INFORMATION SECURITY STRATEGY DEVELOPMENT

A practical overview report for regulated environments

Prepared by

Samuel Boadi Agyekum

London, United Kingdom

Email | LinkedIn | GitHub

Repository: github.com/agyekumboadi/information-security-strategy-playbook

Release tag: v1.0-verification-snapshot

Developed during MSc studies at Arden University (UK)

This overview summarises key risks, recommended controls, and verification artefacts

Abstract

The aim of this paper is to provide an overview of Unique Quality Care (UQC), a private home care provider, which is registered under the Care Quality Commission (CQC) with a 'Good' rating and follows the Health and Care Act 2022. UQC's staff should be educated and trained to identify intrusions and loopholes, and how to detect them when they occur. Employees and management should information security strategies to maintain a secure workflow within the organization and its resources, including the Birdie mobile application used by employees and management to document clients care history. In addition, the causes of attacks are elaborated as well as was to mitigate such occurrences within the company at large.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Care Quality Commission (CQC)

Commercial Off The Shelf (COTS)

Health and Social Care Information Centre (HSCIC)

Information Commissioner's Office (ICO)

International Organization for Standardization (ISO)

Mandatory Access Control (MAC)

Personal Protective Equipment (PPE)

Role-Based Access Control (RBAC)

Rule-Based Access Control (RuBAC)

1.0 Introduction

Sensitive data protection is more important than ever in the current digital era. For people, businesses, and governments alike, having strong information security policies is essential given the increase in cyber threats and data breaches. The techniques and resources employed by hostile actors to undermine information security are becoming more complex as technology develops. To demonstrate the crucial role information security methods play in protecting sensitive data in a connected society, this essay will analyse the significance of information security strategies and look at practical solutions to reduce risks.

1.1 Methodology

1.2 Software Acquisition Models

Software acquisition involves three methods: Commercial Off the Shelf (COTS), Custom-made software, and Open Source Software. COTS is readily available, custom-made software is tailored to specific groups, and Open Source Software is accessible for modification (Blodgett & Phair, 1992).

Advantages	Disadvantages
They are affordable : It is relatively easier less expensive to acquire since it more centred for mass usage.	It can be more expensive over time: although it may be less expensive at initial stages, costs may be incurred over.
Easy to use and implement: after downloading or buying a package, you can use it instantly without any special implementation.	The availability of older versions of Off-the-Shelf Software is contingent on vendor preferences, necessitating users to upgrade to the latest version.

Table 1: Advantages and disadvantages of COTS (personal collection)

Advantages	Disadvantages
It is flexible to use: since this development is tailored to meet organisation or personal needs, it is often centred to meet workflow of such user or organisation.	It involves higher cost to acquire: a high investment is required to develop and implement this software although it may pay off in long term and solve organisational needs if it is well planned.
Easy to work with: since features are not bulky unlike other acquisition models, it is relatively easy to use.	It takes much time to develop and deploy: software development process required to complete custom made software phases is lengthy. It can take months to several years to complete entire phase as well as to deploy prototypes before the actual usage.

Table 2: Advantages and disadvantages of Custom-made software (personal collection)

Cost is less: open-source software's are free or low cost for licensing and accessing all features.	Difficulty of usage: some open source software may be complex setting up and use and may lack user-friendly features
Easy to customize: you can manipulate and amend source code to fit specific needs although there may be certain limitations it can achieve specific goals.	Device incompatibilities: some open source software need specific system requirements in order to run and set up.

Table 3: Advantages and disadvantages of Open Source Software (personal collection)

Birdie, a healthcare technology mobile app company, was established in 2017 to improve homecare for older adults and their caregivers. The app tracks carers' activities, including medication, health status, surroundings, and assistance, in real-time as shown in Figure 1. Carers can log in and out of the app based on proximity to the client's location, and management can create weekly rotas for carers. The app also helps drivers know the location and time spent at the client's residence, enabling them to pick up the carer for their next call. Birdie's innovative approach to homecare is a testament to its potential to enhance the quality of life for older adults and caregivers.

