Cybersecurity Incident Prevention for Telemedicine in gastroenterology

Group 23

Supervisor: Praveen Kumar Donta

Students:

Khondaker Refai Arafat
Samir Hossain Santo Bepu
Golam Sobhani Chowdhury
Pavan Ramesh Gupta
Adit Ishraq
Muhammad Arsalan Khan Mughal

Contents

1. Case study – Local Practice and Problems

Case: (Assignment 4)

Harmony Inside, a healthcare provider for IBS patients, is moving online. It prioritizes the security and privacy of patient data, especially in individual consultations. This work aims to design an artefact that would use past cybersecurity incidents to prevent future breaches by analyzing root causes and generating executable action plans. The study assumes that Harmony Inside has already transitioned to online for all services.

1.1 Local practice

Healthcare services are provided by Harmony Inside, which specializes in providing individualized health consultations for both physical and mental well-being. Patients with IBS can get nutritional and stress-reduction therapies from Harmony Inside, which a few certified dietitians developed. The company recently switched from in-person clinic consultations to an online version. They also provide online courses and a webshop for cookbooks and food supplements for IBD patients. The purpose is to increase client convenience and reach more patients. Security and privacy for patients' data is the utmost priority of Harmony Inside.

A few Key Activities in the practice are as follows:

- Consultation Booking: Clients book appointments through an online portal or mobile app.
- Virtual Consultations: The consultations happen over secure video conferencing, where personal health issues are discussed.
- Data Collection & Management: Patient information, including medical history, symptoms, and consultation notes, are stored and managed digitally.
- Follow-ups and Support: Patients may access follow-up advice and prescriptions via the online portal.

1.2 Stakeholder of local practice and their problems

Stakeholder name	**Action performed by the stakeholders**	**Characteristics of Stakeholders**	**Problems that they can experience in the online business**
Founder dietitians	Providing consultation services to patients, training other dietitians, transforming the company	They are among the few expert dietitians in Sweden. They also have a strong entrepreneurial vision to solve problems for the online system.	They anticipate an increased number of patients in the online version of the practice. Thus an increased risk is relevant to the security and privacy of patients' data.

Stakeholder name	Action performed by the stakeholders	Characteristics of Stakeholders	Problems that they can experience in the online business
Practicing dietitians	Providing consultation services to patients	They are dietitians from all over Sweden, they are trained by Harmony Inside for online consultation.	Not being able to access the system with their account credentials, connectivity issues while providing consultation online, and losing patients' records.
IBS patients worldwide	Getting the following paid services: Online courses individual consultation from dietitians. Purchasing special food products and cookbooks.	From any part of the world. They can be of any age, but mostly elderly.	Not being able to access the system with their account credentials, connectivity issues in the video consultation, their data being exposed to a third party, not being able to access their records
IT and Cybersecurity Team	Managing online systems, solving technical issues, preventing downtime, reporting any IT or information security-related incident, coordinating with third party vendors	Trained in information security-related issues, expertise in system administration and database management	Not having any control over incidents caused by societal factors, not being able to recover the system from severe incidents like data loss
Legal/compliance team	Ensuring legal and regulatory compliance by supporting the executives (founder dietitians)	Experienced in their field	A need to keep updated on the changing landscape of regulations, and law worldwide (Where clients are present).
Third-party vendors	Providing a platform along with security	Market leader for services like cloud infrastructure, SaaS products	Data privacy-related compatibility issues, delay in addressing vulnerabilities.

1.3 Formulation of local problem

Harmony Inside has moved its services online e.g. individual online consultation, online courses, and a webshop for cookbooks and food supplements for IBD patients. They have an incident management system where IT staff reports system-related issues including information security and privacy-related incidents. But there is no mechanism to learn from data-security-related incidents that happened in the past and use the learning to prevent the incidents from happening again or even prevent more severe incidents from happening in the future.

1.4 Justification of the local problem

Severe information security or privacy-related incidents can lead to legal penalties, loss of reputation, and financial losses, ultimately jeopardizing Harmony Inside's operations and patient confidence. Solving this problem before incidents occur will save the organization from future financial, reputational, and operational challenges. Regular learning from minor incidents can prevent larger, more damaging breaches in the future.

By addressing the problem, Harmony Inside can confidently provide secure, private online services that safeguard patient information, ensure regulatory compliance, and foster a trusted relationship with its clients.

2. Knowledge base

This section provides an overview of the relevant literature and fundamental principles for developing an artefact to prevent cybersecurity incidents in telemedicine systems such as that of Harmony Inside. The project aims to address security vulnerabilities in the company's online consultation and data management systems, using knowledge from prior incidents to mitigate risks proactively. In this section, we will summarize the key insights from the literature to inform the design and implementation of the artefact.

Definitions:

Telemedicine: "Telemedicine is a term used to provide remote healthcare to patients without the need for in-person encounters. … Telemedicine includes multiple subtypes such as telemonitoring (patients wearing mobile devices and reporting to their providers about symptoms/disease progression), tele-education (webinars, interactive sessions provided to providers or patients or both), teleconsultation (remote ICU care, ED consultation), and telecare (video interaction to simulate a face-to-face visit in order to assist in diagnosis and treatment)." (Perisetti & Goyal, 2021)

Telehealth: "Telehealth is a broader term that includes a wide range of methods used to communicate with patients using video portals and telephonic communication." (Perisetti & Goyal, 2021)

2.1 Background: Challenges in Cybersecurity Incident Management in Healthcare

The healthcare industry faces heightened vulnerability to cybersecurity incidents due to the sensitive nature of patient data and a complex regulatory environment. Studies have demonstrated that data breaches in healthcare can result in severe consequences, such as loss of trust, financial penalties, and operational disruptions (Seh et al., 2020). For organizations like Harmony Inside, which manages sensitive patient data during online consultations, ensuring robust data security is a top priority.

Existing literature emphasizes healthcare organizations' challenges in securing their online platforms, particularly as they expand into telemedicine and other digital services (AlOsail, Amino, & Mohammad, 2021). The transition to virtual consultations and digital health records has significantly increased the attack surface for cyber threats, highlighting the need for effective incident prevention mechanisms and a structured approach to cybersecurity.

2.2 Learning from Minor Incidents and Root Cause Analysis

Many organizations, including those in healthcare, often fail to learn from past cybersecurity incidents, particularly smaller or "near-miss" events. While these incidents may be less severe, they offer valuable insights that can help prevent more significant breaches in the future (Sheikhtaheri, 2014). Analyzing both major and minor incidents is essential to identifying patterns and addressing root causes of security vulnerabilities. For Harmony Inside, the lack of a formal system to analyze minor incidents has been identified as a critical issue. Implementing a root cause analysis (RCA) system to capture data from these events can assist the organization in detecting recurring problems and preventing future breaches. RCA is crucial because it allows organizations to

go beyond managing symptoms and focus on resolving fundamental issues that cause security breaches, such as technical flaws or human error (Peters & Eng, 2021).

2.3 Barriers to Effective Knowledge Sharing and Organizational Learning

One of the most significant barriers to improving cybersecurity in organizations is the lack of effective knowledge sharing between incident response teams and upper management. Research indicates that communication gaps often lead to underreporting or improper documentation of incidents, which hampers the organization's ability to learn from these events (Oweidat et al., 2023). For Harmony Inside, a well-structured communication system is essential to ensure that incident reports are effectively shared across the organization. This approach would allow both management and technical teams to collaborate on implementing preventive measures. Additionally, the system should address common organizational challenges, such as the reluctance to report incidents due to fear of blame (Lawton & Parker, 2002).

