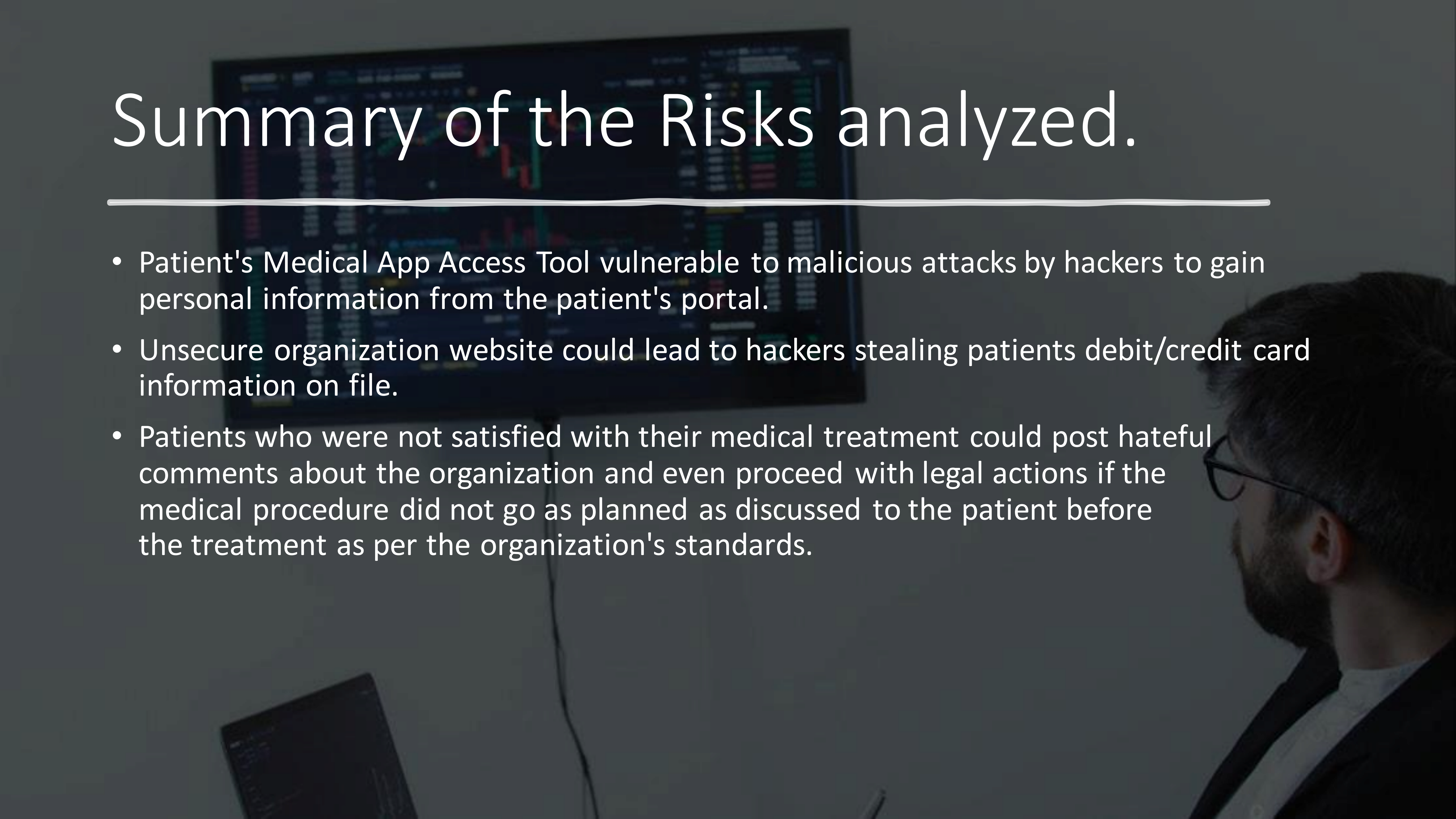
Risk Management & Value To The Organization

Summary

Risk Management is the continuing process to identify, analyze, evaluate, and treat loss exposures and monitor risk control and financial resources to mitigate the adverse effects of loss. More than ever , organizations must balance a rapidly evolving cybersecurity and privacy threat landscape against the need to fulfill business requirements on an enterprise level. Risk management underlies everything that NIST does in cybersecurity and privacy and is part of its full suite of standards and guidelines.

