The George Washington University – School of Business

EPIC SYSTEMS CORPORATION
Risk Assessment on the Use of Open Source Software

Information Systems Security

Samuel Akuffo

Lecturer: Dr. Scott White

April 25, 2025

EPIC SYSTEMS CORPORATION

A Risk Assessment on the Use of Open Source Software

Background:

Epic Systems Corporation, a leader in healthcare technology solutions, has been at the forefront of electronic health record development and patient data management since its founding in 1979 (Epic Systems Corporation, 2025). According to the Healthcare Information and Management Systems Society, the healthcare industry faces increasing demands for interoperability, innovation, and cost efficiency (Healthcare Information and Management Systems Society [HIMSS], 2020). This means that the potential use of Open Source Software (OSS) within Epic's ecosystem has become inevitable and a relevant consideration. OSS, characterized by its publicly available code and community-driven development model, offers significant benefits such as enhanced interoperability, reduced development costs, and accelerated innovation. However, its adoption within a highly regulated and security-sensitive industry such as healthcare raises critical concerns. This report analyzes the risks, benefits, and overall suitability of incorporating OSS into Epic's technology stack, drawing from the risk assessment framework established in my previous analyses.

Risk Analysis – Open Source Software Perspective

Threat Assessment:

This analysis identifies four important threats associated with the potential integration of OSS into Epic's operations and systems: Malware Distribution, Supply Chain Attacks, Insider Threats, and Social Engineering. While some of these threats align with those identified in the previous general risk assessment Epic, their significance becomes amplified when considering OSS specifically.

Malware Distribution:

Malware distribution is an important possibility to consider when dealing with OSS. As is widely acknowledged, no software is impenetrable. Even though many OSS projects benefit from peer review, and mature companies like Epic ensure that they only integrate thoroughly vetted and frequently audited OSS, threat actors constantly seek to exploit vulnerabilities, especially in industries like healthcare. This dynamic makes the relationship between defenders and threat actors resemble a perpetual cat-and-mouse chase with no moment of absolute safety.

The open and transparent nature of OSS, while a strength for collaboration, also means that it’s codebase is publicly available to anyone, including malicious actors (Open Web Application Security Project [OWASP], 2023). All it takes is a single line of cleverly inserted code to enable unauthorized access or stealthy monitoring of a system. Given the rise of ransomware, spyware, and advanced persistent threats, the integration of OSS becomes an increasingly risky and uncertain venture when dealing with sensitive and mission-critical data, such as Personal Health Information.

Supply Chain Attacks:

Supply chain attacks deserve separate and specific attention. In the OSS ecosystem, the supply chain consists of the complex web of libraries, modules, and dependencies that a project might have to rely on. Unfortunately, this supply chain is vulnerable and subject to being exploited by threat actors who can compromise popular OSS systems during regular updates (National Institute of Standards and Technology [NIST], 2021).

In Epic's context, this risk is particularly relevant because the company serves a broad network of healthcare organizations, each with varying levels of IT maturity. With OSS, a single compromised component could ripple across Epic's partners and clients, potentially affecting thousands of endpoints. The decentralized nature of OSS maintenance introduces the problem of consistency: Can Epic realistically make sure that all its partners properly handle updates and patches? (NIST, 2021). Even with the provision of guidelines, enforcement across third-party entities is a challenge, increasing the potential for supply chain compromises.

Insider Threats:

Insider threats are also amplified when dealing with OSS. As previously mentioned in Epic’s broader risk assessment, insiders, whether they are malicious or just negligent, represent a credible threat. In the case of OSS, the situation becomes even more complicated. OSS security depends heavily on the vigilance of its community. However, there is no single, centralized certification body that ensures every piece of open-source code is secure (OWASP, 2023).

The sheer volume of OSS available means that no formal organization can realistically audit all packages comprehensively. While widely used OSS may receive attention from security researchers and reputable contributors, what about the countless smaller but functional packages that Epic or its partners might integrate into their system workflows? These packages may be vetted by niche experts whose work, while helpful, may not meet Epic's rigorous security requirements.