2.4 Incident Prevention Strategies and Best Practices

Literature on incident prevention identifies several best practices that could be incorporated into the artefact design for Harmony Inside. One key strategy is integrating automated systems capable of analyzing incident data in real-time and providing actionable insights to prevent future breaches (Chernyshev, Zeadally, & Baig, 2019). This is especially important in healthcare settings, where regulatory requirements mandate strict data protection measures. In addition to automated analysis, continuous staff training on cybersecurity risks is crucial. Research indicates that human error is often a major contributor to data breaches, particularly in healthcare, where employees may lack sufficient understanding of cybersecurity protocols (Liginlal, Sim, & Khansa, 2009). Incorporating educational tools into the artefact will help address this issue by improving staff awareness and reducing the likelihood of security incidents caused by human behavior. Finally, regular security audits and assessments are necessary to ensure that the artefact remains effective. These audits can identify emerging vulnerabilities as technology evolves and ensure ongoing compliance with legal standards (Herzig & Walsh, 2020).

2.5 Application to Harmony Inside

The insights from the literature provide a solid foundation for designing the cybersecurity artefact for Harmony Inside. The artefact will integrate root cause analysis, behavior-based prevention strategies, and continuous learning mechanisms to create a comprehensive solution for preventing data breaches. By focusing on technical and human factors, the artefact will address the unique challenges of securing sensitive patient data online.

3. Research Process

3.1 Overview of the research process

The phases of the research process had been as follows:

3.1.1 Explicating the problem and analysis of existing solutions

In this phase, we precisely formulated the local problem by reviewing and analyzing recorded interview with the founders of one healthcare provider - Harmony Inside. We also justified the need to address the problem for Harmony inside. The justification was also supported by research on the problem in general practice - telehealth or telemedicine. We also researched to analyze the existing solutions for the generic problems. Literature of type case study and qualitative analysis were reviewed for research for generic practice and problem.

3.1.2 Eliciting the Requirements

In this phase, we identified the type of the artefact and how that might be integrated with the local practice's information system and operations. We identified the functional and non-functional requirements of the artefact that can address the problem. A recorded interview with the CTO of one healthcare provider - Harmony Inside was reviewed. Literature of type case study and qualitative analysis were also reviewed.

3.1.3 Designing the Artefact

In this phase, we designed an outline of the artefact. We got some ideas for the second part (Incident Prevention Playbook) of the artefact from the literature. One relevant source is SOTER: A Playbook for Cybersecurity Incident Management (Onwubiko & Ouazzane, 2020). The detailed design of the artefact is beyond the scope of this design research.

3.1.4 Implementation plan

In this phase, we planned how the artefact would be implemented and installed in the system of Harmony Inside. Interview with Harmony Inside founders and IT support was planned to be conducted. Questionnaires were also planned to be used to collect information from the IT support.

In our plan, we considered compatibility with the existing system and the security of the whole system after attaching the RCA module. We also emphasized the training of the IT support, testing, and fixing iterations before doing the final evaluation of the implemented artefact.

3.1.5 Demonstration and Evaluation Plan

In this phase, we planned how the artefact would be evaluated and demonstrated in front of the stakeholders of Harmony Inside. We considered both qualitative and quantitative metrics for the evaluation. We identified six metrics that could be measured for the evaluation. To allow us to measure some of the metrics, we added some non-functional requirements for the artefact in this stage to support the evaluation.

Questionnaires were decided to be used to collect the qualitative evaluation metrics from IT support of Harmony Inside. Literature was reviewed suggesting qualitative analysis. For quantitative metrics, RCA module logs and reports, and IT support feedback were planned be used as source of data.

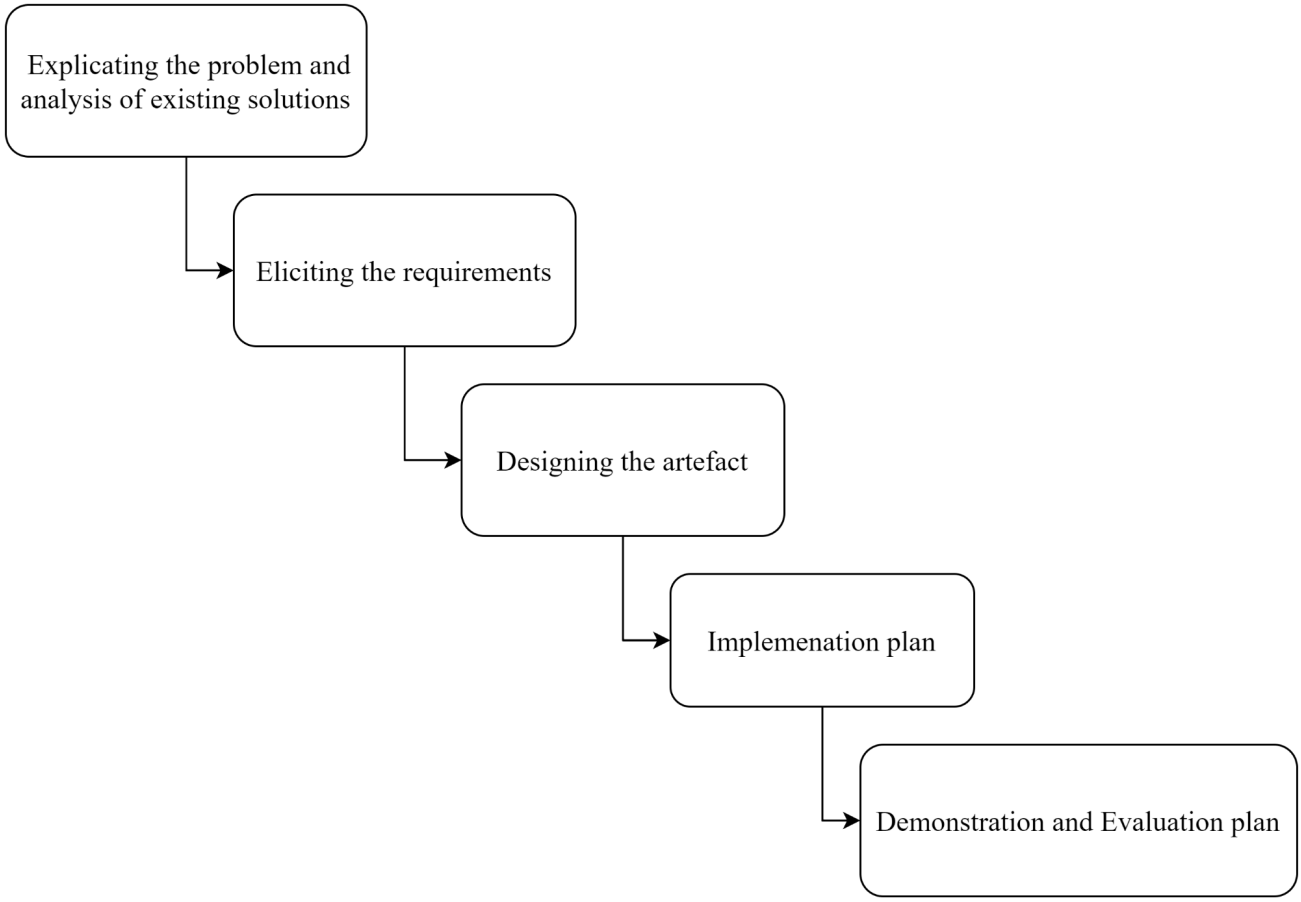

Fig 3.1 The phases of the design research (The arrow shows the dependency between phases, but not a temporal dependency; we did multiple iterations through the phases)

3.2 Research Strategies and Methods

The following table summarizes the method types used in each phase. The details are mentioned in chapter 2 and chapter 4.