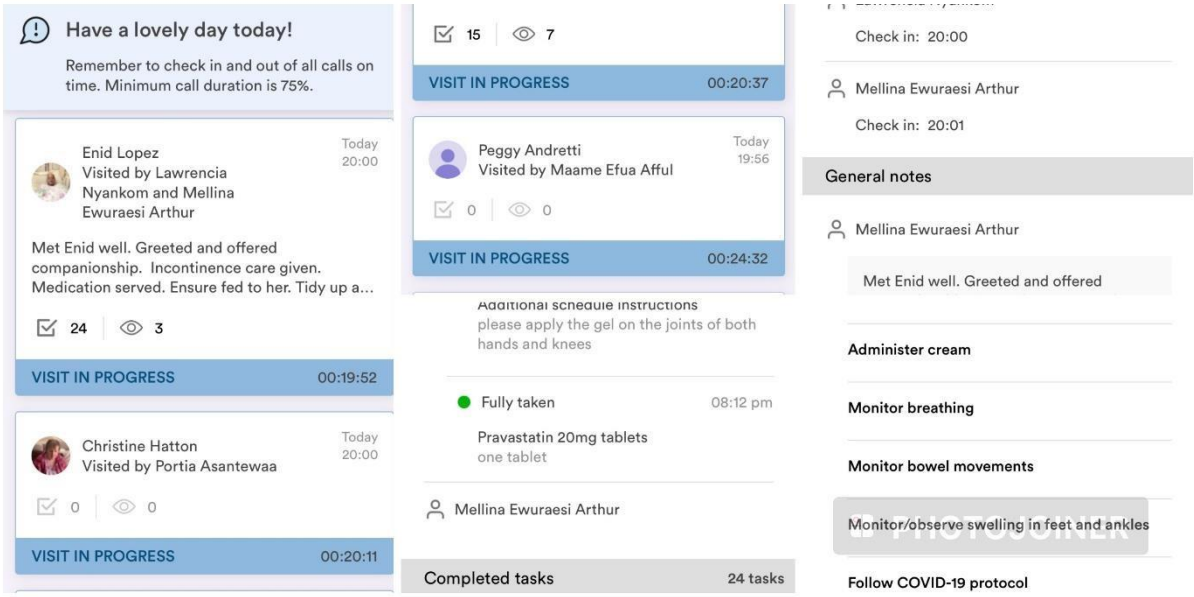

Figure 1: Birdie Mobile Application Interface for Employees **(Birdie Care, 2023).**

Advantages	Disadvantages
Real-time access for management to oversee activities at clients residence.	It involves much cost for UQC to deploy Birdie.
The system allows real-time monitoring of clients' health conditions and sends notifications of lateness of carers to management's backend dashboard.	The carers dashboard only displays a few past activities, making it challenging for them UQC to track previous activities and client health progress.
Birdie's Technical Support Team utilizes feedback from management and carers to enhance the existing system, providing carers with knowledge of previous activities and guidance for new carers.	The app does not allow for the recording of Personal Protective Equipment (PPE) at clients' residences, causing carers to be informed when they reach clients' end.

Table 4: The advantages and disadvantages of Birdie app to UQC (personal collection)

1.3 Security Strategies, Policies and Procedures

Unique Quality Care (UQC), a private home care provider, is registered under the Care Quality Commission (CQC) with a 'Good' rating and follows the Health and Care Act 2022. CQC is responsible for registering health and elderly social care providers, monitoring their safety, taking legal actions, and educating good practices to improve healthcare (Care Quality Commission, 2016). They have a handbook outlining policies and procedures for activities, safety, and handling data from various sources. CQC focuses on three principles for managing information: confidentiality, integrity, and availability. These principles ensure service users personal data are kept safe and used securely, accurate, and available within the organization.

