International Journal of Scientific and Management Research
Volume 8 Issue 5 (May) 2025
ISSN: 2581-6888
Page: 20-50

Securing Public Health in The Digital Age: A Cybersecurity Case Study of Uk Local Council Health Services

Ugochukwu Anthony Igboko[1]* & Olofintuyi Adeolu Temitope[2]
[1]Digital and ICT Department, South Tyneside Council, **United Kingdom**
[2]Big Data Analytics, Sheffield Hallam University, **United Kingdom**
DOI - http://doi.org/10.37502/IJSMR.2025.8503

Abstract

Introduction
While increasing the cyberattack surface and exposing sensitive patient data and vital service continuity to sophisticated threats, the fast digitisation of UK local council health services has improved care delivery. This study investigates institutional readiness and presents cybersecurity issues under decentralised public health governance.
Methodology
We conducted a qualitative systematic literature review, adhering to PRISMA guidelines. We used peer-reviewed articles and policy reports from 2019 to 2019–2025, sourced from Scopus and PubMed. Thematic analysis and critical evaluation methods (JBI checklist) were used to find common weaknesses, response actions to incidents, and how effective national cybersecurity efforts are at the local government level.
Design and Implementation
Drawing on synthesised insights, a novel cybersecurity framework was developed. We mapped the framework to identified management and technical challenge areas to facilitate practical implementation across diverse council IT environments.
Evaluation, Comparative Analysis and the strength of the framework.
We evaluated the efficacy of the framework through a hypothetical attack scenario at "WeCare Hospital", which demonstrated improved containment and rapid recovery. A comparison with current solutions such as blockchain-based identity management and cloud privacy systems showed that it is better because it can be quickly set up, follows regulations well, and can grow easily, especially for on-site and mixed setups.
Conclusion
When the proposed framework is followed, it will significantly enhance cyber resilience for UK local council health services by integrating technical, organisational, and human factor measures. Its adoption promises to safeguard patient data, ensure regulatory compliance, and maintain service continuity.

Keywords: UK council, Healthcare, SLR, cyber resilience.

1. Introduction

The digital transformation of public health in the UK has dramatically improved service delivery, data access, and efficiency of service provision. Local council health services in particular, in partnership with the National Health Service (NHS), are increasingly relying on

digital systems, including cloud-based health records, remote monitoring technologies, and virtual care. However, with digitisation comes a broadened attack surface for cyber threats, exposing sensitive health data and disrupting care services.

The 2024 Cyber Security Breaches Survey revealed that many public sector organisations, including healthcare, continue to struggle with fundamental cyber hygiene, resulting in vulnerability to both AI-driven attacks and ransomware attacks (Mansfield-Devine, 2024). Emerging frameworks such as Virtual Wards, where hospital-level care is delivered at home through digital interfaces, have been accepting the importance of understanding human factors, usability and cybersecurity in the delivery of public health (Fotis et al., 2024). These examples are promising but do present systemic weaknesses in practices related to data protection practices delivered through local council systems.

Government initiatives such as Cyber Essentials have sought to surface gaps related to cyber awareness and infrastructure; however, they have been berated on the ground for their ineffectiveness in implementation and limited uptake (Odebade and Benkhelifa, 2023).

The study sits at the intersection of cybersecurity, digital health governance, and public service delivery, using the case study of local councils in the UK. The study examines the effectiveness of the cybersecurity strategies that have been employed in health service delivery and explores institutional preparedness for protecting patient data and maintaining service provision during cybersecurity incidents.

The study builds on recent developments and case examples to contribute to the knowledge of how cybersecurity can be integrated into the ecosystem of local public health to promote both resilience and equality.

1.1 Background of Study

The health services in the United Kingdom have progressed quickly in the digital era; local councils have played an important role in the provision of public health programmes, alongside NHS trusts. Digitisation has facilitated ongoing patient monitoring, interoperability of health data, and better administration processes. Care models have been adjusted by the introduction of virtual wards and remote consultations, particularly during and after COVID-19 (Fotis et al., 2024). However, this has also led to new risks. There has been an increase in cyber activity against healthcare organisations, with 76% of healthcare breaches due to basic application vulnerabilities and intrusions (van Kessel et al., 2023).