Phase\method	Interview (Harmony Inside founders, IT support)	Questionnaires (Harmony Inside founders, IT support)	Case study (type of Literature review)	Qualitative Analysis (type of Literature review)	Literature Review (type of Literature review)
Explicating the problem	Yes	No	Yes	Yes	Yes
Eliciting the requirements	Yes	No	Yes	Yes	No
Designing the artefact	Yes	No	No	No	Yes
Implementation plan	Yes	Yes	No	No	No
Demonstration and Evaluation plan	Yes	Yes	No	Yes	No

4. Generic Practice and Problem

Practice: Harmony Inside currently provides dietary and nutritional consultations specifically for IBS patients, with dietitians delivering services after hospitals have diagnosed patients. As the practice has shifted to an online model, it can be expanded to offer 'total healthcare' for Gastrointestinal (GI) patients, including those with IBS, IBD, or other chronic GI diseases. This expanded model would encompass services from primary diagnosis and drug prescription to lifelong personalized dietary and lifestyle consultations. Telemedicine in gastroenterology surged by 4000% during COVID-19, largely due to the relaxed rules from the CMS (Centers for Medicare and Medicaid Services) (Perisetti & Goyal, 2021). While telemedicine improved care and minimized exposure risks, it also introduced challenges, including reduced patient contact, lower reimbursements, and concerns over data privacy and system security. For successful adoption, secure technology, provider training, and solutions for patient engagement—particularly for elderly or tech-challenged individuals—are crucial.

In a generalized setting like Harmony Inside's potential expansion, security and privacy concerns must be rigorously addressed. This level of generality is chosen because the telemedicine system requirements for various types of GI patients are likely to be quite similar. On the other hand, supporting even a broader group of patients could introduce additional features, increasing system complexity.

Problem: Telemedicine systems for GI patients do not have an automated system or a mechanism in the design that can suggest how to prevent severe cybersecurity incidents based on small occurrences.

4.1 The Main Activities in the Generic Practice

The generic practice for online healthcare services, particularly those focused on GI patients, typically involves

1) Remote consultations via video or phone: Conduct video visits for conditions like irritable bowel syndrome, chronic abdominal pain, and post-procedure monitoring.
2) Disease monitoring and management: Using platforms like IBD Qorus, HealthPROMISE, and myIBDcoach to track disease progression and improve adherence in IBD patients.[1]
3) Medication adjustments: Adjust biological therapy, corticosteroids, and anti-inflammatory agents for IBD patients via telemedicine.
4) Patient education and counseling: Providing education on disease management and lifestyle modifications through tele-education platforms.
5) Coordination with primary care and specialists: Facilitating discussions between primary care providers and GI specialists on one platform to improve care coordination.

[1] Described in Appendix A: Glossary

4.2 The Stakeholders of the Practice and Their Problems

Stakeholder name	Action performed by the stakeholders	Characteristics of Stakeholders	Problems that they can experience in the online business
Healthcare Providers	Conduct consultations, manage patient data, prescribe treatments	Specialized in IBS treatment, varying levels of tech-savviness	Data security and privacy issues during online consultations; Adapting to new technologies, and managing increased patient load without compromising data security
GI Patients	Seek consultations, share health data, follow treatment plans	Diverse age groups, varying tech skills, concerned about privacy	Not being able to access the system with their account credentials, connectivity issues in the video consultation, their data being exposed to a third party, not being able to access their records
IT Staff	Manage systems, ensure security, and provide technical support	Skilled in healthcare IT, cybersecurity expertise	Data synchronization across various systems while ensuring security and privacy.
Administrators	Oversee operations, ensure compliance, manage resources	Knowledge of healthcare regulations, business management skills	Ensuring regulatory compliance across jurisdictions, staff training and support to ensure security from social engineering attacks, managing operational costs within the budget limitations
Third-party Service Providers	Provide technical infrastructure, data storage solutions	Expertise in cloud services, data management	Ensuring interoperability, ensuring that server capacity and bandwidth can handle peak usage times without degradation of services.

4.3 Justification of the Generic Problem

The inability to learn from past cybersecurity incidents in incident management is a common and critical issue, affecting sectors such as IT, healthcare, and industry. Many research and case studies highlight that many organizations struggle to capture and apply lessons from previous incidents, which leads to the recurrence of

similar or even more severe problems in the future. Here's a summary of the main challenges contributing to this issue:

Failure to Translate Experience into Action: Handling security incidents allows many businesses to gain invaluable experience, but they frequently fall short of translating this knowledge into useful insights. Usually, inadequate communication between incident response teams and more general security management causes this kind of failure by impeding organizational learning (Ahmad, Maynard, & Shanks, 2015).

Knowledge Gap: In many cases, organizations lack a structured process for gathering and sharing information from incidents. For example, a Chinese healthcare organization struggled to integrate incident data into its security processes, causing recurring issues due to poor knowledge-sharing practices (He & Johnson, 2017)..

Underreporting and Communication Barriers: It is frequently not possible to report situations completely and transparently due to social and organizational impediments. As a result, the organization's true security position is not fully understood. It is imperative to remove these obstacles to enhance incident handling and learning procedures (Sveen, Rich, & Jager, 2007).

Missed Learning Opportunities: In high-risk sectors, organizations collect data on past failures to prevent future crises. However, despite having access to this data, many fail to learn from smaller incidents that could help avert larger disasters. Incident reporting systems are crucial for transforming individual incidents into collective knowledge that can be used to prevent future occurrences (Maslen & Hayes, 2016).

Organizations often prioritize resolving immediate technical issues during incidents, which can overshadow the long-term opportunity to learn from the event. This short-term approach leads to missed insights that could improve future security strategies. A comprehensive review of both major and minor incidents is vital for building more effective systems in the future (Ahmad, Hadgkiss, & Ruighaver, 2012).

In summary, incidents leave behind important information that can help prevent similar situations in the future. However, many organizations struggle to derive meaningful lessons from past events due to poor communication, inadequate knowledge-sharing platforms, and a narrow focus on quick fixes. To address these challenges, it is essential to implement reliable systems that gather, record, and share lessons from each incident. Additionally, organizational reporting barriers must be addressed, a process that incorporates lessons from every known incident should be established, and validation and verification must be conducted through in-depth reviews of all incidents to prevent future issues.

4.4 Existing solutions

Ensuring strong security measures is essential in the rapidly evolving field of telehealth to safeguard confidential patient information and maintain patient trust. Numerous investigations have explored innovative ways to enhance security in this area. Telehealth platforms with advanced security features, such as multi-factor authentication, encrypted messaging, and end-to-end encryption, have been introduced to promote trust in telehealth services while protecting patient information during virtual consultations (Spagnuelo et al., 2013).

In a complementary approach, comprehensive cybersecurity training programs for healthcare providers, including dietitians, have been proposed. These programs aim to enhance providers' ability to recognize and

respond to potential security threats. By equipping providers with practical strategies, such training significantly reduces the risks associated with telehealth consultations (Jerry-Egemba, 2024).

The significance of patient education initiatives in telehealth has also been emphasized. Resources have been developed to guide patients through the online consultation process, offering advice on maintaining privacy and recognizing phishing attempts. This approach empowers patients to take an active role in enhancing the security of telehealth services (Almathami, Win, & Vlahu-Gjorgievska, 2020).

A proactive approach to detecting and addressing system vulnerabilities has been promoted through routine security audits and assessments in healthcare institutions. Regular assessments can ensure that the latest security procedures are followed, thereby preventing data breaches and boosting patient trust in online care (Gómez et al., 2022).