1.3.1 Evaluation of Security Strategies and Legal Issues In Handbook

The handbook at CQC outlines security strategies and legal issues for monitoring network activities within the organization and service users, focusing on International Organization for Standardization (ISO) 27001 Standards to manage information security based on individuals, procedures, and technologies (Bhuyan *et al.*, 2022). These security strategies at CQC is geared towards five areas;

1. **Infrastructure/Framework and IT Security**: Atos and Computacenter maintain server centres, assess IT security, and test infrastructure functionalities monthly. They also conduct assessments at regional offices to ensure hardware, software, and networks are safe from unauthorized users, adhering to Canadian health information systems (Culot *et al.*, 2021).
2. **Security Education and Awareness/Realisation Training**: Regular training is mandatory for employees to reduce risks in the workplace, including accessing shared essentials. Intranet reminders under 'Security Matter' and desktop security packages are installed on computers and iPads to protect against unauthorized software launches and malicious links in emails (Care Quality Commission, 2016).
3. **Governance and Risk Management:** The Executive Director of Strategy and Intelligence as the Senior Information Risk Owner, and Chief Inspector of Hospitals, Caldicott Guardian, together with management, deliberate on risk assessment and action plans at internal governance meetings (Care Quality Commission, 2016).
4. **Legislation Compliance:** CQC adheres to legal legislation on information security, including Data Protection 1998 and ISO 27001 standards (Culot *et al*., 2021). To prevent data breaches, CQC has a designated point for employees to learn about data violations and security queries. Additionally, CQC is required to produce a code of conduct under section 80 of the Health and Social Care Act 2008, ensuring data acquisition, management, and confidentiality. Regular assessments of data compliance are conducted to ensure compliance with the law.
5. **Assurance:** The Information Commissioner's Office (ICO) and Health and Social Care Information Centre (HSCIC) set demands for Information Governance, and the CQC evaluates

measures issued by the Governments' 10 steps to Cyber Security at an internal level (Such *et al.*, 2015). These assessments ensure compliance with set of demands and standards.

1.3.1.1 Issues missing in the handbook:

- **Social Media Policy**: Social media usage during working hours can be problematic for companies, as some sites are blocked for workflow purposes. The CQC handbook should address the use of social media in and out of work, as employees and employers hold the credibility of the organization wherever they are.
- **Mental Health Policy**: CQC aims to maintain confidentiality, availability, and integrity. employees mental health needs to be addressed. This includes but not limited to substance abuse, suicide prevention, and self-management. There should be health and fitness programs, stress monitoring and counselling session for employees to promote an overall well-being.
- **Rules of Conduct Policy**: CQC should have policies in place to prevent employees from violating licensing procedures, especially when working with healthcare sub companies. The handbook should clearly state that employees must not falsify documents or breach confidential information for personal gain, as this could lead to legal action.

1.4 Information Security Strategic Plan

CQC's strategic plan aims to ensure a secure system and workflow throughout its day-to-day activities to meet its three main objectives: availability, integrity, and confidentiality (Fibikova & Mueller, 2012). The plan is divided into 10 points:

1. Information Governance training is mandatory for staff, initiated by the Cabinet office.
2. Employees are encouraged to change their passwords frequently, with strong passwords involving at least 8 characters.
3. Emails sent outside CQC's network containing personal and delicate information must be encrypted within an attachment.
4. CQC's information should not be distributed on unapproved social media platforms.

5. Phishing is a major problem within organizations, so employees should delete unsolicited emails and forward concerns to information.access@cqc.org.uk.

6. Personal and sensitive data should be disposed securely and adhere to CQC's Information Security and Governance Policy.

7. Computers should be shut down at the end of working hours or screen locked during breaks or meetings.

8. Employees are required to wear pass holders and not allow non-staff members to escort into unauthorised areas.

9. In case of a risk, data breach, or intrusion, members are advised to report to security@cqc.org.uk.

10. All these security measures must be ensured when employees work from home and CQC's assets are protected when traveling or at home.

1.5 Internal and External Threats to Information Systems

Internal threats are risks arising from internal events within an organization, while external threats are risks resulting from external incidents beyond an organization's control. At UQC, both types of threats can occur which are elaborated below:

1.5.1 Internal Threats

- The birdie app requires carers to make notes on client care, but mistakes in medication or unchecked examinations can increase the risk for the company in case of a client's harm, as employees may not always accurately record events.
- Employees must check-in or checkout clients before and after visiting them, as the birdie app alerts them when to do so. If a client forgets 15 minutes after check-in, the app sends a lateness

notification to management, posing a liability to the employee, management, and the company. Additionally, if a client is unharmed, there is no evidence of the employee's presence during their working period.

