



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Coursework Title:
Report, Component 1

Module Name: Network and Cybersecurity
Essentials

Module Code: ACCA4024_BIRM

Student Name: Alexandru Emilian Ciorascu

Student ID: 2436639

Lecturer Name: Muhammad Azeem Abbas

Submission date: 27.03.2026

Contents

Abstract	4
1. Introduction	5
2. Theoretical Background	6
2.1. The CIA	6
2.2. ISO/IEC 27001	6
2.3. NIST Cybersecurity Framework	7
2.4. Data Protection	7
3. Identification of Threats	8
3.1. External Threats	8
3.1.1. Ransomware	8
3.1.2. Phishing	9
3.1.3. DDoS	9
3.1.4. Cloud Security Breaches	9
3.2. Internal Threats	10
3.2.1. Insider Threats	10
3.2.2. Weak Password Practices	10
3.2.3. Device Misuse	10
4. Security Policies	11
4.1. Access Control Policy	11
4.2. Data Protection Policy	11
4.3. Bring Your Own Device Policy	12
4.4. Incident Response Policy	12
4.5. Password and Authentication Policy	12
5. Mitigation Measures	12
5.1. Ransomware Protection	14
5.2. Phishing Prevention	14
5.3. Insider Threat Mitigation	14
5.4. Cloud Security Controls	14

6.	Monitoring and Incident Response.....	15
6.1.	Incident Response Diagram	15
7.	Training and Awareness Program	16
8.	Critical Analysis	16
9.	Conclusion.....	17
10.	References.....	18
	Appendix	19

Developing a Data Security and Governance Framework for HealthPlus Analytics (HPA)

Abstract

Data security increasingly has become critical amongst organizations in healthcare. Health Plus Analytics (HPA), a UK-based healthcare technology company, processes large volumes of sensitive patient data, and it is the target of cyber assaults. Recent instances, such as unauthorized access to cloud-based data and a ransomware attack on analytics servers, have shown weaknesses in the security measures within the organization. This report intends to build the data security and governance framework in the context of HPA. The report examines the top-off threats the organization faces from the inside and outside and proposes security policies that are consistent with international cyber security best practices such as ISO 27001 and the NIST Cybersecurity Framework. The report outlines several methods to mitigate those risks along with how to carry out our program to track and respond to bad behaviors to the same standards. It also highlights training of staff as a critical aspect of security at work. In this regard, applying theoretical models such as the CIA triad and operational work, this report will clearly explain how HPA may work for the confidentiality, integrity and availability of its systems and data in the future. The proposed framework is harmonized with the UK GDPR and is needed in an organization to improve its cyber resilience as well.

1. Introduction

Cybersecurity has become a major concern for most businesses today and organizations that deal with sensitive data such as healthcare. Cloud, mobile services, including internet banking and remote office work have all changed organizations and those are more vulnerable and are also becoming more targeted at being hacked with cyber tools. Healthcare data is valuable to cybercriminals and with all data including personal, financial and medical accounts. HealthPlus Analytics (HPA) operates in a high-risk economy with data-centric processes at hospitals and clinics across the UK. Because it employs a cloud-based data infrastructure, employees frequently access systems from any remote position and even, so they go to see the entire site. All these advantages of flexibility and productivity will come at cost that HPA may only reap as it must address if it is not fully protected. Also, it is known that recent ransomware attacks of the malware-prone ransomware and unauthorized data capture are just a part of these already well-written HPA security protocols in dealing with the ever-increasing volume of new things and threats in terms of threat [1]. Even apart from technical complexity, HPA needs to satisfy strict regulations that are well defined including the UK GDPR, due to safeguarding personal data in good technical and organizational settings. Nonconformity may create long-term financial costs as well as damage to reputation and in case the sector and NHS will be negatively affected if they don't comply with such regulations. This report aims to develop a coherent and measurable information security and governance context which provides an outline of data security and governance and solves the problems by identifying risk and how to respond to these. It is shown how these aspects of cybersecurity theory can be applied and implemented to put data security policy and security technology in a more realistic organizational setting such that HPA could become more secure and resilient in all aspects of its organization.

