Secure Implementation of ASMIS

Introduction

Queens Medical Centre provides first contact medical services to a rapidly growing community. The accompanying rise in demand for services is overloading the current appointment system which is based on individual phone contact.

The facility management has determined that a technology-based solution is appropriate and has directed implementation of an Appointment Scheduling Management Information System (ASMIS) This system will allow direct interface between patients and the appointment calendar via a web portal and interactive application. This solution addresses the need to reduce demand on the current appointment system which is solely based on human interaction. However, use of an automated system that incorporates internet connections from unverified sources introduces risk. Careful analysis suggests risk for patients, staff, and the organization.

As the web portal access will be open to connection by anyone seeking an appointment and require entry of personally identifying information (PII), it is imperative that system design and deployment include careful analysis of code and connection infrastructure to inform selection and implementation of appropriate controls to eliminate or mitigate risk.

This report addresses the system elements from a cyber-physical viewpoint and provides guidance toward achieving a robust security posture for the system.

Examining the Use Case

Figure 1 presents a system overview from a use case perspective.

The Queens Medical Centre Appointment Scheduling Medical Information System is an automated, interactive system which facilitates patient interface for selecting available appointment times by service and/or provider.

This proposed system will greatly enhance patient experience while providing more efficient and less labor-intensive processes. This is critical given the exponential growth of demand for services.

Implementation of such a system does however introduce expanded risk to patient data, and organizational reputation.

See "Abuse Case Diagram"

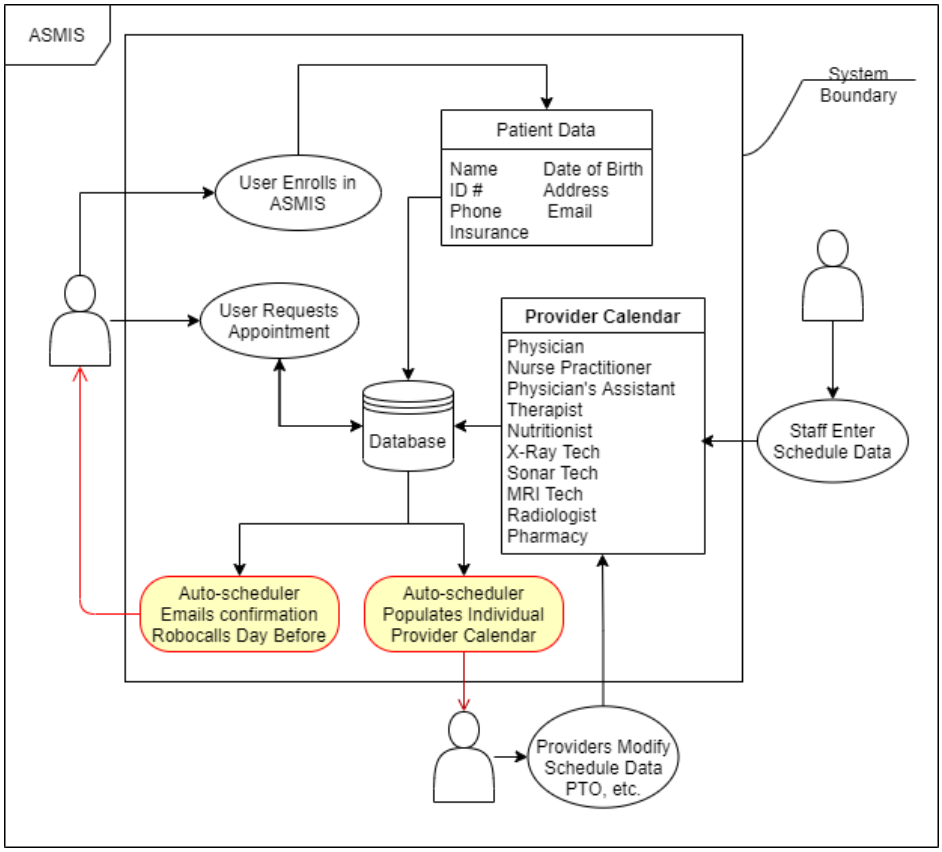

Figure 1

Examining the Abuse Case

Figure 2 provides a visual presentation of where potential abuse cases could be applied to various vulnerability points within the system design. The abuse case must be viewed with an understanding of the use case presented in Figure 1.