- If an employee loses their phone due to third-party intrusion, they can submit incorrect notes on their behalf.

  Office employees may display sticky notes with login details or board tasks, potentially causing intrusion and causing conflicts with necessary documents.

1.5.2 External Threats

- Birdie's system issue could disrupt UQC's workflow, preventing us from taking notes, logging in, or logging out after conducting client assessments.
- In the event of a fire outbreak or natural disaster at the office, all necessary documentation, whether paper or computer-based, may be lost.
- Emails sent to council and affiliate healthcare providers may be unencrypted at the office before being shared.
- Birdie's data, despite a backup plan, will be lost if the care history and clients' data are also compromised.

1.5.3 Security Strategy to Mitigate the Threats

To protect against threats, UQC should implement strategies such as auto-correcting employee notes, automated notifications for check-in and out, training employees on strong passwords, and Multi-Factor Authentications on office computers (Bhuyan *et al.*, 2022). Management should also raise concerns about external threats and implement measures to keep the system up-to-date, such as late night time upgrades, to prevent interference with working hours. All office documents should be backed up to cloud services to prevent loss of confidential information in case of natural disasters, and emails sent with sensitive data should be encrypted.

1.5.4 Risk Assessment Methodology Flow-chart

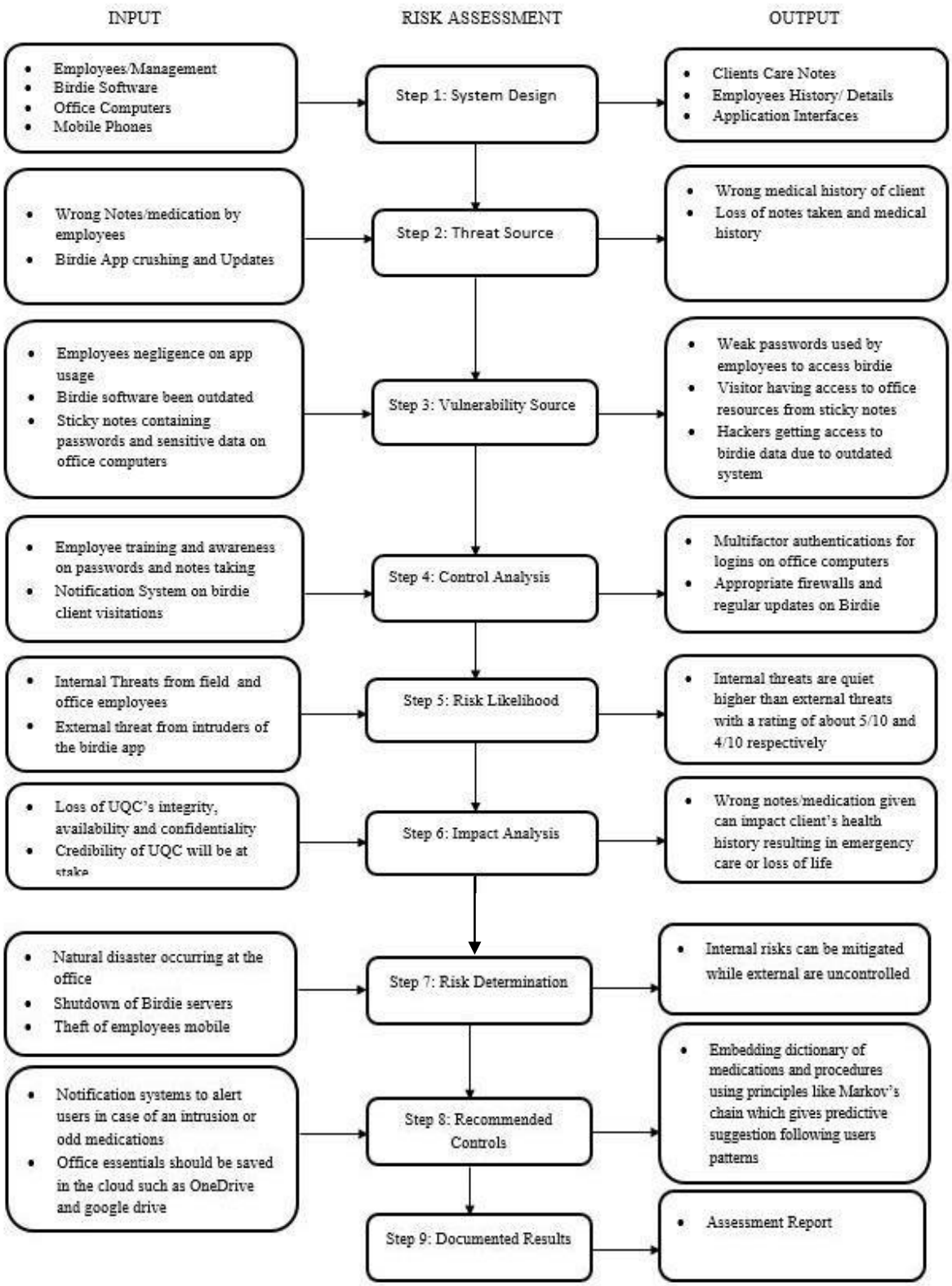
INPUT
RISK ASSESSMENT
OUTPUT
Employees/Management
Birdie Software
Office Computers
Mobile Phones
Step 1: System Design
Clients Care Notes
Employees History/ Details
Application Interfaces
Wrong Notes/medication by employees
Birdie App crushing and Updates
Step 2: Threat Source
Wrong medical history of client
Loss of notes taken and medical history
Employees negligence on app usage
Birdie software been outdated
Sticky notes containing passwords and sensitive data on office computers
Step 3: Vulnerability Source
Weak passwords used by employees to access birdie
Visitor having access to office resources from sticky notes
Hackers getting access to birdie data due to outdated system
Employee training and awareness on passwords and notes taking
Notification System on birdie client visitations
Step 4: Control Analysis
Multifactor authentications for logins on office computers
Appropriate firewalls and regular updates on Birdie
Internal Threats from field and office employees
External threat from intruders of the birdie app
Step 5: Risk Likelihood
Internal threats are quiet higher than external threats with a rating of about 5/10 and 4/10 respectively