2. Theoretical Background

A strong understanding of fundamental cybersecurity concepts is essential when designing effective security frameworks.



Figure 1. Background

2.1. The CIA

One of the best-known systems approaches this field is CIA triad of which the current information security models are based. The model is rooted in 3 main ideas which are confidentiality, integrity and availability. Confidentiality ensures that sensitive issues can only be disclosed to the authorized ones, integrity ensures that information remains accurate and unaltered, and availability guarantees that the systems and information are available to people from when required. For healthcare this notion of confidentiality or integrity will be critical [2].

2.2. ISO/IEC 27001

Based on these principles, one of the most used standards was ISO/IEC 27001 implemented by the ISO. It helps companies take an organization to see how security practices are structured and is based on an Information Security Management

System (ISMS). Management of sensitive information is based on risk assessment and controls are being put into place and quality continues to be addressed, so that meeting international best practice. For organizations like HPA, the ISO 27001 framework makes clear security policies with which it works and meets your business requirements and international standard in this field which is based on trust in organization shows the focus of that organization for it to work and the company when applying [3].

2.3. NIST Cybersecurity Framework

Like ISO standards and the Cybersecurity Framework of the NIST, the framework is designed in a framework which looks at how organizations deal with cybersecurity risk along the line of the five functions. NIST means identify, protect, detect, respond and recover. These functions provide a lifecycle approach for cybersecurity organizations. They can detect incidents and are able to react and respond effectively in response to incidents when they encounter these situations. This approach is very relevant to HPA considering the recent experience of a ransomware attack, where we must recover quickly and effectively [4].

2.4. Data Protection

It is also important that regulatory compliance plays a key role in company security processes. UK GDPR calls upon organizations to put adequate protective measures in place that also extend to encryption, access controls and breach notification. Such legal measures only highlight the need to create a structured and proactive approach to cybersecurity from now on. From an HPA perspective, these are all areas for it to protect such that trust is strong but also are transparent in it when compared to industry norms and to also deliver the security standards that are required for customers to remain happy [5].

3. Identification of Threats

HealthPlus Analytics operates in a global cyber security environment that involves face-to-face threats and a lot of external and internal threats that have an impact that can be felt around the organization. Due to the sensitive nature of health care data and the company dependent on cloud infrastructure, the threats must be carefully analysed and must fit with main values of confidentiality, integrity and availability [6].



Figure 2. Threat

3.1. External Threats

External threats arise from actors located outside the organization and can be very sophisticated. These are quite dangerous given the fact they operate predominantly on vulnerabilities in systems.

3.1.1. Ransomware

Ransomware is one of HealthPlus Analytics' most major threats. HealthPlus Analytics already faces this type of attack. Malware encrypts important data and does not allow access to data until a higher ransom is paid. The main effect of ransomware is on what's available because as soon as the code is received it goes blank. Modern

ransomware attacks could also be about data exfiltration, which breaks down the confidentiality and the organizational reputation. For health organizations the lack of access at least to patient data can lead to lost clinical care and the hospital's reputation is also badly affected.

3.1.2. Phishing

Phishing attacks exploit human weaknesses by deceiving employees to reveal sensitive information or to download malware. These activities are most presented through email and especially work in organizations that make good use of digital communication. Phishing has largely an impact on confidentiality and login details. In this way, the attack may lead to a broader deterioration in system integrity and availability.

3.1.3. DDoS

Distributed Denial of Service (DDoS) attacks are designed to inundate systems with a high volume of traffic, rendering services inaccessible to legitimate users. For HealthPlus Analytics, these attacks have the potential to hinder access to essential analytics platforms utilized by healthcare providers. This disruption directly affects availability, a fundamental aspect of the CIA triad. Extended service interruptions may also diminish trust in the organization's capacity to provide dependable services.

3.1.4. Cloud Security Breaches

Cloud-based systems are essential among HPA's operations, but they are also vulnerable. Misconfigured storage, weak authentication and even insecure are the basis for inappropriate access to patient data. Such exposures violate confidentiality and may also cause breaches of the UK GDPR. Because of the regulatory environment in the UK healthcare industry this threat is exceptionally serious.