Collaboration between cybersecurity specialists and healthcare professionals is also crucial. Given the constantly changing nature of cyber threats, the suggestion for partnerships to create incident response plans and conduct ongoing security assessments is particularly relevant. This cooperative strategy can help healthcare organizations maintain a strong security posture and regulatory compliance (He et al., 2022).

Finally, integrated compliance management systems have been proposed to assist healthcare firms in navigating complex regulatory obligations. These systems allow providers to deliver safe, high-quality telehealth services while ensuring robust protection of patient data by aligning security measures with compliance initiatives (Bincoletto, 2019).

5. Drafting an Artefact

5.1 Artefact type

The type of the artifact would be a combination of an instantiation and a method: A root cause analysis system and A playbook. The root cause analysis system would be integrated with the incident management system. Based on the root cause, an IT support personnel will be able to use the playbook to generate an 'Action Plan' containing possible steps, e.g. troubleshooting, educational training, etc. The action plan also explains the reasoning, i.e., what kind of risk the system has predicted.

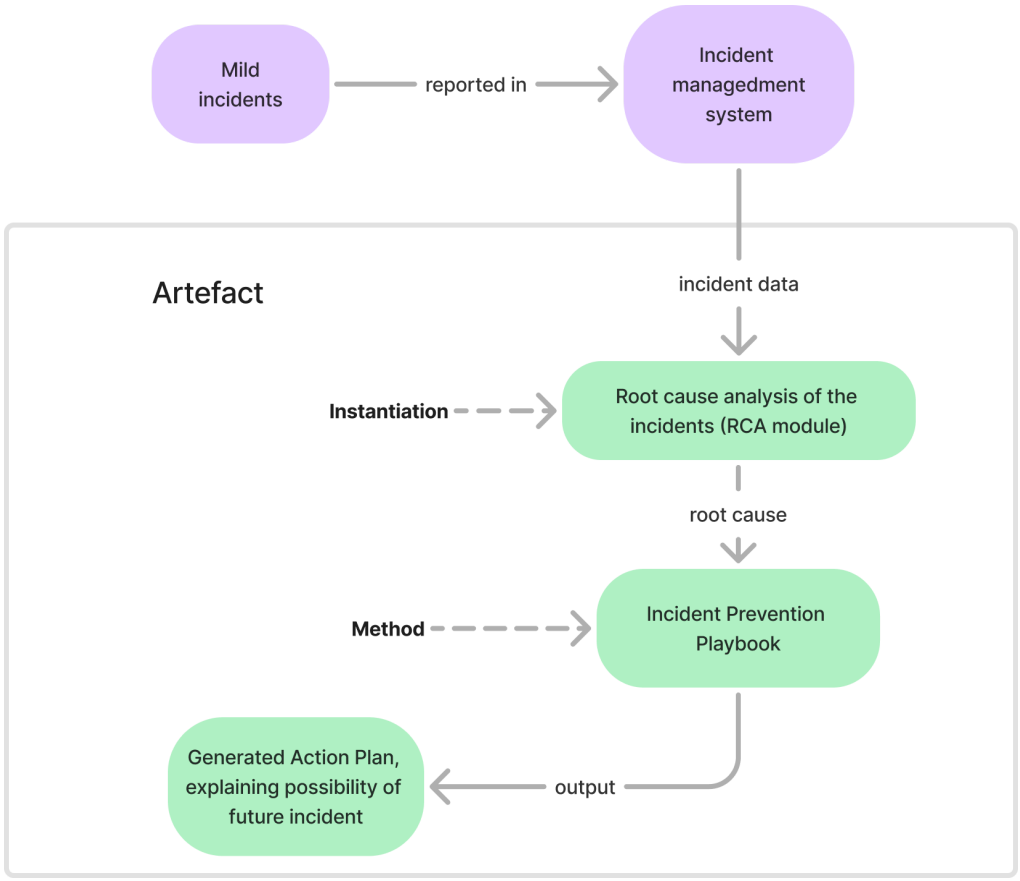

Figure 5.1: Integration of Root Cause Analysis with an Incident Management System and the role of a Playbook for Incident Prevention

5.2 Requirements

Requirement	Functional/ nonfunctional	Justification - relation to the goal/problem or to practice/stakeholders
Should be Integrated with the existing incident management system	Functional	Necessary to ensure the smooth incorporation of the new artefact without disrupting existing processes. Directly impacts operational continuity.
Incident data should be collected for analysis	Functional	Required to gather and analyze minor incidents to predict and prevent severe incidents.
It should do the root cause analysis from the gathered data	Functional	Required to narrow down the possible causes that can help to generate an action plan.
It should provide detailed steps in the form of an action plan.	Functional	The action plan is the outcome of the artifact, it would say what needs to be done to prevent severe incidents e.g. educating a group of users about social engineering.
It will generate logs showing the number of incidents identified, and the processing time of an incident to find the root cause.	Non-functional	Would be required for evaluation of the artefact
It will generate one report showing the number of incidents analyzed finding the root cause(s) vs the total number of incidents analyzed	Non-functional	Would be required for evaluation of the artefact
It should comply with healthcare regulations	Nonfunctional	Ensures that the system complies with global healthcare and data protection regulations, supporting the legal team's needs.

It should have a low additional cost for integration	Nonfunctional	To be affordable within the budget limitations of the stakeholders, especially the third-party vendors and the IT team.
The playbook shall comply with the CIA triad.	Nonfunctional	The playbook must be only modified by authorized people, it must be viewed by chosen roles and must be available at all times.

5.3 Artefact outline

The proposed artefact consists of two main components: a **Root Cause Analysis (RCA) module** and a **Prevention Playbook**.

The RCA module integrates with the existing incident management system and analyzes data from past cybersecurity incidents to identify root causes. It focuses on understanding user behavior patterns and societal factors contributing to security incidents.

The Prevention Playbook is a large set of rules and decision trees written in natural language. Given a root cause, an IT support staff can generate customized action plans by going through the playbook.

Taking root cause from the RCA module and with the help of the Prevention Playbook, IT support personnel deduce actionable plans. These plans include:

- Immediate mitigation steps
- Long-term preventive measures
- Educational content for staff and patient training
- Recommended system updates or configuration changes
- Strategies to address societal and behavioral factors

The artefact functions as follows:

1. Incident data is collected and fed into the RCA module
2. RCA module analyzes the data, focusing on user behavior and societal factors
3. The RCA module provides the root cause information as input to the Prevention Playbook
4. Prevention Playbook helps to create a customized action plan, emphasizing education and behavioral changes
5. IT security staff acts based on the generated Action plan

This structure allows for a comprehensive approach to incident prevention, combining user behavior and societal factors analysis with tailored response strategies. The focus on education and behavioral changes aims to create a more secure environment by addressing the human element of cybersecurity.

Example usage of the prevention playbook:

Given - Root Cause: An employee fell victim to a phishing attack by clicking on a malicious link in an email that appeared to be from the IT department, resulting in the compromise of their credentials.