Loss of UQC's integrity, availability and confidentiality
Credibility of UQC will be at stake
Step 6: Impact Analysis
Wrong notes/medication given can impact client's health history resulting in emergency care or loss of life
Natural disaster occurring at the office
Shutdown of Birdie servers
Theft of employees mobile
Step 7: Risk Determination
Internal risks can be mitigated while external are uncontrolled
Notification systems to alert users in case of an intrusion or odd medications
Office essentials should be saved in the cloud such as OneDrive and google drive
Step 8: Recommended Controls
Embedding dictionary of medications and procedures using principles like Markov's chain which gives predictive suggestion following users patterns
Step 9: Documented Results
Assessment Report

Figure 2: Risk Assessment Methodology Flowchart (personal collection)

1.6 Access Control Strategy

Access control strategy is a system that controls access to organizational resources and their level of restrictions (Feruza & Kim, 2007). It involves validation and permission policies to manage access, verifying user identity and controlling access to intended resources. An example is a swipe card used by employees to enter an office, which is authenticated based on the employee's role before the door opens.

There are several access control strategies with three elaborated below for the purpose of this study:

- Role-Based Access Control (RBAC): This strategy assigns permissions to service users based on their roles and duties (Schaad *et al*., 2001). A bank teller accessing transaction interfaces for withdrawal, deposits, and international remittances are typical examples.
- Rule-Based Access Control (RuBAC): This strategy employs fixed principles to regulate access to sensitive information of systems, allowing only designated departmental resources to be accessed by a bank's client service department.
- Mandatory Access Control (MAC): This strategy is implemented based on the security levels assigned to users and the materials they have accessed.

UQC should implement a Role-Based Access Control (RBAC) strategy to maintain a secure workflow within the organization and its resources, including the Birdie app used by employees and management. This strategy assigns super roles to management, based on their role in the Birdie app, which includes checking in and out at clients' residences, making notes on care and medication, and assigning weekly rotas based on availability. The super roles are assigned to management by Birdie company which shows a Rule-Based Access Control (RuBAC) (Schaad *et al*., 2001). Management also receives notifications if clients are 15 minutes late for each call assigned to them.