3.2. Internal Threats

Internal threats originate from within the organization and are often more difficult to detect because they involve trusted users.

3.2.1. Insider Threats

Insider threats arise when individuals use access to systems and leak information to individuals or other employees with harmful motivation or simply bad form. This potentially means the theft of data or unauthorized release of information, or accidental disclosure of sensitive data may compromise those same relationships of trust and information.

3.2.2. Weak Password Practices

Weak passwords are leading to the risk of unauthorized use of these vulnerable passwords. Attackers can exploit these vulnerabilities with brute force or credential stuffing. This threat can not only affect confidentiality because unauthorized users are gaining access to the contents but can also impact data integrity if the data is changed, deleted or misused. The widespread use of remote access systems also increases.

3.2.3. Device Misuse

The use by the employees of personal devices has potential risks too, particularly if these devices are not secured or well located. In combination with missing, accidentally stolen or compromised devices are critical organizational data lost or stolen.

4. Security Policies

To address the identified threats, HealthPlus Analytics must implement a set of clearly defined security policies aligned with industry standards and regulatory requirements [7].



Figure 3. Security Policy

4.1. Access Control Policy

An active access control regime is crucial to ensure only authorized users can access sensitive data. It should be role-based access control in HealthPlus Analytics. Permissions are issued according to their job or their tasks. This system mitigates the risk of insiders' access to sensitive tools and reduces unnecessary access to the critical processes.

4.2. Data Protection Policy

A data protection policy is in place to maintain secure and legal management of sensitive patient information. This policy should involve encryption of data and data

transport, from the time of data transfer to the time when it is retained and used and clear guidance regarding data storage and access and sharing.

4.3. Bring Your Own Device Policy

Because of the remote working role of the organization, a BYOD policy is essential. Anyone who uses the devices for the job should have basic security levels such as device encryption, secure authentication and software updates.

4.4. Incident Response Policy

An incident response policy can allow the organization to respond fast and effectively to high-security incidents, such as ransomware attacks. The policy must specify the procedures that are to be followed to detect and report incidents.

4.5. Password and Authentication Policy

A strong password policy is essential to limit unauthorized access. Strong passwords, regular updates and multi-factor authentication are crucial.

5. Mitigation Measures

To effectively reduce the risks HealthPlus Analytics needs to incorporate technical and managerial controls [8].



Figure 4. Mitigation

Threat	Impact (CIA)	Mitigation Measures	Type of control
Ransomware	Availability, Integrity	Regular offline backups	Technical
Phishing	Confidentiality	Email filtering, security awareness training	Technical / Human
DDoS	Availability	Firewalls	Technical
Insider Threat	Confidentiality, Integrity	Role-Based Access Control	Managerial
Weak Passwords	Confidentiality	Strong password policy	Technical

Figure 5. Table of most common attacks

5.1. Ransomware Protection

HPA should do regular data backups stored securely offline or in an isolated setting to prevent ransomware attacks and ensure that systems are restored. Endpoint Detection and Response solutions can also facilitate real-time monitoring of endpoints, ensuring that data is no longer stolen or disrupted during the ransomware attacks.

5.2. Phishing Prevention

The technical controls of phishing may contribute to minimizing a victim's information. The company should implement email filtering technology in their company so that it is able to identify and prevent viruses before the threat reaches an employee.

5.3. Insider Threat Mitigation

HPA must also implement role-based access control to minimize insider threats. Access rights should be regularly reviewed and adjusted according to jobs. Monitoring of user activity may offer context for unusual behaviors that may indicate misuse of access.

5.4. Cloud Security Controls

To remedy cloud security risk, HPA needs to introduce strong encryption to protect data at rest and in transit. Multi-factor authentication security needs to be in place for every cloud service in terms of protecting users from unauthorized activities. Regular security audits and configuration checks are also necessary to identify security gaps and correct those.