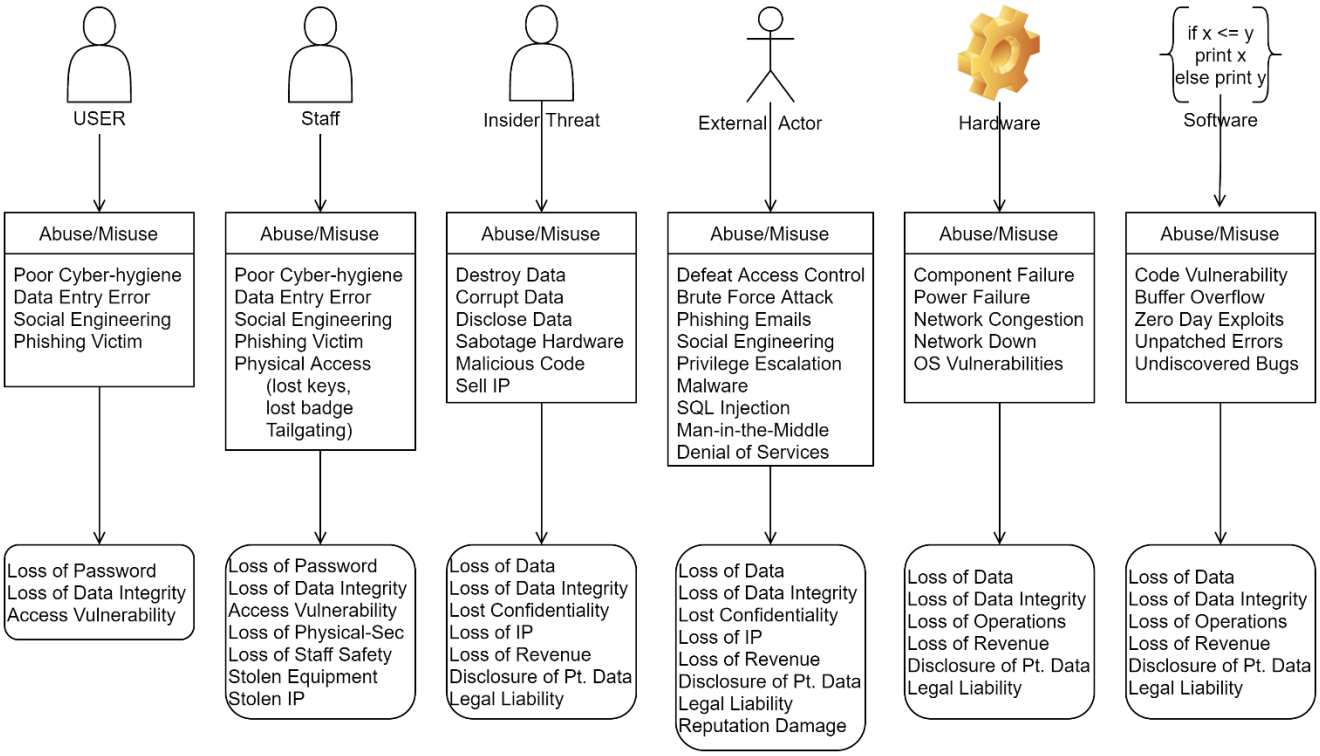

Figure 2 Abuse Case

Examining the Threat Surface and Exploring Resolution Strategies

As can be seen in figure 2, threats to the security and reliability of the ASMIS comprise several categories, including human interface, hardware, and software. Let's examine these from the context of the "big three" foundations of cybersecurity, Confidentiality, Integrity and Availability (CIA). Table 1 presents these threats by type with correlation to CIA, risk factors and controls.