Although the NHS is undergoing significant IT reform, it has attracted criticism for being heavily focused on operational efficiency and not on integration of security (Waynforth, 2024). Local councils are particularly susceptible due to fragmented IT systems, an inconsistent budget and a lack of trained staff. Reports by the BMJ have pointed out that local councils cannot plan robust digital health services, including those that would require investment in cybersecurity, because of delays in budgets being confirmed (Limb, 2023).

In addition, the recruitment of national cybersecurity initiatives has not always been straightforward. For example, Cyber Essentials and 'Get Safe Online' schemes were designed to standardise cyber protections, but evaluations have shown little impact as a consequence of inadequate training, lack of measurement, and consequently poor take-up by neighbourhood practice (Odebade and Benkhelifa, 2023). Further complicating this landscape is the shift from

"cybersecurity" to "cyber power" notions of strategy, which refocus strategy on a perception of global cyber dominance and diffuse attention from domestic resilience (Devanny and Dwyer, 2023).

Local councils' health services are tasked with operating in a complicated, underfunded and often misaligned digital security environment. These must be addressed comprehensively for all aspects, including policy, systems, training and technology. The case study method will allow for detailing the dimensions of digital health and security in practice and practically identify steps to reduce cybersecurity risk while navigating decentralised models of health governance.

1.2 Problem Statement

While UK health services are rapidly being digitised, local councils have an ongoing gap in readiness for cyber preparedness. These agencies deliver critical public functions to public health and frequently do not have a foundation of strong technical infrastructure, financing, and specific staff to ensure they are addressing cyber threats while doing so.

Existing national government initiatives on cybersecurity are not sufficiently leverageable for local authorities and jurisdictions to implement in practice, leading to some implementation, but not all of those jurisdictions complying with the minimum expectations (Odebade and Benkhelifa, 2023).

Health data, as a target for cybercriminals, creates significant risk to individual privacy and operational continuity in public health. The risk posed to virtual wards and remote systems highlights the need for context-based frameworks for cybersecurity (Fotis et al., 2024). This research is orientated toward the evaluation and addressing of urgent revitalisation of local council health service jurisdictional cybersecurity techniques (and overall practice).

1.3 Research Aim

To critically assess the cybersecurity challenges and strategies within UK local council health services and propose practical, policy-aligned recommendations for securing public health in a digital environment.

1.4 Research Objectives

1. To examine the current cybersecurity practices and digital infrastructure of UK local council health services.
2. To identify key vulnerabilities and barriers to effective cybersecurity implementation in decentralised public health systems.
3. To evaluate the effectiveness of national cybersecurity initiatives at the local government level.
4. To recommend actionable strategies and policy reforms for enhancing cyber resilience in public health service delivery.

1.5 Research Questions

To achieve the research objectives, this study review seeks to answer the following research questions:

i. What are the common causes and contributing factors of cyber breaches in UK local councils?
ii. How effective are the incident response strategies employed by local councils in the aftermath of a breach?
iii. What are the key challenges and barriers to effective cybersecurity in local councils?

1.6 Significance of Study

As healthcare transitions to a digitally embedded model, exposure of health-related data and important services to cyber risk has increased. Local councils, which manage many of the public health services and to whom the NHS delegates responsibility, are often under-resourced in their cybersecurity preparedness and are particularly exposed (Waynforth, 2024).

This proposal is important because it systematically reviews contemporary cybersecurity risks associated with frameworks in UK local health governance, with the purpose of developing relevant evidence-based mitigation strategies. This research will make public health systems and services safer and more reliable by looking at both the technical and human aspects of risk. For example, the risks that come up in NHS virtual wards (Fotis et al., 2024) will be studied.

