The George Washington University – School of Business

EPIC SYSTEMS CORPORATION
Risk Assessment on Current Information Systems and Risk Mitigation Strategies

Information Systems Security

Samuel Akuffo

Lecturer: Dr. Scott White

April 25, 2025

Basic Information;

Epic Systems Corporation is a privately held healthcare software corporation that provides homogenized solutions for keeping electronic health records and also other healthcare management systems. The company is headquartered in Verona, Wisconsin, United States, where it performs its business operations (Epic Systems Corporation, 2025).

History;

Epic Systems was founded in 1979 by Judith R. Faulkner as Human Services Computing Inc. in Verona, Wisconsin with just three part-time employees in a small basement office. Initially focused on data analysis, they managed to secure early contracts with state and local governments and the University of Wisconsin's psychology department. By 1983, Epic introduced Cadence; used in scheduling patients appointments, and by 1985, their revenue hit $1 million. They rebranded as Epic Systems Corporation and by 1990 had broadened their product offerings and had a larger workforce (Eisen, 2008).

The company's early growth came about as a result of their key technological innovations, such as the introduction of EpicCare in 1992; the first Windows-based electronic medical records system. They followed this achievement launching EpicWeb in 1997; a software package of web-based healthcare IT programs, positioning Epic as a leader in healthcare software industry (Eisen, 2008).

Epic's breakthrough came in 2003 when they secured a $1.8 billion IT project with Kaiser Permanente; the nation's largest non-governmental healthcare provider, cementing their reputation. By 2008, Epic's workforce had grown to over 3,000 employees, and were making a revenue of more than $500 million (Eisen, 2008). Epic's software, including its flagship Epic EHR, is now used in a wide range of healthcare settings, from academic medical centers to community hospitals, independent practices, and mental health organizations. Today, it serves over 325 million patients globally (Dun & Bradstreet, 2022).

The company's commitment to innovation and unique corporate structure is a reason for their success. Epic is privately held and employee-owned, with a significant portion of operating expenses being invested in research and development. The support of developer-led innovation has helped it stay ahead in the competitive healthcare IT space. Epic's products enable seamless data exchange between healthcare organizations, improving care coordination and patient outcomes (Crunchbase, 2024).

Having over 35 years of growth and innovation, Epic's leadership under Judith Faulkner has been integral to success. As a company that is committed to its mission, they continue to set the standard for healthcare technology by striving to enhance patient care through innovative strategies (Dun & Bradstreet, 2022).

Mission;

The mission statement of the company is; “At Epic, our core mission is improving healthcare: helping people get well, helping people stay well, and helping future generations be healthier.” (Epic, 2025).

Products/Service and Customers;

As a major stakeholder in healthcare technology, they offer product and services concerned with electronic health records and also patient care and medical data management. The range of products from Epic includes; EpicCare, Care Everywhere, and Carequality. The company's core software was built using the MUMPS programming language, designed for the processing of high-performance transactions and allows Epic to handle complex healthcare applications efficiently and help healthcare organizations to simplify their patient records, scheduling and data exchange for improved care coordination, and better patient care outcomes. They have a diverse customer base consisting of academic medical centers, community hospitals, independent practices, and mental health organizations and hence indirectly serve over 325 million patients globally (Mazurek, 2024).

Future Business:

Epic Systems Corporation is ready for substantial growth as the global healthcare technology market expands. The electronic health records market is expected to exceed $60 billion dollars by 2030 and the revenue cycle management market by $11.98 billion by 2027 and based on current progress, Epic is well-positioned to capture these opportunities. With the broader healthcare technology market expected to reach heights of $457.7 billion by 2033, the environment becomes friendlier for expansion (PharmiWeb, 2024)

Epic has also embraced AI and machine learning as part of their commitment to innovation and technology. They are currently rolling out over 20 new programs with a notable one being AI-driven tools in MyChart, aiming to improve patient engagement. Embracing modern technologies such as Caché, and supporting standards such as Fast Healthcare Interoperability Resources, allows Epic to meet the ever changing needs of global healthcare systems (GlobeNewswire, 2024).

Risk Assessment – Epic;

Corporations such as Epic, who manage Private Health Information (PHI) are highly predisposed to systems breaches from individuals seeking to exploit vulnerabilities for financial or other personal gains. In a study from the Center for Strategic and International Studies, cybercrime costs have reached $600 billion annually and shows no signs of slowing down (Lewis J.A, 2018).

It has therefore become very important for companies to properly assess all their assets so they can properly protect themselves against both man-made and natural threats. A widely used method resulting from years of research, is the threat-risk assessment technique SANS Institute (2021). This technique helps in determining the likelihood of a threat and the potential impact.