6. Monitoring and Incident Response

Consistent surveillance and incident management are absolute essential for HealthPlus Analytics to identify, monitor or deal with cybersecurity threats early. HealthPlus Analytics must implement ongoing network monitoring through Security Information and Event Management (SIEM) systems throughout its network and an intelligent intrusion detection and prevention. These systems collect information from several sources and automatically detect suspicious activities. All these tools together improve the organization's ability to detect and respond to attacks as early as possible and manage them in a timely manner for the security of life. As well a well-organized incident response protocol is necessary to handle security incidents effectively and uniformly. Lifecycle monitoring, identification, analysis, containment, eradication and recovery in terms of detection can be managed using a commonly identified procedure [9].

6.1. Incident Response Diagram

Detection is about looking for security problems based on monitoring systems. In the stage of the containment, the attack spread by isolating the affected systems rather than being spread around all of them.

This structured approach allows HPA to minimize downtime and protect sensitive data.

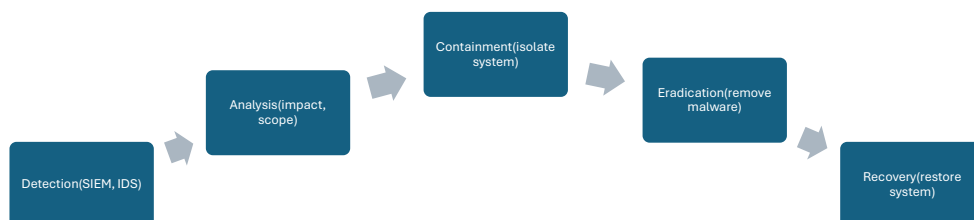


Figure 6. Diagram

7. Training and Awareness Program

An effective cybersecurity strategy must respond to human factors because more attacks are motivated by user behavior than technical weaknesses. HealthPlus Analytics need to develop formal onboarding training that will ensure a written framework in which employees will know their security duties and data protection objectives at ground level. Employee awareness training should happen occasionally in the form of phishing simulations to develop employee training to find the level of knowledge that is being used. Implementation of monthly training on common threat awareness and on threat escalation awareness from staff would make it more useful to be aware of current threats [10].



Figure 7. Training

8. Critical Analysis

Though the proposed security enhancements offer some strength and certain weaknesses to HPA, the system's security controls also come with some additional costs. Smart tools such as SIEM and EDR can be expensive and require huge levels of organizational resources. Security controls can be very strict and multi-factor authentication will take longer and work poorly, to what end can only be used on time and where should the employees not worry about it. Technical controls can never prevent human risks, insiders or social engineers for example.

9. Conclusion

This report has sets HealthPlus Analytics security strategy for data that will improve the protection of the sensitive healthcare data provided while continuing conforming to the UK GDPR framework. By combining technical controls on IT and staff with continuous security monitoring, HPA will better secure the data and companies to help maintain the level of security of the whole business. Strategic engagement and cybersecurity on a preventive basis for a long-term security perspective is an integral part of trust and sustainable maintenance.

10. References

- [1] ENISA, Threat Landscape 2023, European Union Agency for Cybersecurity, 2023.
- [2] W. Stallings, Effective Cybersecurity: A Guide to Using Best Practices and Standards, Addison-Wesley, 2018.
- [3] ISO/IEC, ISO/IEC 27001:2022 Information Security Management Systems, International Organization for Standardization, 2022.
- [4] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018
- [5] UK Government, UK General Data Protection Regulation (UK GDPR), 2023.
- [6] M. Higgins, M. Regan, and J. J. Pauli, Cybersecurity. Minneapolis, Minnesota: Essential Library, an imprint of Abdo Publishing, 2017.
- [7] M. Dunn Caveltty and A. Wenger, Eds., Cyber Security Politics : Socio-Technological Transformations and Political Fragmentation, 1 ed. s.l: Routledge, 2023.
- [8] C. Florackis, C. Louca, R. Michaely, and M. Weber, “Cybersecurity Risk,” The Review of financial studies, vol. 36, no. 1, pp. 351–407, Jan. 2023, doi: 10.1093/rfs/hhac024.
- [9] Y. Jiang, M. A. Jeusfeld, J. Ding, and E. Sandahl, “Model-Based Cybersecurity Analysis: Extending Enterprise Modeling to Critical Infrastructure Cybersecurity,” Business & information systems engineering, vol. 65, no. 6, pp. 643–676, Dec. 2023, doi: 10.1007/s12599-023-00811-0.
- [10] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, “Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behavior,” International journal of information management, vol. 45, pp. 13–24, Apr. 2019, doi: 10.1016/j.ijinfomgt.2018.10.017.