The deliverables of the project will support local councils, public health leaders and policymakers to both shape practical and scalable cybersecurity interventions for public health and ensure continuity of care and public trust in the health digital ecosystem.

1.7 Research Rationale

This study originates from the increasing recognition of the fact that the public health system in the UK (in particular, at the local government level) is ill-equipped to address cybersecurity threats. Even with national programmes, such as Cyber Essentials promoting minimum standards for cyber hygiene, several councils cannot meet the minimum standards due to insufficient funding and training and poor collaboration between IT and healthcare staff (Odebade and Benkhelifa, 2023).

The growth in using digital tools such as virtual wards has further increased exposure to cyber-related risks, especially for vulnerable groups (Fotis et al., 2024). In an attempt to achieve some methodological rigour, a systematic literature review will allow for an overarching approach to synthesise disparate insights across health, IT, and policy.

This project aims to answer some important knowledge gaps and convert academic knowledge into actionable ways to translate academic knowledge into practical solutions for improving cyber resilience in health service delivery, operating in local council areas where support is sparse.

1.8 Research Scope

This research is a systematic literature review specific to cybersecurity challenges faced by local council health services across the UK. Specifically, it reviewed peer-reviewed research, government reports, and policy documents published from 2023 onwards. This research focuses on solutions that can reduce risks when delivering public health within health services and directly strengthen local resilience.

2. Literature Review

UK local councils are grappling with escalating cybersecurity challenges amid a wave of increasingly frequent cyber breaches. Recent analyses reveal that councils face a relentless barrage of attacks – on the order of thousands per day – targeting the critical services and sensitive data they manage. This chapter carefully discuss the cyber security issues related to the UK council through the conceptual, theoretical and the empirical review.

2.1 Conceptual Review

2.1.1 Cybersecurity Definition and Importance

Cybersecurity, in simple terms, is the practice of securing networks, systems, and data from cyberattacks or unauthorised access (NACCHO, 2024). Local government cybersecurity includes safeguarding citizens' information and maintaining council business continuity amidst cyber threats (National Audit Office, 2025). The importance of strong cybersecurity for councils cannot be exaggerated — local government possesses vast amounts of personal data on citizens (from financial information to sensitive health and social care records) and manages essential public services.

An effective cyber-attack can divulge sensitive data and paralyse the provision of services, affecting the well-being of a community directly. The UK government defines cyber resilience as the capacity of an organisation to continue delivering essential services and safeguarding data despite being under cyberattack. For councils, it means ensuring services such as social care, emergency services, and tax collection keep running without interruption in a secure way. The drive towards digital public services during the COVID-19 pandemic stretched the local councils' attack surface, providing malicious actors with more avenues to disrupt if appropriate cybersecurity measures are not implemented (National Audit Office, 2025).

2.1.2 Types of Cyber Threats to Councils

UK local councils confront a range of cyber threats, with phishing and malware attacks being the most prevalent. Phishing – fraudulent emails or messages crafted to trick staff into divulging credentials or downloading malware – is reported by three-quarters of councils as the most common attack vector (Gallagher, 2025). Such tactics often serve as the entry point for more destructive breaches; for instance, Gloucester's breach began with a spear-phishing email carrying malware (Gloucester City Case Study, 2023). Once inside a council's network, attackers may deploy ransomware (malicious software that encrypts systems to extort payment) or other malware to steal data. Ransomware has become a scourge in the public sector: in the Hackney Borough attack, hackers not only encrypted council files but also exfiltrated thousands of records, later demanding ransom under threat of leaking sensitive citizen data (ICO, 2024). Another threat vector is Distributed Denial of Service (DDoS) attacks, which overwhelm public-facing websites or online services by flooding them with traffic. While DDoS is less frequent than phishing, it is still a significant concern – a 2022 survey ranked it the second most common cyber-attack method on councils (cited as the top threat by 6% of authorities) (Gallagher, 2025). DDoS attacks can knock out online portals for services like payment systems or reporting platforms, impeding residents' access. Furthermore, councils must guard against web application attacks such as SQL injection, wherein attackers exploit vulnerabilities in online forms or databases to steal or manipulate information. Though not as widely publicised as ransomware incidents, SQL injection and similar exploits remain an