Companies have different levels of risk tolerance and this is mostly based on their industry and how they operate. A company like Epic cannot be risk seeking because they handle sensitive data, their customer base and the various regulatory bodies they must comply to. These include but not limited to; the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, Federal Information Security Management Act (FISMA) and the General Data Protection Regulation (GDPR) National Institute of Standards and Technology (2020) . Despite Epic emphasizing the need for innovation and showing it through their culture they must maintain strict access controls, strong security measures, and continuous compliance with regulatory obligations that have to be in good legal and business standing.

Threat and Assessment Analysis:

Threat Assessment:

This analysis looks at four key intentional and unintentional man-made threats; insider threats, social engineering, security breaches and malware respectively.

Insider threats significant threat to Epic Systems Corporations' operations and assets because they deal with both direct and indirect insiders. The involvement of many stakeholders means that their systems are more open to potential compromise. The exposure of private health data through negligent or intentional acts could be detrimental as it involves health and other sensitive data. This could lead to a lot of legal disputes for Epic and even the possibility of people manipulating these records and leading to deaths of targeted patients as changes would ripple through to their prescriptions (Healthcare (Basel), 2020).

The second risk being considered is social engineering. Humans are gullible and it has nothing to do with intelligence, they just feel the moral right to help others in situations even if they are not supposed to (White, 2025). This problem transcends technological issues such as phishing attacks to physical breaches. The possibility that an employee might give their credentials to someone they believe is in a position to help fix an issue without proper verification or be physically lured from behind a system, giving access to a person with malicious intent is very likely.

Security breaches are a major threat to all companies handling sensitive data including Epic. In modern times, the sale of stolen data has become a lucrative venture for crackers. The more sensitive the data you handle is, the more profitable you are on the black market. These activities range from cracking passwords through to elevating privileges and breaking into servers which not only pose extensive financial threats to Epic but can also affect their market share as it builds mistrust (Lewis, 2018).

Finally we can look at malware; the umbrella term for software that has malicious purpose. Any system connected to a network is susceptible to attacks from viruses, worms, adware, Trojan horses, and spyware. Despite many incriminating laws associated with all malware associated activities, it is still not enough to deter people from related orchestrations. In modern times, they are even glorified; having review sites, communities guided by codes and potential for more financial gains especially with ransomware. It is therefore important for Epic to make sure they do not become victims (IBM, 2021).

Likelihood and Impact:

In the context of Epic's operations, the likelihood and impact of the assessed threats above are as follows;

For insider threats the likelihood of occurrence is high due to the different actors involved. It could be a compromised hospital administrator, a malicious insider intentionally stealing data or an accidental breach through a negligent employee. The overall impact is severe as it would lead to exposure of private health information, regulatory violations, downtime and even patient harm. A real world example would involve the employee from Mayo Clinic who accessed patient records and damaging their reputation and plunging them into legal battles they are still addressing today (Adler S, 2023).

Social engineering also has a high likelihood of occurrence. It can be achieved through phishing, impersonation and even physically breaches. People with high access privileges such as system administrators and finance managers are mostly targeted. The impact can be severe as skilled threat actors can gain access into Epics servers or impersonate legitimate users to manipulate patient records or commit insurance fraud. An example is the attack on Magellan Health where a ransomware was deployed through client impersonation causing downtime and affecting 55,637 plan members (Adler S, 2023).

Due to the extensive use of Epics products they are a prime target of security breaches. The likelihood of occurrence is high and involves activities such as password cracking, abuse of access privileges and the exploitation of system vulnerabilities. The impact will be critical and lead to long-lasting reputational damage, regulatory penalties and loss of customer trust. An example would be Broward Health where a third-party not implementing multi-factor authentication lead to the security breach into their patient database (Kost E, 2025).

Finally Epic's use by cross functional teams effects a high likelihood of being affected by malware. In recent times healthcare has become the target of ransomware groups with several actors having to pay ransoms to recover data. The impact will be critical as it includes downtime and ransom costs which compromise care of patients and halt operations. A typical example is Ascension Health where a ransomware attack caused delayed and lost lab results, medication errors, and an absence of routine safety checks due to weeks of disruption (Fitzgerald A, 2025).

Vulnerability Assessment:

The following are Epic's vulnerabilities to the identified threats;

In dealing with insider threats the presence of direct and indirect insiders make it nearly impossible to Epic to have complete control, making them highly exposed. The presence of third parties makes it harder to enforce guidelines and rules as it would require extra resources and legalities.

Social engineering is also a threat they are highly exposed to. As many as 90% of successful hacks and data breaches start with some form of social engineering. Once you work with people there is a possibility that their human nature will be exploited (Mitnick Security, 2024).