Appendix

PowerPoint Slides Presentation with link.

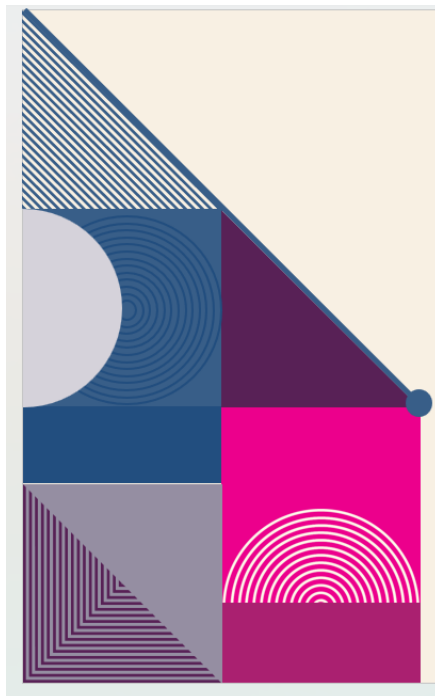


HEALTHPLUS ANALYTICS-DATA SECURITY

ALEXANDRU EMILIAN CIORASCU

**MODULE NAME: NETWORK AND
CYBERSECURITY ESSENTIALS**

MODULE CODE: ACCA4024_BIRM



PROBLEM CONTEXT

CYBERSECURITY CHALLENGES IN HEALTHCARE

- Recent ransomware attack on analytics servers
- Unauthorized access to cloud-stored patient data
- Remote & hybrid working increases exposure
- HPA must comply with GDPR & NHS standards



2



KEY THREATS

MAIN CYBER THREATS

- Ransomware can disrupt operations and data
- Phishing targets employees to steal credentials
- Insider threats exploit internal access
- Cloud misconfigurations risk patient data exposure



IMPACT

EFFECT ON DATA SECURITY

- Confidentiality: patient data could be exposed
- Integrity: unauthorized changes to analytics data
- Availability: ransomware or DDoS could halt services



SECURITY POLICIES

POLICIES TO PROTECT

- Access Control: restrict sensitive data access
- GDPR Data Protection Policy: legal and ethical compliance
- BYOD Policy: secure personal devices accessing corporate data
- Incident Response Policy: structured handling of threats
- Password Policy: enforce strong authentication practices

5

MITIGATION MEASURES

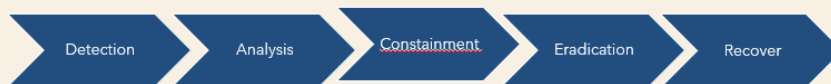
- Ransomware: Regular backups; Endpoint Detection & Response (EDR)
- Phishing: Email filtering; staff training; Multi-Factor Authentication (MFA)
- Insider Threat: Least privilege access; monitor user activity
- Cloud Breach: Data encryption; MFA; configuration audit
- DDoS: Firewalls; IDS/IPS; cloud-based DDoS protection

6

MONITORING AND RESPONSE

INCIDENT RESPONSE LIFECYCLE

- Detection: monitor systems using SIEM & IDS
- Analysis: identify scope & impact of incident
- Containment: isolate affected systems quickly
- Eradication: remove malware or unauthorized access
- Recovery: restore systems & strengthen defenses



7

TRAINING AND AWARENESS

EMPLOYEE SECURITY

- Onboarding training: basics of cybersecurity
- Phishing simulations: test staff awareness
- Monthly awareness: updates on emerging threats
- Role-based training: specific guidance per team



8



CRITICAL ANALYSIS

LIMITATIONS

- Cost vs security investment
- Usability vs strict controls
- Human factor risk remains significant



9



CONCLUSION

- Integrated framework reduces cyber threats
- Supports GDPR and regulatory compliance
- Improves trust and operational resilience
- Proactive security minimizes future incidents



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

10