UQC uses a proactive approach to mitigate problems and take precautionary measures before they occur. This includes assigning roles to carers on the Birdie app, foreseeing alerts, not using sticky notes at the office, updating office computers regularly, installing firewalls, changing the PIN at the entrance to the

office building, and educating staff on the importance of multifactor authentication on hand-held devices used to access the Birdie app. This proactive approach may require long-term planning and effort, but it helps UQC make informed decisions and ensures long-term success (Lin *et al.*, 1993).

1.7 Incident Management Strategy

Incident management is the process of identifying and addressing organizational risks quickly and preventing their recurrence (Ozbay *et al.*, 2016). In an Information Security environment, technical incidents like virus detection, email disruptions, and system navigation problems can occur. An effective incident management strategy should cover various stages of an incident response plan for reliable response. This cyclic strategic plan is elaborated below;

1. **Preparation:** this is the initial and most crucial stage of this response plan (Bartolini *et al*., 2008). The response plan's initial stage involves training UQC employees, involving the Birdie application response team, and utilizing resources like a new alert system on the Birdie application. This will enable real-time notifications to all UQC employees in case of an attack or intrusion.
2. **Identification:** In the event of a suspicious attack or data breach, employees and management must be informed (Alharbi, 2020). At UQC, if an employee makes an error with notes or medication, their phone is stolen or hacked, and the birdie team is notified, the device is logged out of the system entirely. This ensures a smooth workflow and prevents data breaches.
3. **Investigate and Contain:** This stage emphasizes employee identification and management of attacks on the birdie app to prevent further harm. UQC employees will be trained on how to recognize unfamiliar login names and alert management when an issue arises, as fear can sometimes lead to panic.

4. **Eradication:** This is where the precise threat will be expelled (Ozbay *et al.*, 2016). Threats at UQC will be promptly communicated to Birdie's Recovery Team, ensuring that data is not lost after removing any attack on employees or UQC as a whole, as the app is hosted on cloud services.

5. **Communication**: UQC management must communicate ethically with stakeholders like employees, council, and social workers, and the Birdie team to collaborate, coordinate, and expedite mitigating attacks.
6. **Recovering:** After the attack is resolved, UQC's management will contact birdie to restore all data, including medication history, client notes, employee Rota, and care worker visits, for future reference.
7. **Learning and Improving:** In the final stage, the cause of an attack, such as an employee's mobile phone or management's interface, is explained, and employees are trained on protecting their devices with multi-factor authentication and strong passwords.

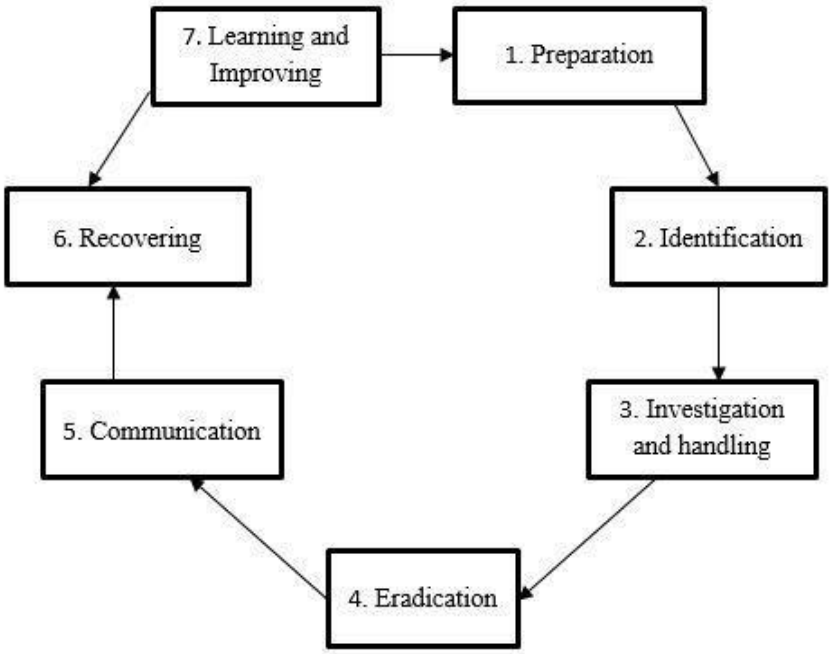

Figure 3: Incident Response Model (personal collection)