Threat Type	Threat Example	CIA Initial Target	Likelihood	Impact	Recommended Controls (Treatment)	Control Type
Human Element	Social Engineering	C	High	Moderate	Recurrent Training	Administrative
	Phishing	C	High	Moderate	Recurrent Training	Administrative
	Poor Cyber-hygiene	C	High	Moderate	Recurrent Training	Administrative
	Data Entry Errors	I	Moderate	Low	Programming Tools	Technical Control
	Physical Access	CIA	Low	High	Recurrent Training	Administrative
					Surveillance / Alarm System	Physical Control
	Insider Threat	CIA	Low	High	Recurring Audits	Administrative
					Role Based Access	Administrative
Infrastructure (Hardware / Network Connections)	Unmitigated Vulnerabilities (IE: unpatched firewall)	CIA	Moderate	High	ISAC or subscription-based vulnerability management system	Technical Control

					Intrusion Detection / Prevention System (IDS/IPS) & Security Event Incident Management (SEIM)	Technical Control
	Hardware Failure, power outage	A	High	Moderate	Failover Power Backup	Physical Control
	Hardware failure, component failure	A	High	Moderate	RAID drives and network backup storage	Technical Control
Software Based	Access Control Subverted	CIA	Moderate	High	MFA, IDS/IPS, SEIM	Technical Control
	Privilege Escalation	CIA	Moderate	High	AI/ML-based IDS/IPS	Technical Control
	Malware / Ransomware	CIA	High	High	Anti-virus, Anti-malware	Technical Control
					AI/ML-based Monitoring	Technical Control
	Security Bug in Code	CIA	Moderate	High	Security team involved from development stage	Administrative
					Automated security scans of modules and full code	Technical Control
					Deploy in sandbox prior to production	Administrative

Table 1

Proposed Approach to Mitigation of Security Threats/Risk

Risk Assessment – First Steps

The approach to selecting appropriate controls to eliminate or mitigate risk is guided by several factors to be considered by the organization. A critical first step is to document the governance structure for managing risk and implementing system security policies. It is imperative for the executive suite to be a part of establishing this baseline and communicating organization wide, the importance of adherence to established policies and procedures. The CEO, COO, CIO, CFO and General Counsel should all understand their role and accountability in protecting shareholders, staff, and patients. While the day to day responsibility for implementation will fall to IT and security teams, senior leadership must remain engaged and demonstrate continued buy-in to the chosen direction. (ISO 31000, 2018)

Additionally, before strategies for addressing risk can be selected, the risk appetite and risk tolerance of the organization must be established. Risk appetite is the “amount and type of risk that an organization is willing to pursue or retain” (ISO, 2009). Risk tolerance is the “organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives” (IBID). With these characteristics of the company understood, one is prepared to evaluate risk treatment or mitigation based on cost to treat, versus projected cost of non-treatment. Treatment or application of controls can take many forms depending on the cost to benefit ratio and the firm’s risk appetite. A few examples of risk treatment are:

- Avoidance – cease the activity that creates the risk.
- Sharing – distribute the risk with others to reduce each participant’s level of risk.
- Modify Consequences – purchase insurance against risk occurrence.
- Modify Likelihood – reduce likelihood of the risk occurring through mitigating controls, IE: make it more difficult for an actor to exploit the risk.

- Modify Impact – reduce the impact of risk occurrence, IE: daily data backups so that data loss is limited to 24 hours' worth of lost data.
- Acceptance – realization that the risk is not able to be avoided or mitigated within an acceptable cost/benefit ration, and an informed decision to continue the activity or pursuit anyway.