Value To The Organization

- Enable Long term cybersecurity and risk management
- Bridge the gap between the technical and business-side stakeholders
- Flexibility and Adaptability of the Framework
- Built for future regulation and compliance requirements
- Risk management is a vital skill for any organization that wants to achieve its objectives , avoid or reduce losses and seize opportunities.



Summary of the Risks analyzed.

- Patient's Medical App Access Tool vulnerable to malicious attacks by hackers to gain personal information from the patient's portal.
- Unsecure organization website could lead to hackers stealing patients debit/credit card information on file.
- Patients who were not satisfied with their medical treatment could post hateful comments about the organization and even proceed with legal actions if the medical procedure did not go as planned as discussed to the patient before the treatment as per the organization's standards.

Highlights about the Risks Of Concern

1.Patient Medical App Access Tool:

An application attack consists of cyber criminals gaining access to unauthorized areas. Attackers most commonly start with a look at the application layer, hunting for application vulnerabilities written within code. These attacks exploit target both custom code and open-source frameworks and libraries. Because of the impact that both companies and users can experience due to an application attack , securing applications in development and deployment and protecting them once they are in production is crucial .

2.Unsecure Organization Website

- Websites that are not secure are more susceptible to malware and other online risks. If your website is the target of a cyberattack, it may suffer functional issues, be inaccessible to users, or have the personal data of your clients compromised. Reputational damage and lost business are further consequences of cybercrime. According to research, 65% of your clients won't visit your website again if their private information is hacked. Losing clients also means losing money, which can be extremely damaging for small firms.

- Your clients are at risk for fraud and identity theft if their TLS certificate has expired. The certificate helps deter some of the largest online hazards, such as hackers and impostors, in addition to keeping your website free of warning warnings. They accomplish this by authenticating your website and encrypting important data.

- When a customer visits your website, the first thing they see is a warning, they will know right away that your company is unreliable.

3.Unsatisfied Patients filing lawsuits

- The first major drawback is the fact that litigation can be a costly process. Lawsuits will consume not only a significant amount of company funds, but also company time and resources. For smaller businesses, the impact can be particularly devastating. Another major drawback to lawsuits is that it can end up completely damaging the relationship with the parties engaged in it, which can have an impact on future business dealings if the lawsuit involves crucial vendors and suppliers. And last but not least, the public nature of a lawsuit can quickly damage the reputation of a company, causing the public perception to turn, if they choose to side with the other party. Even in situations where court resolutions or settlements are kept private, the initial damage from the announcement of the lawsuit in the media can have a damaging effect that may be hard to recover from. A lawsuit cannot only damage your reputation with the public but can also make other businesses hesitant to work with your company, which can mean a loss of resources vital to business operations.

Pointers to the Risks Found.

- 1.Using instrumentation to embed RASP within an application's source code , security teams have a continuous monitor that sits inside of the application
- 2.Site vulnerabilities can be patched and blocked by using tools like web application firewalls (WAFs), malware scanners, and patching software.
- 3.Earning and maintaining a good reputation can be a significant challenge for both new and established businesses, which makes any negative publicity devastating.

Conclusion to the Report Findings.

- 1.Patient's medical app is vulnerable to malicious attacks which can be solved by Application and Pen Testing and also adding Multi Factor Authentication.(Control: AC-4,CM-3,CM-7)
- 2.Secure Debit/Credit Card Payments can be done by patching the site vulnerabilities and using web application firewalls and also daily monitoring of SIEM.(Control : AU-16,SR-2,SR-6)
- 3.Compliance and training departments work closely to monitor pending legislation(Control : None).

Source List

- https://www.nist.gov/risk-management#:~:text=Risk%20Management%20Framework%20(RMF)&text=The%20NIST%20RMF%20links%20to,%2C%20assessment%2C%20and%20continuous%20monitoring.
- https://www.linkedin.com/advice/1/whats-best-way-demonstrate-value-risk-management
- https://www.cybersaint.io/blog/benefits-of-nist-cybersecurity-framework#:~:text=Enable%20long%2Dterm%20cybersecurity%20and%20risk%20management,posture%20of%20managing%20cybersecurity%20risk.
- https://www.marquette.edu/riskunit/riskmanagement/whatis.shtml
- https://www.contrastsecurity.com/glossary/application-attacks
- https://www.linkedin.com/pulse/consequences-unsecured-business-website-pseudosquare
- https://www.lobbplewe.com/3-concerns-corporate-executives-face-in-2020/