It would generate the following 'Action Plan':

1. Immediate Response:
    - Reset the affected employee's credentials
    - Conduct a thorough scan of the employee's system for malware
    - Monitor the compromised account for any suspicious activity
2. Investigation:
    - Analyze the phishing email to identify its characteristics and origin
    - Review email logs to determine if other employees received similar emails
    - Check for any data exfiltration or unauthorized access attempts
3. Employee Education:
    - Conduct a company-wide refresher training on phishing awareness
    - Create a simulated phishing campaign to test and reinforce employee vigilance
    - Develop and distribute a quick reference guide for identifying phishing attempts
4. Technical Measures:
    - Implement or enhance email filtering rules to catch similar phishing attempts
    - Enable multi-factor authentication for all employee accounts
    - Deploy an endpoint detection and response (EDR) solution on all company devices
5. Policy Updates:
    - Revise the incident reporting procedure to encourage prompt reporting of suspicious emails
    - Implement a policy requiring IT to use a standardized format for system-wide communications
    - Establish a protocol for verifying the authenticity of requests for sensitive information
6. Ongoing Monitoring:
    - Implement regular security assessments to identify potential vulnerabilities
    - Set up alerts for unusual login attempts or account activities
    - Conduct periodic reviews of email security measures and their effectiveness
7. Communication:
    - Issue a company-wide alert about the incident without identifying the affected employee
    - Provide clear instructions on how to report suspicious emails or potential security breaches
    - Share lessons learned and best practices with all employees
8. Follow-up:
    - Schedule a review meeting after 30 days to assess the effectiveness of implemented measures
    - Adjust the action plan based on feedback and any new insights gained
    - Plan for quarterly phishing simulations to maintain employee awareness

This action plan addresses the immediate security concern, implements preventive measures, enhances employee awareness, and establishes ongoing processes to mitigate future social engineering risks. It takes a comprehensive approach by combining technical solutions with human-focused strategies to create a more resilient security posture against social engineering attacks.

5.4 Expected Effects on the Stakeholders

Effect	Positive/ negative	Healthcare Providers	GI Patients	IT Staff
Improved incident prevention	Positive	Reduced risk of data breaches, enhanced patient trust	Increased confidence in data security	A more proactive approach to security management
Need for additional training	Negative	Time investment required to learn new security practices	Time investment for security awareness training	Additional workload to implement and manage new processes
Enhanced security awareness	Positive	Better understanding of security risks and prevention	Improved ability to protect personal data	Reduced workload from user-caused incidents
Initial implementation effort	Negative	Potential disruption to workflow during implementation	Possible temporary inconvenience during system updates	Increased workload during the integration phase
Improved user behavior	Positive	Reduced risk of human-error-related incidents	More secure practices when using telehealth services	Fewer user-related security issues to manage

5.5 Ethical Consideration

Implementing this solution raises several ethical considerations:

1. **Data privacy**: The system will analyze incident data, which may contain sensitive information. Ensuring this analysis doesn't compromise patient confidentiality is crucial.
2. **User autonomy**: Balancing the need for security with respect for user autonomy in how they interact with the system.
3. **Transparency**: Stakeholders should be informed about how the system works and make decisions to maintain trust and allow for accountability.
4. **Equitable implementation**: Ensuring the system benefits all patients equally, regardless of their technological literacy or access.
5. **Behavioral monitoring**: Ethical implications of monitoring and analyzing user behavior for security purposes.
6. **Continuous evaluation**: Regular ethical audits should be conducted to assess the system's impact on patient care, privacy, and user experience.

5.6 Novelty - Comparison with the Existing Solutions

Solution name	Focus on User Behavior	Customized Prevention Strategies	Integration with Existing Systems	Emphasis on Societal Factors	Healthcare -Specific
Our solution	High	Yes	High	High	Yes
Traditional SIEM	Limited	No	Moderate	No	No
Generic IRP software	Limited	Limited	Low	No	No
Healthcare-specific security tools	Moderate	Limited	Moderate	Limited	Yes

Our solution differs from existing ones in several key aspects:

1. User Behavior Focus: Unlike traditional Security Information and Event Management (SIEM) systems, our solution emphasizes understanding and improving user behavior to prevent incidents.
2. Customized Prevention Strategies: While generic Incident Response Plan (IRP) software may offer templated responses, our system generates tailored action plans based on specific incident data and behavioral patterns.
3. Integration: Our solution is designed to seamlessly integrate with existing healthcare IT systems, providing a more cohesive approach than standalone security tools.
4. Emphasis on Societal Factors: Unlike most existing solutions, our system considers broader societal factors that may influence security risks in healthcare settings.
5. Healthcare-Specific: The artefact is tailored to the unique needs and regulations of the healthcare industry, unlike generic cybersecurity tools.

This novel approach combines behavioral analysis, customized response generation, and healthcare-specific features to provide a more comprehensive and proactive security solution for telehealth providers.

6. Metrics and Ways of Measurement

The methods to measure the performance of the artefact toward solving the problem are as follows:

Metric Name	Description	Source of Data/Information	Way of Measuring
Percentage of incidents identified successfully	It would show the performance of the RCA module.	RCA Module of the artefact	Review the logs of RCA module
Percentage of incidents analyzed successfully	It would show the performance of the RCA module. An incident is analyzed successfully if it finds the root cause.	RCA Module of the artefact	Review the relevant report of RCA module
Response Time	The average time is taken from incident received by the RCA module to action plan deduction by the user using the playbook.	RCA Module Logs, User (IT support) Feedback	The log would tell how much time it takes to find the root cause, and the user (IT support) would note down how much time it takes to go through the playbook given a root cause until an action plan is identified
Health-care provider Satisfaction	Average satisfaction rating from staff (IT, support providers, admin) with the incident management process with the artefact	Staff Surveys & Feedback Forms	Distribute and collect surveys among staff during evaluation and quarterly after launch
Patient Satisfaction	Satisfaction level of patients acting in response to any request from IT support based on the playbook	Patient Surveys & Feedback forms	Digital surveys and online feedback form analysis during evaluation and quarterly after launch.
Ease of Process	Evaluation of the ease and efficiency of the artefact	IT support Interviews & Feedback	Conduct structured interviews and collect feedback.

The questions for interviews/surveys are presented in Appendix B

7. Demonstration

7.1 Implementation plan

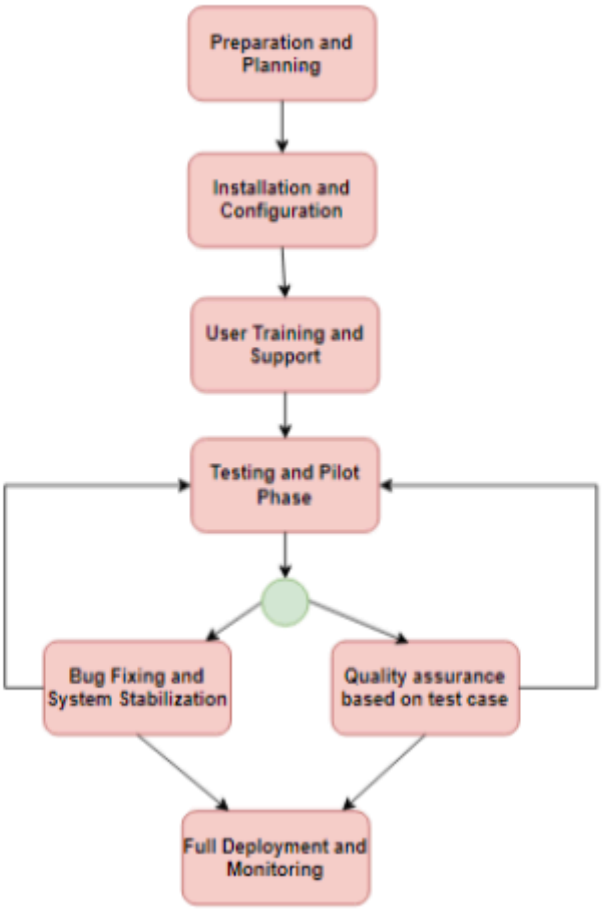

Fig 3. The figure illustrates the Phases of the System Implementation and Testing Process.