Finally malware and security breaches can however be seen to have moderate exposure. This is because even though in this context the actors might act quickly and infiltrate multiple systems, Epic has enough maturity to be able to isolate and contain these attacks without them spreading.

Risk Management – Epic:

Epic is a mature corporation with several measures in place to deal with threat actors and vectors they face in their daily operations. Even though they implement Integrated Risk Management into their own risk management framework, the dynamic cyber security landscape requires the continuous reiteration of such procedures. In this section, I will discuss how Epic Systems can address the risks I identified.

According to statistics 70% of data breaches are a result of insider threats (Verizon, 2024). Although most of their customers use third-party organizations such as ColorTokens to address this, Epic could implement its own guide to a Zero Trust Architecture strategy for users (National Institute of Standards and Technology, 2020). This would enforce identity based access controls for authentication of all users. The framework should include role-based access controls IBM (2021) and multi factor authentication. Behavioral and psychological assessments to reassure the background checks done initially should be repeated intermittently putting focus on conflicting interests of employees (SANS Institute, 2021). Making whistleblowing of unusual activities rewarding can also be helpful. The developments in the analytics field such as software that can track and report anomalous behavior can be integrated as part of Epic's AI initiatives. They can the log this data into Security Information and Event Management system and help them develop a more robust incident response plan.

The best way to mitigate social engineering is through continuous training and retraining of personnel on security techniques (Center for Internet Security, 2021). However, since that alone won't stop the possibility of occurrence, multi-factor authentication should be integrated in the actual system so that even if credentials such as passwords are compromised, the need for additional secure verification steps will make it nearly impossible to gain full access. Red teaming should also be encouraged and more frequent as Epic continues to grow and enter new technological and legal landscapes making the blue teams more effective and help anticipate emerging trends and threats.

For security breaches, I recommend that Epic enforces higher security stands on the customers. Business is about profits but not if they come with unbalanced costs hence only medical institutions with an NIST Maturity Level: Level 3 or higher (National Institute of Standards and Technology, 2020) should be allowed access to Epic's sensitive network resources. As the mission of Epic is strong on health is wealth I suggest a network segmentation strategy for medical centers with lower security maturity levels to protect their more secure counterparts as customers with lesser security maturity levels are the biggest vulnerabilities to Epic. Continuous security audits should be offered at a subsidized price for customers guarantee it is done and the continuous development of an incident response team would help them not only red-team-blue-team but also perform in-depth research on possibilities of security breaches and potentially reduce impact.

Regarding malware, currently Epic's mitigation tools are based on BlueVoyant's Modern SOC, Azure Sentinel and Microsoft XDR (Mocanu, Shaw-Young, & Grigorof, 2021). Since the malware landscape is constantly evolving due to leaps in computing and over 190,000 are deployed per second, it is crucial for Epic to reevaluate and update their Endpoint Detection & Response systems always. To add to previous strategy of forming a research driven response team, they can have specialized divisions within focused on innovating solutions for dealing with newer, more sophisticated polymorphic threats. As part of their AI innovations, it is essential to invest in AI detection strategies and systems (MITRE, 2020). Also penetration tests and simulation drills will go a long way in ensuring preparedness against evolving threats (OWASP, 2021). Finally implementing strong backups and recovery plans including offline backups will act as a safety net against malware such as ransomware.

As a prime target in the ever evolving world of cyber security and cyber threats, risk management is always going to be a critical function for companies like Epic. Through advanced Predictive Decision Support Interventions, Epic continuously addresses risks and keeps their promise of is improving healthcare, helping people get well, helping people stay well, and helping future generations be healthier.

REFERENCES

Epic Systems Corporation. (2020, October 28). *Crunchbase*. Retrieved from https://www.crunchbase.com/organization/epic-systems-corporation

Crunchbase. (2024, October 4). *Epic Systems Corporation*. Retrieved January 26, 2025, from https://www.crunchbase.com/organization/epic-systems-corporation/signals_and_news

Dun & Bradstreet. (2022, August 26). *Epic Systems Corporation*. Retrieved from https://www.dnb.com/business-directory/company-profiles.epic_systems_corporation.c10ab2c2e4cd91a27637c12183d16552.html?_gl=1*fwgkof*_up*MQ..*_gs*MQ..