Furthermore, the risk of malicious insiders within OSS projects cannot be dismissed. Not every contributor is driven solely by goodwill. Some may intentionally introduce vulnerabilities, backdoors, or code intended to exfiltrate sensitive information. While this scenario may seem extreme, documented cases of malicious commits have surfaced in various OSS projects in the past, such as the SolarWinds Hack and Event-Stream NPM library backdoor, and therefore underscores the real possibility of insiders abusing their roles within the OSS ecosystem (Cybersecurity and Infrastructure Security Agency [CISA], 2021).

Social Engineering:

The intersection between OSS and social engineering is subtle but highly significant. Malicious actors are often motivated by the potential payout, and with Epic handling sensitive healthcare data, the incentive is significantly high. According to Verizon (2023), social engineering is a leading cause of breaches globally and could facilitate the introduction of compromised OSS into Epic's environment.

Consider a scenario where an attacker monitors Epic or one of its subsidiaries, learning of their intent to adopt OSS for a specific project. What would stop such an attacker from cloning a legitimate OSS repository, subtly embedding malicious code, and strategically convincing or luring Epic's procurement or engineering team to use the tampered version? The open-source community largely operates on trust, referrals, and peer validation, which, while generally positive, can also be exploited.

Even well-intentioned developers can be manipulated into recommending compromised code. In OSS, the barrier between trusted and malicious contributions can become a blurred line, especially when urgency, deadlines, or lack of expertise are involved on the receiving end.

Vulnerability Assessment – Open Source Software Perspective

Public Code Exposure & Limited Malware Screening in OSS

The open nature of OSS means that all source code is freely available for anyone to inspect, modify, and use including malicious actors. While this transparency fosters innovation, it also introduces the potential for malware to be subtly embedded within seemingly legitimate code (OWASP, 2023). Despite Epic's best practices and thorough review procedures, identifying a cleverly disguised backdoor or trojanized component is not always so feasible, especially if the malicious logic is buried deep in nested dependencies. The increasing sophistication of malware such as polymorphic code or obfuscated scripts makes malware detection even more challenging. This poses a significant risk to Epic's systems that manage public health information and other sensitive health data.

Exposure: **Moderate**
Severity: **High**

Limited Control over Open Source Software Supply Chains

OSS, by nature, is built and maintained by distributed communities that are beyond Epic's direct control. This creates a situation where Epic is highly dependent on the integrity and security practices of third-party developers. While Epic has mature internal security teams and vetting processes, it is impossible to completely oversee all the OSS supply chain components (NIST, 2021). Epic frequently integrates OSS to support interoperability and emerging technologies and hence, if a compromised dependency is integrated, it could affect core Epic systems and ripple through the entire healthcare network.

Exposure: **High**
Severity: **High**

Inability to Vet Contributor Identities or Intentions in OSS Communities

One of the major vulnerabilities associated with insider threats in OSS is Epic's lack of visibility into who is contributing to the code they might adopt. Unlike internal staff who have to undergo background checks and security training, OSS contributors may remain anonymous or pseudonymous. While community-based peer review is a key strength of open-source development, it also allows for the possibility of bad actors intentionally submitting harmful

code, particularly to less-scrutinized repositories. Epic cannot always distinguish between a helpful update and one with malicious intent, especially when working with large-scale, niche OSS libraries.

Exposure: **Moderate**
Severity: **High**

Informal and Trust-Based OSS Procurement Channels

The process of selecting OSS is often influenced by community trust, peer recommendations, or perceived popularity. In many cases, developers may choose a library based on GitHub stars, user reviews, or advice from open forums rather than a formalized evaluation process (OWASP, 2023). This creates an opportunity for social engineers to distribute modified or malicious versions of OSS by mimicking legitimate projects. An attacker who has identified Epic's technology stack or upcoming projects could specifically target its teams with convincingly presented OSS packages. If integrated without deeper inspection, these could give the threat actors access privileges or data exfiltration capabilities.

Exposure: **Moderate**
Severity: **High**

Overall Risk of Using Open Source Software

The overall risk of adopting OSS within Epic Systems Corporation can be assessed as moderate to high which is contingent on the implementation of rigorous governance controls. Epic's existing technological maturity, robust security posture, and distributed operational structure provide a strong foundation to manage the unique challenges presented by OSS.