Preparation and Planning:

The team will review current IT systems, software, and cybersecurity measures to identify integration points. They will ensure compatibility between the artifact and existing systems. Key stakeholders will be involved in gathering specific requirements and feedback.

Installation and Configuration:

The Root Cause Analysis (RCA) module will be integrated into Harmony Inside's servers. Secure connections and authentication protocols will be set up to protect patient data and comply with healthcare regulations.

User Training and Support:

Comprehensive training will be provided to different stakeholders, including IT staff and healthcare providers, focusing on understanding the functionalities of the RCA module and proper use of the Prevention Playbook.

Testing and Pilot Phase:

Rigorous tests will be conducted to ensure the artifact functions as intended and integrates smoothly with the existing incident management system. The system will be rolled out in a controlled environment to monitor performance and gather feedback data. Necessary adjustments will be made based on observations and user feedback.

Bug Fixing and System Stabilization:

Any bugs found during the testing phase will be fixed with proper documentation.

Quality Assurance Based on Test Case:

The quality will be checked based on test cases, such as the number of incidents detected or how incidents are categorized. After passing the quality standards, test reports will be sent to stakeholders before deployment.

Full Deployment and Monitoring:

The artifact will be deployed across all systems and healthcare services at Harmony Inside. Monitoring mechanisms will be established to track artifact performance, data protection efficiency, and user satisfaction.

7.2 Evaluation Plan

To assess the effectiveness of the implemented artefact at Harmony Inside, we will use a combination of quantitative and qualitative metrics over six months following full deployment.

Quantitative Metrics

1. Percentage of incidents identified and analyzed successfully:
    - Data Source: RCA Module logs and reports
    - Measurement: Monthly review to calculate successful identification and analysis rates
    - Used for: RCA module
2. Response Time:
    - Data Source: RCA Module logs for analysis time and IT support feedback for Playbook usage.
    - Measurement: Calculate the average time from incident detection to action plan creation weekly
    - Used for: RCA module and the playbook combined (whole artefact)

Qualitative Metrics

1. Healthcare Provider Satisfaction:
    - Data Source: Staff surveys and feedback forms
    - Measurement: Quarterly surveys among IT staff, healthcare providers, and administrators
    - Used for: RCA module and the playbook combined (whole artefact)
2. Patient Satisfaction:
    - Data Source: Patient surveys and feedback forms
    - Measurement: Quarterly digital surveys to assess satisfaction with security measures
    - Used for: RCA module and the playbook combined (whole artefact)
3. Ease of Process:
    - Data Source: IT support interviews and feedback
    - Measurement: Bi-monthly structured interviews with IT support staff
    - Used for: RCA module and the playbook combined (whole artefact)

Evaluation Process

1. Establish baselines before full deployment (example in a table below)
2. Collect data according to specified intervals
3. Use collected data for continuous improvement
4. Compile final evaluation report after six months, comparing results to baseline and initial targets

Metric	Description	Baseline	Target
Percentage of incidents identified successfully	Performance of the RCA module in identifying incidents	70%	95%
Percentage of incidents analyzed successfully	Performance of the RCA module in finding root causes	60%	90%
Response Time	Average time from incident receipt by RCA module to action plan deduction	3 days	1 hour
Stakeholder (from Harmony Inside) Satisfaction	Average satisfaction rating from staff with the incident management process	3.5/5	4.5/5
Patient Satisfaction	Satisfaction level of patients responding to IT support requests based on the playbook	75%	90%
Ease of Process	Evaluation of the ease and efficiency of the artefact	3/5	4.5/5

table 7.1: example baseline for performance metrics

This evaluation plan will provide a comprehensive assessment of the artefact's performance, its impact on Harmony Inside's cybersecurity posture, and its effects on various stakeholders.

7.3 Expected effects

7.3.1 Positive Effects

Stakeholder	Effect	Explanation
Healthcare Providers	Reduced sense of risk of data breaches	Improved data security measures and real-time monitoring will minimize the occurrence of data breaches.
Healthcare Providers	Enhanced Confidence and Trust on the system	Healthcare providers will gain confidence in the system's ability to secure patient information, leading to improved patient-provider trust.
IT and Cybersecurity Team	Proactive Incident Management Capability	The artefact's automated RCA module will help the team quickly identify and mitigate potential threats, reducing manual intervention.
IT and Cybersecurity Team	Efficiency Gains in incident response	Well-designed playbook and root cause analysis software reduce the manual effort needed to address minor incidents.
GI Patients	Improved Experience of Data Security	Patients will experience better privacy protection, increasing their confidence in using telehealth services.
GI Patients	Enhanced Service Continuity	By reducing cybersecurity incidents, the system will provide more reliable access to healthcare services.
Administrators	Compliance Assurance Capability	The artifact ensures adherence to regulatory standards HIPAA, and GDPR, reducing legal and financial risks.
Administrators	Operational Efficiency	The reduction in incidents and quick response times will optimize resource allocation and reduce costs.

7.3.2 Negative Effects

Stakeholder	Effect	Explanation
Healthcare Providers	Training Time Investment	Providers may need to dedicate time to undergo training, potentially reducing the time available for consultations during the initial phase.
Healthcare Providers	Initial Adjustment Period	Providers might face temporary disruptions while adapting to the new system features and security protocols.
IT and Cybersecurity Team	Increased Workload During Implementation	The IT team will need to allocate extra resources to support the initial integration, bug-fixing, and user training phases.
GI Patients	Temporary Disruptions in Service	Patients might experience minor inconveniences during system updates or initial implementation phases.
Administrators	Resource Allocation for Training and Support	Administrators will need to allocate resources for continuous training and support programs for staff and patients.

8. Synopsys

8.1 Design Science Canvas (reduced)

<table>
<tr><th colspan="3">Practice</th></tr>
<tr><td colspan="3">The practice is telemedicine for Gastrointestinal (GI) patients. The purpose of the practice is to provide total healthcare for GI patients, including those with IBS, IBD, or other chronic GI diseases. The main activities in the practice are remote consultations, disease monitoring, medication adjustments, patient education, and care coordination between primary care providers and GI specialists. The stakeholders are healthcare providers, GI patients, IT staff, administrators, and third-party service providers.</td></tr>
<tr><th>Problem</th><th>Requirements</th><th>Artefact</th></tr>
<tr><td>Telemedicine systems for GI patients do not have an automated system or a mechanism in the design that can suggest how to prevent severe cybersecurity incidents based on small occurrences.

Addressing the problem is important because, severe information security or privacy-related incidents can lead to legal penalties, loss of reputation, and financial losses, ultimately jeopardizing the company’s operations and patient confidence. Solving this problem before incidents occur will save the organization from future financial, reputational, and operational challenges.</td><td>Functional:
- should be Integrated with the existing incident management system.

- Incident data should be collected for analysis
- It should do the root cause analysis from the gathered data
- It should provide detailed steps in the form of an action plan.

