of the general threats the hospital faces, the potential vulnerabilities in its systems, the likelihood of these threats materializing, and the potential impacts if they do. By thoroughly understanding these elements, the hospital can prioritize its risks effectively. Based on this detailed assessment, the paper will offer recommendations on appropriate risk management strategies, including risk avoidance, risk acceptance, risk mitigation, and risk transference. These strategies will help Tampa General Hospital to safeguard its critical information, ensure compliance with regulations, and maintain the trust and safety of its patients and staff.

Cyber threats pose a significant risk to Tampa General Hospital, encompassing various malicious activities that could severely disrupt operations and compromise patient data. One of the most concerning cyber threats is malware and ransomware. Attackers can deploy malicious software designed to encrypt the hospital's data, effectively locking access to critical patient records and operational information. In such cases, attackers demand a ransom for the decryption key, placing the hospital in a difficult position where paying the ransom may seem like the quickest way to restore functionality, but it also encourages further attacks and does not guarantee the safe return of the data. Phishing attacks are another prevalent threat that targets hospital employees through deceptive emails or messages that appear legitimate. These phishing attempts often aim to steal login credentials or deploy malware, leading to unauthorized access to hospital systems. This can result in compromised patient information, disrupted operations, and potential financial loss. Given the high volume of sensitive data handled by the hospital, phishing attacks pose a significant risk that requires constant vigilance and employee training to recognize and avoid such schemes. Distributed Denial of Service (DDoS) attacks can overwhelm the hospital’s servers, causing significant disruptions in accessing critical services. During a DDoS attack, multiple compromised systems are used to flood the hospital’s network with excessive traffic, making it difficult or impossible for legitimate users to access necessary applications and information. This can have severe implications for patient care, as it hinders the hospital’s ability to operate smoothly and respond to emergencies efficiently.

Insider threats are another critical concern for Tampa General Hospital. Employees with access to sensitive data could intentionally or unintentionally compromise data security. This could happen through malicious intent, such as a disgruntled employee stealing data for personal gain, or through negligence, such as inadvertently sharing confidential information or falling prey to social engineering attacks. Insider threats are particularly challenging to manage because they involve individuals who already have legitimate access to the hospital’s systems and data. The variety of cyber threats facing Tampa General Hospital requires a comprehensive and proactive approach to cybersecurity. Implementing robust security measures, conducting regular training and awareness programs for employees, and continuously monitoring and updating systems are essential steps in protecting against these threats and ensuring the security and integrity of the hospital’s operations and patient data. Physical threats pose significant risks to Tampa General Hospital, ranging from theft and vandalism to natural disasters. Physical intrusion could lead to the theft of hardware that contains sensitive information or damage to essential equipment. Such incidents can result in the loss of critical data and disrupt hospital operations, impacting patient care and safety. Furthermore, natural disasters such as hurricanes, floods, or other severe weather events pose a substantial threat to the hospital's infrastructure. These events can cause extensive physical damage, leading to data loss and prolonged service disruptions, which can severely impact the hospital’s ability to function effectively during and after the disaster.

Cyber vulnerabilities present a considerable risk to Tampa General Hospital’s digital infrastructure. Outdated software is a major vulnerability, as systems and applications that are not regularly updated with the latest security patches are more susceptible to exploitation by cyber attackers. Weak password policies, where simple or reused passwords are used, make it easier for attackers to breach systems. Additionally, a lack of employee training can lead to staff being unaware of security protocols, making them more likely to fall prey to phishing and social engineering attacks. Inadequate network security, such as poorly configured firewalls and network access controls, can leave the hospital’s systems exposed to external attacks, increasing the risk of unauthorized access and data breaches. Physical vulnerabilities also pose significant risks to the hospital’s security and operations. Insufficient physical security measures, such as a lack of surveillance and access control, can make the hospital facilities more vulnerable to unauthorized entry and physical intrusions. Also, inadequate disaster recovery plans can leave the hospital unprepared for significant events such as natural disasters. Without robust disaster recovery and backup plans in place, the hospital could suffer substantial data loss and extended downtime, severely affecting its ability to provide continuous patient care and maintain operational efficiency during emergencies.