1.8 Brief Security Strategy

The strategic approach to UQC's information system involves a collaborative effort from employees, management, and stakeholders, focusing on five elements to meet business and security requirements as shown in figure 1.3 (Fibikova & Mueller, 2012).

1. **Identify:** UQC's staff should be educated and trained to identify intrusions and loopholes, and how to detect them when they occur.
2. **Safeguarding:** Employees and management are urged to ensure client data safety by avoiding exposure to third parties, such as companies that supply Personal Protective Equipment (PPE).
3. **Discovery:** Birdie has introduced a new feature that allows management to send a single notification to all employees in case of an attack.
4. **React:** Management should notify Birdie team of app threats to deactivate devices, while office computers should be protected with multi-factor authentication and strong passwords.
5. **Restore:** After removing the attack, management should contact Birdie to restore employee interface and client visits, and back up personal and sensitive office data on cloud storage.
6. **User awareness:** A care planner and documented risk management assessments as explained in section 1.4.4 of this document should be utilized by employees and management to monitor UQC performance and train them on their roles and responsibilities.
7. **Governance, policy and data protection:** The strategy should comply with government policies, including the Data Protection Act 2018, Health and Safety Act 1974, and Health and Safety at Work Regulations 1999 (Hale & Booth, 2019).

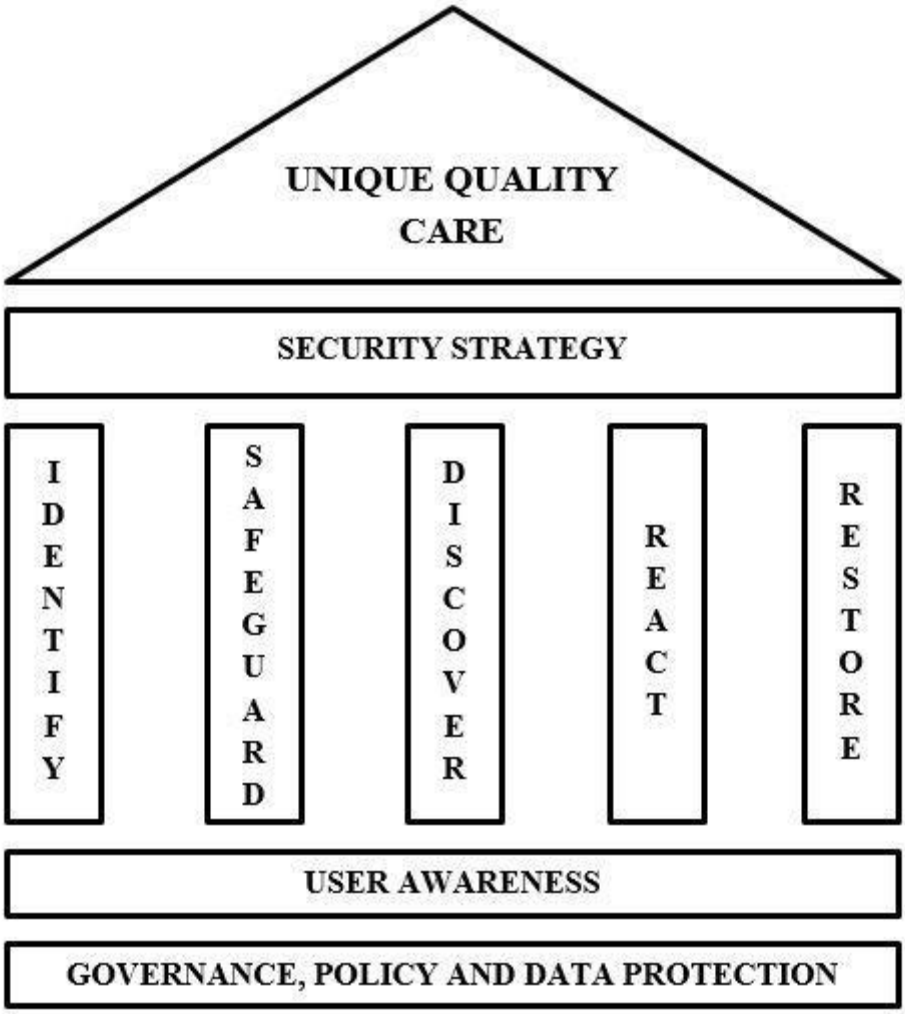

Figure 4: Diagram for a Brief Security Strategy (personal collection)

2.1 Conclusion

UQC's staff should be educated and trained to identify intrusions and loopholes, and how to detect them when they occur. Employees and management should adhere to information security strategies to maintain a secured workflow within the organization and its resources, including the Birdie mobile application used by employees and management to document clients care history.

References

Alharbi, F. S., (2020). Dealing with Data Breaches Amidst Changes In Technology. *International Journal of Computer Science and Security (IJCSS)*, 14(3), pp. 108–115.

Bhuyan, F. A., Lu, S., Reynolds, R., Zhang, J. and Ahmed, I., (2022). A Security Framework for Scientific Workflow Provenance Access Control Policies. *IEEE Transactions on Services Computing*, 15(1), pp. 97-109.