Non-functional:
- It will generate logs showing the number of incidents identified, and the processing time of an incident to find the root cause.
- It will generate one report showing the number of incidents analyzed finding the root cause(s) vs the total number of incidents analyzed
- It should comply with healthcare regulations
- It should have a low additional cost for integration
- The playbook shall comply with the CIA triad.</td><td>The type of the artifact would be a combination of an instantiation and a method: A root cause analysis system and A playbook. The root cause analysis system would be integrated with the incident management system. Based on the root cause, an IT support personnel will be able to use the playbook to generate an ‘Action Plan’ containing possible steps, e.g. troubleshooting, educational training, etc.</td></tr>
<tr><th colspan="3">Research Process</th></tr>
<tr><td>To explicate the problem, an interview with the founders of one such healthcare provider -</td><td>To elicit the requirements of the artefact, an interview with the CTO of one such healthcare provider - Harmony Inside was conducted.</td><td>While designing the artefact, an interview with the founders of one such</td></tr>
</table>

Harmony Inside was conducted. Literature of type case study and qualitative analysis were also reviewed.	Literature of type case study and qualitative analysis were also reviewed.	healthcare provider - Harmony Inside was conducted. A literature describing the concept of an ‘incident management playbook’ was reviewed.
For the implementation plan, Interview with Harmony Inside founders and IT support was planned to be conducted. Questionnaires were also planned to be used to collect information from the IT support. In our plan, we considered compatibility with the existing system and the security of the whole system after attaching the RCA module. We also emphasized the training of the IT support, testing, and fixing iterations before doing the final evaluation of the implemented artefact.	For demonstration and evaluation plan, questionnaires were decided to be used to collect the qualitative evaluation metrics from IT support of Harmony Inside. Literature was reviewed suggesting qualitative analysis. For quantitative metrics, RCA module logs and reports, and IT support feedback were planned be used as source of data.	
Comments		
The quntitative metrics for evaluation were: Percentage of incidents identified successfully, Percentage of incidents analyzed successfully, and Response Time. The qualitative metrics for evaluation were: Stakeholder (from Harmony Inside) Satisfaction, Patient Satisfaction, Ease of Process		

8.2 Implementation Canvas (reduced)

Business case (local practice)	
Harmony Inside, a healthcare provider for IBS patients, has recently moved all their services to online. It prioritizes the cyber security in all the services including consultation booking, virtual consultation, patient data management, patient follow ups and support, online courses, and a webshop for cookbooks and food supplements for IBD patients.	
Problems in local practice (instantiation of the generic problem)	**Instantiation of the Artefact (adjustment, configuration, etc.)**
Harmony Inside has an incident management system where IT staff reports system-related issues including information security and privacy-related incidents. But there is no mechanism to learn from data-security-related incidents	The RCA module is a software system collected from a vendor, it integrates with the existing incident management system of Harmony Inside and analyzes

that happened in the past and use the learning to prevent the incidents from happening again or even prevent more severe incidents from happening in the future.	data from past security incidents to identify root causes. The Prevention Playbook is adapted for Harmony Inside. Given a root cause, an IT support staff can generate customized action plans by going through the playbook. Taking root cause from the RCA module and with the help of the Prevention Playbook, IT support personnel deduce actionable plans. These plans include: Immediate mitigation steps, long-term preventive measures, educational content for staff and patient training, recommended system updates or configuration changes, strategies to address societal and behavioral factors
Implementation plan	**Evaluation plan**
1. Review systems and gather requirements 2. Integrate RCA module and configure security 3. Train users on functionality and usage 4. Conduct tests and pilot phase 5. Fix bugs and stabilize system 6. Perform quality assurance 7. Deploy fully and monitor performance	1. Measure quantitative metrics (incident analysis rates, response times) monthly 2. Assess qualitative metrics (staff and patient satisfaction, ease of use) quarterly 3. Establish baselines pre-deployment 4. Collect and analyze data regularly 5. Use findings for ongoing improvements 6. Compile final report after six months, comparing results to baselines and targets
Expected Positive Effects of the Artefact	
On health-care providers: Reduced sense of risk of data breaches, Enhanced Confidence and Trust on the system's ability to secure patient information On IT and cybersecurity team: Proactive Incident Management Capability, Efficiency gain in incident response On GI patients: Improved Experience of Data Security, Enhanced Service Continuity. On Administrators: Compliance Assurance Capability, Operational Efficiency.	

8.3 Synopsis

Background

Online healthcare providers specializing in Gastrointestinal (GI) patient care have transitioned their services to digital platforms. This shift necessitates robust cybersecurity measures to protect sensitive patient data during various online interactions, including consultations and data management.

Problem

The primary challenge faced by online GI healthcare providers is the absence of an automated system capable of learning from minor cybersecurity incidents to prevent more severe breaches. This gap poses risks to patient data security and could lead to legal and reputational damage.

Research Question

How can an integrated system be designed to effectively analyze minor cybersecurity incidents and generate actionable insights to prevent future severe incidents in an online healthcare setting for GI patients?

Method

The research employs a design science approach, incorporating literature reviews, stakeholder interviews, and case studies to develop an artefact. This artefact combines a Root Cause Analysis (RCA) system with a Prevention Playbook tailored to the specific needs of online GI healthcare providers.

Result

The proposed artefact successfully integrates with existing incident management systems to analyze incident data and produce detailed action plans. It emphasizes user behavior analysis and societal factors influencing cybersecurity risks in the context of online GI healthcare services.

Discussion

Implementing this solution enhances the ability of online GI healthcare providers to manage cybersecurity proactively. By focusing on both technical and human factors, the artefact not only addresses immediate security concerns but also fosters a culture of continuous learning and improvement in cybersecurity practices for telehealth services in gastroenterology.

This synopsis outlines the key elements of the research, focusing on the generic practice of online GI healthcare and the associated cybersecurity challenges, without specific reference to Harmony Inside.

9. Reflection on our work

Completing this project has been a comprehensive learning experience, individually and as a group. Our work on developing the Cybersecurity Incident Prevention Playbook for Harmony Inside has deepened our understanding of various design science concepts, particularly in the context of socio-technical systems. Additionally, we have gained valuable insights into the specific business domains of online healthcare, incident management, and cybersecurity in healthcare organizations.

Individually, the most significant learning came from understanding the complexity of designing socio-technical systems. Healthcare cybersecurity is a challenging domain where technical artefacts, like incident management systems, are deeply embedded in a broader social and organizational environment. The relationship between technical systems and human actors—dietitians, IT staff, patients, and administrators—made it clear that cybersecurity challenges cannot be resolved solely through technology. Understanding how social dynamics, user behaviors, and organizational rules influence the security landscape has been crucial.

Root Cause Analysis (RCA) concepts and learning from minor incidents stood out as pivotal. These concepts helped me appreciate that minor incidents often contain valuable data, which, if analyzed correctly, can prevent larger breaches. This perspective shifted my focus from addressing only the technical flaws to considering the human factors and social interactions that often contribute to security vulnerabilities.

Another key takeaway was a better understanding of the design science research methodology, which focuses on creating artefacts to solve real-world problems. This methodical approach allowed me to structure our project around the iterative development of the artefact, ensuring that each project phase was built on the previous one. By continuously refining the artefact based on literature reviews and feedback, I learned the importance of flexibility and adaptation in the design process.

We encountered challenges and opportunities that contributed to our collective learning as a group. One major challenge was coordinating our work across different disciplines, including cybersecurity, healthcare, and software design. Each member brought a unique perspective to the project, and this diversity enriched the final artefact design. By distributing responsibilities based on our strengths, we managed the workload efficiently.

Our group divided the tasks as follows:

- **Golam Sobhani Chowdhury and Samir Hossain Santo Bepu** focused on the technical aspects, such as designing the Root Cause Analysis system and the Prevention playbook.
- **Khondaker Refai Arafat and Pavan Ramesh Gupta** concentrated on researching healthcare cybersecurity frameworks and ensuring compliance with data privacy regulations.
- **Adit Ishraq and Muhammad Arsalan Khan Mughal** handled the literature review and knowledge base, synthesizing key findings from research into the artefact design.

Regular communication and collaboration were essential. We conducted weekly meetings to align on our progress, and any conflicts regarding design choices were resolved through discussion and consensus. This collaborative approach not only helped us refine the artefact but also improved our ability to work as a cohesive unit, particularly in a complex, interdisciplinary project.