Cyber threats to Tampa General Hospital include malware and ransomware, which have a moderate likelihood due to the high value of healthcare data on the black market and the increasing frequency of such attacks. Phishing attacks have a high likelihood as healthcare organizations are often targeted for their valuable patient data. DDoS attacks have a low to moderate likelihood, depending on the visibility and perceived value of disrupting hospital services. Insider threats, involving employees with access to sensitive information, also have a moderate likelihood, reflecting the potential for both intentional and unintentional security breaches. Physical threats include theft and vandalism, which have a low to moderate likelihood depending on the effectiveness of the hospital's physical security measures. Natural disasters have a high likelihood in Tampa due to the region's susceptibility to hurricanes and floods, posing significant risks to the hospital's infrastructure and operations.

Cyber threats to Tampa General Hospital can have varying levels of impact. Malware and ransomware attacks can have a severe impact due to potential data loss, significant financial costs, and the disruption of patient care. Phishing attacks can lead to significant impacts if sensitive data is compromised, resulting in financial loss and reputational damage. DDoS attacks can cause moderate to severe impact by disrupting services that affect patient care and hospital operations. Insider threats can have a severe impact if critical data is compromised, leading to regulatory fines, loss of patient trust, and operational disruption. Physical threats also pose significant risks to Tampa General Hospital. Theft and vandalism can have a moderate to severe impact, especially if critical equipment is stolen or damaged, affecting the hospital’s ability to provide care. Natural disasters have a severe impact due to the potential for extensive damage to infrastructure, data loss, and long-term service disruptions, which can significantly impair hospital operations and patient care.

Conventional cybersecurity methodologies have historically focused on establishing robust perimeter defenses, such as firewalls and intrusion detection systems, to protect an organization's network infrastructure (Mizrak, 2024). To effectively avoid risks, Tampa General Hospital should implement comprehensive cybersecurity measures, including regular software updates, strong password policies, and robust network security configurations, to prevent cyber-attacks. Additionally, strengthening physical security through enhanced access controls, surveillance systems, and secure storage for sensitive equipment can further mitigate potential threats. In some cases, it is practical to accept minor risks where the cost of mitigation exceeds the potential impact. For instance, the hospital can accept occasional low-level phishing attempts that are unlikely to cause significant harm if proper awareness and response protocols are in place. Similarly, accepting minor physical incidents that are unlikely to cause major disruption or loss is a reasonable approach. Risk mitigation strategies are essential to manage and reduce the impact of potential threats. Conducting ongoing employee training can raise awareness of phishing tactics, cybersecurity best practices, and emergency response protocols. Developing and regularly updating disaster recovery and business continuity plans ensure rapid response and recovery from natural disasters and other significant events. Performing regular security audits and vulnerability assessments helps identify and address potential weaknesses in the hospital's systems and processes. To transfer some of the financial risks, Tampa General Hospital should obtain comprehensive cyber insurance to cover potential financial losses from cyber incidents, including data breaches and ransomware attacks. Securing property insurance can cover physical losses from theft, vandalism, and natural disasters, providing an extra layer of financial protection for the hospital's assets.

Risk assessment and management are critical for ensuring the security and resilience of Tampa General Hospital. By understanding the general threats, vulnerabilities, likelihood, and impact of various risks, the hospital can implement effective risk management strategies, including risk avoidance, acceptance, mitigation, and transference. Quantitative risk assessment formulas provide a clear framework for prioritizing these efforts. The NIST CSF is a framework that can help companies to manage and mitigate cybersecurity risk in a standard way (Melaku, 2023). With robust cybersecurity measures, regular training, comprehensive disaster recovery plans, and appropriate insurance coverage, Tampa General Hospital can protect its critical information and maintain trust and continuity in its operations.

# References

Ampel, Benjamin M., Sagar Samtani, Hongyi Zhu, Hsinchun Chen, and Jay F. Nunamaker Jr. 2024. “Improving Threat Mitigation Through a Cybersecurity Risk Management Framework: A Computational Design Science Approach.” Journal of Management Information Systems 41 (1): 236–65. doi:10.1080/07421222.2023.23

Melaku, H. M. (2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. Risks, 11(6), 101. https://doi.org/10.3390/risks11060101

Mizrak, F. (2024). Enhancing Cybersecurity Risk Management through Conceptual Analysis of Hrm Integration. Journal of Administrative Sciences / Yonetim Bilimleri Dergisi, 22(51), 96–118. https://doi.org/10.35408/comuybd.1342408