The threat actors are cybercriminals who according to ("Cybersecurity spotlight - Cyber threat actors," 2021) are profit driven and target data to sell, hold for ransom, or exploit for their own gain. Cybercriminal's motivation is financial gain or to increase their reputation. The next threat actor is insiders, a current or former employee who has access to the organization's networks, systems, and data ("Cybersecurity spotlight - Cyber threat actors," 2021). Insiders' motivation is to seek revenge or financial gain. Next threat actor is nation-state, an actor that aggressively targets and gain persistent access to public and private sector networks to compromise, steal, change, or destroy information ("Cybersecurity spotlight - Cyber threat actors," 2021). Nation-state actors' motivation according to ("Cybersecurity spotlight - Cyber threat actors," 2021) are Espionage, political, economic, or military. Hacktivist actors are politically, socially, or ideologically motivated to cause change or create publicity by targeting high profile people. Finally, terrorists' organization actors are designated by the U.S. Département of the state. According to ("Cybersecurity spotlight - Cyber threat actors," 2021) These terrorists' organizations usually are disruptive and harassing. Their motivations are propaganda, financial gain, espionage, political or ideological.

The threat actors who would target my scenario are cybercriminals and insiders. Cybercriminals would target the application software for all the data inside that they could profit from by selling the data. Cybercriminals could also attack the application software for reputation purposes as a healthcare firm holds a lot of data. Insiders would target the application software because they could steal all the data and gain profit, or insiders could just steal the data to seek revenge against the organization.

The best way to detect the threat actors in the scenario is to use monitoring, auditing, awareness, and testing. Monitoring collects operational metrics and analyses them to help stop attacks ("Top seven logging and monitoring best practices | Synopsys," 2022). Auditing records information

such as controls, control monitoring, and event information (“Audit Log Best Practices for Information Security,” 2018). This auditing also records and documents destination addresses, source addresses, and timestamps. Awareness, as this helps follow cybersecurity rules, helps improve cybersecurity system, and be wary of insider threats ("Insider threat awareness: What is it, why does it matter, and how can you improve it?," 2021). Awareness would help the healthcare firm catch insider threat actors. Testing would help catch cybercriminals as it helps detect vulnerabilities in the software and security flaws (“Security Testing - Threats, Tools, and Techniques,” 2017).

Legal factors are Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS). These legal factors state that a certain number of employees or those that are in a certain industry have internal and external audits. Industries that are required to do these audits are any organization that handles medical records (Kim & Solomon, 2016). Ethical factors are the organization's security policy that tell the employees what is acceptable and what is not acceptable. Another ethical factor is Communications and other actions specifically banned in your security policy are unacceptable meaning, any action that reveals confidential information is unacceptable, as it could damage the system's integrity or make the system unavailable. Lastly, the healthcare firm might create its own standards based on standards bodies endorsed or developed (Kim & Solomon, 2016).

To counter and respond to cybercriminals and insiders the healthcare firm should use incident handling. Incident handling includes preparation which has an incident response team which will have training and documentation to respond to incidents as they occur (Kim & Solomon, 2016). Incident handling has identification which will find out if the incident is serious or whether it is a common occurrence (Kim & Solomon, 2016). Next step is notification, the goal is to contain the

incident and to improve the situation (Kim & Solomon, 2016). After that step it is to respond to the incident, respond step helps limit the damage by containment. Next step is to do a recovery and follow up which recovery deals with the exploited vulnerabilities before returning to normal use of the system (Kim & Solomon, 2016). Follow up step helps shows what you learned from the incident and how management can react more effectively in the future. Finally, documentation and reporting as this step helps create valuable information to the quality of future incidents. You can improve the incident response plan when you document what actions worked well and those that did not (Kim & Solomon, 2016).

To reduce the likelihood of this happening again the healthcare firm should use security controls. The first step in security controls it to monitoring which reviews and measures all controls to capture actions and changes on the system (Kim & Solomon, 2016). Auditing reviews logs and overall environment to give an isolated analysis of how well the controls and security policies are working (Kim & Solomon, 2016). The improve step in security controls are recommendations for the security program to make improvements and controls in the audit results. Lastly, security ensures controls work together to protect the intended level of security whether new or existing (Kim & Solomon, 2016).

The ramifications of using security controls for the likelihood of another attack is that security controls place limitations on activities that could pose a risk to the healthcare firm. If the healthcare firm does have multiple controls that address the same threat that is fine, but each control needs to address at least one threat (Kim & Solomon, 2016). Another ramification is when you use a control that costs more than the potential loss if a threat is realized, you may be wasting your organization's resources (Kim & Solomon, 2016). The ramifications of incident handling are that if you are flooded by incidents that cannot be assumed due to bad training of

both employees and non-human resources ("Challenges and risks of incident management," 2020).

References

Kim, D., & Solomon, M. G. (2016, October). Fundamentals of information systems security, 3rd edition. O'Reilly Online Learning. https://learning.oreilly.com/library/view/fundamentals-of-information/9781284116465/?sso_link=yes&sso_link_from=SNHU

Security Testing - Threats, Tools, and Techniques. (2017, August 2). Testbytes. https://www.testbytes.net/blog/security-testing-threats-tools-techniques/

Insider Threat Awareness: What Is It, Why Does It Matter, and How Can You Improve It? (2021, April 13). Www.ekransystem.com. https://www.ekransystem.com/en/blog/insider-threat-awareness

Top seven logging and monitoring best practices | Synopsys. (2022, January 24). Application Security Blog. https://www.synopsys.com/blogs/software-security/logging-and-monitoring-best-practices/

Audit Log Best Practices For Information Security. (2018, August 16). Reciprocity. https://reciprocity.com/audit-log-best-practices-for-information-security/

Cybersecurity spotlight - Cyber threat actors. (2021, June 15). CIS. https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-cyber-threat-actors

Challenges and risks of incident management. (2020, December 23). ServiceTonic. https://www.servicetonic.com/itil/challenges-and-risks-of-incident-management/