Risk Assessment – Following a Framework

Recent introduction of several risk assessment frameworks has enabled more consistent and repeatable formats for conducting a comprehensive risk assessment as well as selecting the right tools and techniques for treatment of risk. The National Institute of Standards and Technology (NIST) released its Cybersecurity Framework (CSF) for use in the United States. Its use is mandated by Presidential Executive Order 13800 (Trump, 2017) for U.S. Government agencies and owners of critical infrastructure. It is voluntary but recommended for use by private firms.

The NIST CSF has three major elements: "the Core, Implementation Tiers, and Profiles". (NIST CSF, 2018) The Core provides a common lexicon of terminology and activities required to meet cybersecurity goals. The Tiers discuss levels of effort and cost versus risk appetite, providing guidance on appropriate controls. The Profiles assist an organization in establishing and documenting the priorities and goals of their cybersecurity programs. An example of profiles would be "Current State" (as it exists today) and "Target State" (The planned to-be state).

The "Framework Core" also provides five "Functions" as a tool for implementing and managing a full lifecycle cybersecurity program. These are: (NIST CSF, 2018)

- "Identify – Documentation of Asset Management, Business Environment, Governance, Risk Assessment, Risk Management and Supply Chain Risk Management."
- "Protect - Identity Management and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology"
- "Detect - Anomalies and Events, Security Continuous Monitoring, and Detection Processes"
- "Respond - Response Planning, Communications, Analysis, Mitigation, and Improvements."
- "Recover - Recovery Planning, Improvements, and Communications."

The UML Use Case diagram (Fig 1) presented in this report forms a visual basis for "identifying" the assets and business practices to be protected along with the required supporting elements of the ASMIS.

The UML Abuse Case (Fig 2) provides a visual reference for "identifying" the vulnerabilities (risk) that must be protected against.

Table 1 represents the analysis of those risks and suggests potential treatment (controls) for each. These controls represent the "Detect" and "Respond" functions of the framework.

The final function of the framework is "Recover" and should not only include recovery planning but regular practice of recovery actions via exercises, drills, after action reports, recommended improvements and communication of lessons learned and resulting modification to system policy or procedures.

Roadmap to Successful Implementation of ASMIS in a Secure Environment

This document has provided a discussion of the need for and benefits of deploying an ASMIS to improve the patient experience, facilitate staff efficiency and future proof Queens Medical Centre against a growing demand for services. Let us now layout a roadmap of successive tasks which if followed will result in a successful deployment with a sustainable security posture.

- ✓ Engage both senior leadership and security team from project initiation.
- ✓ Base system requirements and design on demonstrated use case modeling, eliminating modules or functions that introduce risk without comparative value or requirement.

- ✓ Conduct baseline and periodic risk analysis throughout system design.
- ✓ Conduct gap analysis to identify need to add staff, infrastructure, or other supporting elements.
- ✓ Ensure adequate allocation of funding for full implementation of ASMIS.
- ✓ Conduct regular, cross-functional team meetings to assess system requirements are met and security reviews are completed.
- ✓ Update risk assessment documentation based on software development cycles and security reviews.
- ✓ Ensure security controls are implemented as part of system deployment and beta testing prior to live rollout to patient population.
- ✓ Follow full-lifecycle management process for continued review and process improvement including:
  - ➢ Security audits of administrative policies and procedures.
  - ➢ Security audits of technology controls for effectiveness, false positives vs. false negatives.
  - ➢ ML/AI based SEIM with integrated IDP/IPS
  - ➢ Ongoing patch management with subscription-based automated vulnerability monitoring and notification.

Critical Review of Proposed Approach to Secure Implementation

Alternative Technologies/Solutions Considered but Rejected

The following technology options or solutions were given consideration but rejected based on accompanying logic.