Eisen, M. (2008, June 20). *Epic Systems: An Epic timeline*. Isthmus. Retrieved from https://isthmus.com/news/cover-story/epic-systems-an-epic-timeline/#:~:text=1979:%20Human%20Services%20Computing%20Inc,than%20half%20from%20EpicCare%20sales

Epic. (2025, January 8). *About*. Retrieved from https://www.epic.com/about/

Mazurek, M. (2024, June 15). *Epic. A Condensed Historical Overview*. Retrieved from https://www.linkedin.com/pulse/epic-condensed-historical-overview-matt-kqv1e/

Bove, M. (2023). *Epic EHR Use in Research*. PMC. Retrieved from https://pmc.ncbi.nlm.nih.gov/articles/PMC10757236/

BusinessWire. (2024). *Epic Systems expands language services through collaboration with GLOBO.* Retrieved from https://www.businesswire.com

Epic Systems. (2025). *Innovations and expansions in healthcare delivery*. Retrieved from https://www.epic.com

GlobeNewswire. (2024a). *Global healthcare information system market to surpass $457.7 billion by 2033*. Retrieved from https://www.globenewswire.com

GlobeNewswire. (2024b). *Epic's role in fostering interoperability through TEFCA*. Retrieved from https://www.globenewswire.com

GlobeNewswire. (2024c). *Strategic partnerships boost Epic's growth strategy*. Retrieved from https://www.globenewswire.com

PharmiWeb. (2024). *EHR market expected to exceed $60 billion by 2030.* Retrieved from https://www.pharmiweb.com

PRNewswire. (2024a). *Epic partners with Cohere Health to streamline prior authorizations.* Retrieved from https://www.prnewswire.com

PRNewswire. (2024b). *Revenue cycle management market set to grow by $11.98 billion.* Retrieved from https://www.prnewswire.com

Lewis J.A (2018, February 21). *Economic Impact of Cybercrime* Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime

Adler, S. (2023a, January 18) *Mayo Clinic Settles Lawsuit Alleging Former Employee Viewed Nude Patient Images* Retrieved from https://www.hipaajournal.com/mayo-clinic-settles-lawsuit-alleging-former-employee-viewed-nude-patient-images/

Adler, S. (2023b, January 3) *Healthcare Data Breaches Due to Phishing* Retrieved from https://www.hipaajournal.com/healthcare-data-breaches-due-to-phishing/#:~:text=Magellan%20Health%20Inc.,that%20affected%2055%2C637%20plan%20members.

Kost E. (2025, January 2) *14 Biggest Healthcare Data Breaches [Updated 2025]* Retrieved from https://www.upguard.com/blog/biggest-data-breaches-in-healthcare

Fitzgerald, A. (2025, January 9) *Ransomware Attacks: Definition, 10 Famous Examples & Tips to Prevent Them* Retrieved from https://secureframe.com/blog/ransomware-attacks

Verizon (2024, April 23) *Verizon 2014 Data Breach Investigations Report Identifies More Focused, Effective Way to Fight Cyber threats* Retrieved from https://www.verizon.com/about/news/verizon-2014-data-breach-investigations-report-identifies-more-focused-effective-way-fight-cyberthreats

Healthcare (Basel) (2020, May 13) *Healthcare Data Breaches: Insights and Implications* Retrieved from https://pmc.ncbi.nlm.nih.gov/articles/PMC7349636/#:~:text=Due%20to%20software%20vulnerabilities%2C%20security,healthcare%20data%20breaches%20%5B8%5D.

Mocanu, M., Shaw-Young, J., & Grigorof, A. (2021, July 7). Threat detection and response in Epic electronic medical record (EMR) environments. *BlueVoyant*. https://www.bluevoyant.com/blog/threat-detection-and-response-in-epic-electronic-medical-record-emr-environments

National Institute of Standards and Technology. (2020**).** *Zero Trust Architecture (SP 800-207)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Federal Information Systems and Organizations (SP 800-53 Revision 5)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

IBM. (2021). Access Management Overview. IBM. https://www.ibm.com/security/identity-access-management

SANS Institute. (2021). *Behavioral Analytics in Insider Threat Detection. SANS Institute.* https://www.sans.org/white-papers/

Center for Internet Security. (2021). *Critical Security Controls for Effective Cyber Defense (Version 8.1*). Center for Internet Security. https://www.cisecurity.org/controls/

Google. (2021). *Multi-factor Authentication for Enterprises*. Google.

https://workspace.google.com/security/2-step-verification/

National Institute of Standards and Technology. (2020). *Cybersecurity Framework (Version 1.1)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162019

BlueVoyant. (2021). *Endpoint Detection & Response Systems*. BlueVoyant. https://www.bluevoyant.com/solutions/edr

MITRE. (2020). The Role of Artificial Intelligence in Cybersecurity. MITRE. https://www.mitre.org/publications

SANS Institute. (2021). *Penetration Testing and Ethical Hacking*. SANS Institute.

https://www.sans.org/cyber-security-courses/penetration-testing/

OWASP. (2021). *Red and Blue Teaming for Cyber Defense*. Open Web Application Security Project.

https://owasp.org/www-project-penetration-testing/