Bartolini, C., Stefanelli, C. and Tortonesi, M., (2008). SYMIAN: A Simulation Tool for the Optimization of the IT Incident Management Process. *In*: De Turck, F., Kellerer, W. and Kormentzas, G., eds. 2008. *Managing Large-Scale Service Deployment.* Berlin: Springer, pp. 83–94.

Birdie Care, (2023). *Privacy Notice* [online]. London: Birdie Care. Available from: https://www.birdie.care/terms/privacy-notice [Accessed 27 November 2023].

Blodgett, D. S. and Phair, D. J., (1992). *Integrating Commercial Off-The-Shelf Tools for Custom Software Development* [online]. Bedford:MITRE. ADA252462.

Care Quality Commission, (2016). *Policy statement on information security and governance* [online]. Newcastle: Care Quality Commission.

Culot, G., Nassimbeni, G., Podrecca, M. and Sartor, M., (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *TQM Journal* [online], 33(7), pp.76-105.

Feruza, S. and Kim, P. T., (2007). IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. *International Journal of Multimedia and Ubiquitous Engineering* [online], 2(2), pp.17-32.

Fibikova, L. and Mueller, R., (2012). Threats, Risks and the Derived Information Security Strategy. *In*: Reimer, H., Pohlmann, N. and Schneider, W. eds. *ISSE 2012 Securing Electronic Business Processes* [online]. Wiesbaden: Springer, pp. 11-20.

Hale, A. and Booth, R., (2019). The safety professional in the UK: Development of a key player in occupational health and safety. *Safety Science*, 118, pp. 76–87.

Lin, Z. and Carley, K., (1993). Proactive or Reactive: An Analysis of the Effect of Agent Style on Organizational Decision-making Performance. *Intelligent Systems in Accounting, Finance and Management* [online], 2(4), pp. 271-287.

Özbay, K., Xiao, W., Jaiswal, G., Bartin, B., Kachroo, P. and Baykal-Gursoy, M., (2016). Evaluation of incident management strategies and technologies using an integrated traffic/incident management simulation. *World Review of Intermodal Transportation Research* [online], 2(2/3), pp.
155–186.

Schaad, A., Moffett, J. and Jacob, J., (2001). The role-based access control system of a European Bank: A case study and discussion. *In:* Proceedings of Sixth ACM Symposium on Access Control Models and Technologies (SACMAT 2001). Chantilly: VA, Available from: https://dl.acm.org/doi/abs/10.1145/373256.373257 [Accessed 27 November 2023].

Such, J. M., Vidler, J., Seabrook, T., Rashid, A., (2015). Cyber Security Controls Effectiveness: A Qualitative Assessment of Cyber Essentials. *Security Lancaster* [online], pp.1-28.