- Cloud-based, SaaS implementation of ASMIS.
  - This approach while requiring less capital expenditure up-front, brings an ongoing and inflation-influenced operating cost.
  - This approach while minimizing the requirement for new staff also results in outsiders providing first level support to patients, adding risk of negative customer support experience.
  - SaaS limits the organization's ability to make rapid changes to system parameters or affect overrides for special circumstances
  - Cloud-based SaaS typically provides minimal risk sharing beyond basic service level agreements and limits compensation to fees for service.
- Fully outsourced, 3rd party ASMIS.
  - This approach while requiring less capital expenditure up-front, brings an ongoing and inflation-influenced operating cost.
  - This approach while minimizing the requirement for new staff also results in outsiders providing first level support to patients, adding risk of negative customer support experience.
  - This type of service limits the organization's ability to make rapid changes to system parameters or affect overrides for special circumstances
  - This type of service typically provides minimal risk sharing beyond basic service level agreements and limits compensation to fees for service.
- Commercial Off The Shelf (COTS) ASMIS
  - COTS packages preclude involvement of internal security team during development lifecycle. This means that security analysis of the code is minimized to after-the-fact scans.
  - COTS Packages reviewed did not present robust options for customization of access by provider type (role-based access).
  - COTS packages reviewed did not include robust options for customized reports or predictive forecasting.

Confidence in Recommendations

The analysis and conclusions of this report follow the NIST CSF (IBID), consider use case, abuse case, organization risk appetite/tolerance, impact to reputation and patient confidence, resiliency of operations and

cost/benefit ratio. The recommended treatment/controls are appropriate based in the above analysis exercises and the technologies represented while current and relevant are well established and proven effective. Confidence is high that following the recommendations of this report will result in a successful deployment of a new ASMIS within an operating environment that represents a robust cybersecurity protective posture. With buy-in and communicated support by senior leadership, proper application of selected technologies and regular improvement reviews, the system should continue to operate efficiently and securely for the foreseeable future.

Supporting Case Study

Appointment scheduling in health care: Challenges and Opportunities (Gupta and Denton, 2006) presents a case study examining appointment scheduling systems readily available and widely used throughout manufacturing, transportation, and logistics and whether they can be easily adapted to healthcare appointment scheduling needs. A primary conclusion from their study is

> *"It is our position that existing models in the manufacturing, transportation and logistics areas cannot be easily "tweaked" to fit the health care environment, and that this, in part, accounts for the lack of adoption of these models in the health care setting."*

One roadblock to adaptability is the privacy and security requirements inherent in patient data. HIPPA in the U.S. and GDPR in Europe impose privacy restrictions that preclude adoption of these COTS solutions from other industry sectors without extreme modification and security reviews. The cost of these modifications for an "adapted" system is not attractive when compared to similar cost for a targeted development project that delivers a truly custom product with security-by-design.

Conclusion

The decision to develop a full-featured, custom web-based portal for medical appointment scheduling by patients of Queens Medical Centre is well supported and timely in the face of exponential growth. The principles and best practices presented on this report will facilitate a secure environment for successful implementation of this important project.

References

ISO 31000:2018 Risk Management Guidelines, (Chapter5, section 2). Available from https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en [Accessed 4 July, 2021]

ISO Guide:2009, Risk Management Vocabulary (3.7.1.2). Available from https://www.iso.org/obp/ui#iso:std:iso:guide:73:ed-1:v1:en:term:3.7.1.2 [Accessed 4 July, 2021]

Trump, President Donald, J, May 11, 2017. Executive Order # 13800 as published in Federal Register, The Daily Journal of the United States Government. Available from: https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure [accessed 4 July, 2021]

NIST Cybersecurity Framework, February 5, 2018. Available from: https://www.nist.gov/cyberframework/new-framework#components [Accessed 4 July, 2021]

Gupta, D and Denton, B, August 2006. Appointment Scheduling in Health Care: Challenges and Opportunities. Available from: https://btdenton.engin.umich.edu/wp-content/uploads/sites/138/2015/08/Gupta-2008.pdf [Accessed 4 July, 2021]