As a group, we gained a deeper appreciation for how technical artefacts function within socio-technical systems. The project's complexity increased as we realized the necessity of balancing technical security measures with human-centric considerations, such as user behavior, knowledge sharing, and regulatory compliance. This complexity required us to design a system that is technically sound and adaptable to the unique behaviors and needs of the healthcare providers and patients at Harmony Inside.

We found that understanding stakeholder roles and perspectives was critical to the success of the artefact. In this regard, the literature on socio-technical systems guided us to ensure that our solution was comprehensive and considered the different interests of dietitians, patients, IT staff, and administrators.

Key takeaways from this project include the realization that technology alone cannot solve security issues in socio-technical systems like healthcare. Human behavior and organizational dynamics are equally important. We also learned the value of proactive incident management through RCA, shifting our focus from reactive solutions to preventive strategies. Additionally, the need for continuous refinement of our design reinforced the importance of flexibility in responding to feedback and changing security threats. Overall, this project has prepared us to tackle future challenges in similar contexts, especially those that involve complex interactions between technical systems and human factors. Our collaborative, multidisciplinary approach throughout the project strengthened our teamwork and led to a more effective, well-rounded solution.

References

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams–Challenges in supporting the organisational security function. *Computers & Security*, 31(5), 643-652.

Almathami, H. K. Y., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Barriers and facilitators that influence telemedicine-based, real-time, online consultation at patients' homes: systematic literature review. *Journal of Medical Internet Research*, 22(2), e16407.

AlOsail, D., Amino, N., & Mohammad, N. (2021). Security issues and solutions in e-health and telemedicine. In *Computer Networks, Big Data and IoT: Proceedings of ICCBI* 2020 (pp. 305-318). Springer Singapore.

Bincoletto, G. (2019). A data protection by design model for privacy management in electronic health records. In *Privacy Technologies and Policy: 7th Annual Privacy Forum, APF 2019, Rome, Italy, June 13–14, 2019, Proceedings 7* (pp. 161-181). Springer International Publishing.

Chernyshev, M., Zeadally, S., & Baig, Z. (2019). Healthcare data breaches: Implications for digital forensic readiness. *Journal of medical systems*, 43, 1-12.

Gómez, J., Olivero, M. Á., García-García, J. A., & Escalona, M. J. (2022). A Practical Experience Applying Security Audit Techniques in an Industrial Healthcare System. In *Illumination of Artificial Intelligence in Cybersecurity and Forensics* (pp. 1-20). Cham: Springer International Publishing.

He, Y., & Johnson, C. (2017). Challenges of information security incident learning: an industrial case study in a Chinese healthcare organization. *Informatics for Health and Social Care*, 42(4), 393-408.

He, Y., Zamani, E. D., Lloyd, S., & Luo, C. (2022). Agile incident response (AIR): Improving the incident response process in healthcare. *International Journal of Information Management*, 62, 102435.

Herzig, T., & Walsh, T. (2020). *Implementing information security in healthcare: Building a security program*. CRC Press.

Jerry-Egemba, N. (2024, January). Safe and sound: Strengthening cybersecurity in healthcare through robust staff educational programs. In *Healthcare Management Forum* (Vol. 37, No. 1, pp. 21-25). Sage CA: Los Angeles, CA: SAGE Publications.

Lawton, R., & Parker, D. (2002). Barriers to incident reporting in a healthcare system. *BMJ Quality & Safety, 11(1)*, 15-18.

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, 28(3-4), 215-228.

Maslen, S., & Hayes, J. (2016). Preventing black swans: Incident reporting systems as collective knowledge management. *Journal of Risk Research*, 19(10), 1246-1260.

Onwubiko, C., & Ouazzane, K. (2020). SOTER: A playbook for cybersecurity incident management. *IEEE Transactions on Engineering Management*, 69(6), 3771-3791.

Oweidat, I., Al-Mugheed, K., Alsenany, S. A., Abdelaliem, S. M. F., & Alzoubi, M. M. (2023). Awareness of reporting practices and barriers to incident reporting among nurses. *BMC Nursing,* 22(1), 231.

Perisetti, A., & Goyal, H. (2021). Successful distancing: telemedicine in gastroenterology and hepatology during the COVID-19 pandemic. *Digestive diseases and sciences,* 66(4), 945-953.

Peters, H., & Eng, P. (2021). Root Cause Analysis (RCA) for the improvement of healthcare systems and patient safety. CRC Press.

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020, May). Healthcare data breaches: insights and implications. *In Healthcare* (Vol. 8, No. 2, p. 133). MDPI.

Sheikhtaheri, A. (2014). Near misses and their importance for improving patient safety. Iranian journal of public health, 43(6), 853-4.

Spagnuelo, D. P., Martina, J. E., Custódio, R. F., & Andrade, R. (2013). Multi-factor authentication in telemedicine systems. In *The Fifth International Conference on EHealth, Telemedicine, and Social Medicine*. IARIA.

Sveen, F. O., Rich, E., & Jager, M. (2007). Overcoming organizational challenges to secure knowledge management. *Information Systems Frontiers,* 9, 481-492.

10. Appendixes

Appendix A: Glossary

IBD Qorus:

A learning health system developed by the Crohn's & Colitis Foundation to improve quality of care for adults with inflammatory bowel disease (IBD). It enables rapid data-sharing between physicians and patients to define, measure and improve the quality of IBD care. IBD Qorus incorporates standardized care pathways and quality metrics reported directly by patients.

HealthPROMISE:

A mobile health platform developed to improve quality of care and quality of life for patients with inflammatory bowel disease. It allows patients to track symptoms, medications, and quality of life measures, and share this information with their healthcare providers. The platform aims to facilitate patient engagement and shared decision-making.

myIBDcoach:

A telemedicine system developed for monitoring and managing all subtypes of inflammatory bowel disease. It allows patients to regularly report on their disease activity, symptoms, medication use, and quality of life through a web-based or mobile application. The system provides personalized feedback and education to patients, while also alerting healthcare providers about potential issues.

Appendix B: Interview questions for measurement of the qualitative metrics

Healthcare Provider Satisfaction

Interview questions for staff (IT, admins):

Q1. How satisfied are you with the new incident management process?

Q2. What aspects of the new system do you find most helpful?

Q3. Are there any areas where you think the system could be improved?

Survey questions for IT security staff:

Q4. On a scale of 1-5, how satisfied are you with the new incident management process? (1 being very dissatisfied, 5 being very satisfied)

Q5. How has the new system affected your ability to handle security incidents? (Much worse, Somewhat worse, No change, Somewhat better, Much better)

Patient Satisfaction

Interview questions for patients:

Q6. How comfortable do you feel with the security measures in place for your online consultations?

Q7. Have you noticed any changes in the way security-related concerns are handled?

Survey questions for patients:

Q8. On a scale of 1-5, how satisfied are you with the security measures for your online consultations? (1 being very dissatisfied, 5 being very satisfied)

Q9. How would you rate your experience when responding to security-related requests from IT support? (Very poor, Poor, Average, Good, Excellent)

Ease of Process

Interview questions for IT support:

Q10. How would you describe the ease of use of the new artefact?

Q11. What aspects of the artefact do you find most efficient?

Q12. Are there any parts of the process that you find challenging or time-consuming?

Survey questions for IT support:

Q13. On a scale of 1-5, how easy is it to use the new artefact? (1 being very difficult, 5 being very easy)

Q14. How would you rate the efficiency of the new process compared to the previous one? (Much less efficient, Somewhat less efficient, No change, Somewhat more efficient, Much more efficient)