The risk associated with OSS is not inherent in its nature but rather in its management, vetting, and integration. Without strong governance, standardized review pipelines, and license compliance checks, exposure could be high. However, with the appropriate protocols, Epic can reduce this risk to manageable levels while still realizing significant benefits. Given Epic's existing capabilities, the successful integration of OSS is achievable, provided that governance remains a top organizational priority.

Ills and Benefits of Using Open Source Software

Benefits:
The adoption of OSS offers significant benefits to Epic Systems. One primary advantage is cost efficiency, as OSS eliminates the need for costly licensing fees, allowing resources to be redirected toward innovation and development initiatives. OSS also provides flexibility and fosters innovation thus enabling Epic to rapidly adapt to emerging technologies such as artificial intelligence, big data analytics, and healthcare informatics. Another critical benefit is interoperability, as OSS supports compatibility with diverse health information systems, aligning directly with Epic's mission to facilitate seamless healthcare data exchange (Red Hat, 2020).

Moreover, OSS helps to avoid vendor lock-in and reduces the risks associated with reliance on proprietary vendors who may delay system updates based on potential financial incentives and

demand. Adopting OSS would also support the health tech workforce by encouraging partner institutions to hire skilled technology graduates for system maintenance and innovation roles. In addition, OSS promotes enhanced transparency. This means that the availability of source code for review by independent security auditors and researchers fosters greater trust among healthcare clients. Finally, OSS contributes to the acceleration of health technology growth by enabling collaborative problem-solving, where diverse contributors work together to solve industry-wide challenges and improve healthcare outcomes.

Ills:

Despite its benefits, the adoption of OSS presents notable challenges. The most significant concern is the security risk of publicly available code which if not properly vetted, may contain hidden malware, backdoors, or vulnerabilities that can be exploited by threat actors. OSS also introduces compliance complexities, as the interpretation and adherence to open-source licensing terms can vary, potentially exposing Epic to legal risks if mismanaged (OWASP, 2023). Another challenge is training requirements, as OSS solutions may require more specialized knowledge and hands-on experience for system administrators compared to commercial proprietary software.

In addition, Epic would likely become an attractive target for hackers, given the potential financial incentives associated with compromising a major healthcare technology provider. Governance related costs also presents a challenge as managing OSS components across a distributed healthcare network would necessitate rigorous tracking, patching, and monitoring protocols, increasing administrative burdens. If not carefully controlled, internal distribution practices could inadvertently lead to license violations, further complicating Epic's compliance posture.

Recommendation

Given both the risks and benefits outlined, Epic Systems should proceed with adopting OSS, but only after establishing a carefully structured and deeply scrutinized governance model. The benefits of OSS, particularly cost savings, flexibility, interoperability and innovation, are closely aligned with Epic's strategic vision for healthcare technology advancement. However, these advantages can only be realized if OSS usage is strictly controlled through comprehensive policies and oversight mechanisms.

Epic should also look to implement a formal OSS adoption policy that includes mandatory security audits and license compliance checks for all OSS components and support strict documentation practices for OSS usage and version control. The policy should also require training programs for procurement and development teams on OSS-related risks, as well as the deployment of internal monitoring tools to track OSS components across all client-facing and internal systems.

This approach will allow Epic to remain competitive, adaptive, and secure while making extensive use of the open-source community to advance the outcomes of healthcare technology.

REFERENCES:

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

Healthcare Information and Management Systems Society. (2020). *Open source health IT*. HIMSS. https://www.himss.org/resources/open-source-health-it

Open Web Application Security Project. (2023). *Open source security*. OWASP. https://owasp.org/www-project-top-ten/

National Institute of Standards and Technology. (2021). *Software supply chain security guidance* (NIST Special Publication 800-218). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-218

Verizon. (2023). *2023 Data breach investigations report* (16th Ed.). Verizon. https://www.verizon.com/business/resources/reports/dbir/

Red Hat. (2020). *Understanding open source software*. Red Hat. https://www.redhat.com/en/topics/open-source/what-is-open-source