Achilles' heel for any poorly secured council websites (Jamie, 2024). In aggregate, these threat types – whether social engineering (phishing), malware/ransomware, or network and application attacks – form a diverse threat landscape that local councils must vigilantly manage. The sheer volume of attacks is daunting: one investigation estimated an average of 37 cyber-attack attempts per minute on UK councils (Ashford, 2018). This highlights the need for councils to be prepared for not if but when an attack gets through.

2.1.3 Key Cybersecurity Frameworks and Regulations

The UK councils operate under stringent regulations on cybersecurity and data protection. These include the General Data Protection Regulation, GDPR, which became law in the UK as the Data Protection Act 2018. The requirements for this would involve organisations ensuring that they protect personal data with adequate technical and organisational measures, including notification to relevant authorities within 72 hours of serious breaches. If these obligations are not met, the regulatory body may impose severe fines on the local government, among other consequences.

The ICO (2024) investigation concluded with an inquiry stating that the council has not implemented proper security controls, like patching systems and account protection, which breaches the duty of data protection. In addition to complying with GDPR/DPA, councils need to follow the guidance of national cyber frameworks. NCSC issues the best practice guidance, including the '10 Steps to Cyber Security', or specific guidance to the public sector entities along with support for the incidents.

Many councils are either Cyber Essentials scheme members of the NCSC or follow some standards such as ISO/IEC 27001 for the management of their information security. In addition to general advice, sector-specific advice can also be obtained; for example, the LGA produced a "Cyber Security Strategy for Local Government" along with case studies to communicate the lessons learnt from incidents (TechInformed, 2024). Besides, the evolving legislation may influence councils' cyber duties – the proposed UK Cyber Security and Resilience Bill plans to improve critical infrastructure with new demands on public sector cyber defences (National Audit Office, 2025).

2.2 Theoretical Review

Understanding why cyber breaches occur in UK local councils and how those organisations respond benefits from multiple theoretical lenses. This section applies three pertinent theories – Routine Activity Theory, Protection Motivation Theory, and Human Factors Theory – to interpret councils' cybersecurity risk environment and behaviours.

Routine Activity Theory (RAT)

Originally formulated as a criminological theory, RAT assumes that a crime (cyber-incident) can be committed when three elements converge: motivated offender, suitable target, and absence of a capable guardian (Madarie, Kranenbarg, and Poot, 2025). The concept of RAT provides the answer for why UK local councils have become easy prey for cybercriminals.

The target has value since it contains personal identifiers, financial records, and information related to health and social care, while also providing a great number of vital services; this means a breach is easy if completed with great value or a high impact. Besides, some local councils use legacy IT systems, thus having unequal security posture; such could mean the

council has some weaknesses or gaps for guardianship. Motivated offenders are easily found among attackers; such include financially motivated ransomware gangs and hostile-state-sponsored actors viewing public sector organisations as easy prey.

As such, the rise of ransomware-as-a-service lowers the entry bar for offenders and lets even less-capable hackers obtain tools for advanced attacks on councils (Joint Committee on the National Security Strategy, 2023). The last one of the mentioned components – the absent guardian – can be understood as inadequate security measures taken by the local authority to protect the digital assets of the council. For example, weak access control, unpatched systems, or lack of employee training means that a 'guardian' does not exist, allowing a motivated offender to commit the act with impunity.

Thus, RAT explains the dangers of a council breach, like an account that is easy to get into with a weak password and no patches for one council, which encourages criminals to target the council's network (ICO, 2024) as a valuable target. Applying RAT allows improvement in local councils' cybersecurity, which would increase guardianship or the strengthening of a council's systems through the harder and better protection of data that makes motivated attackers' chance of committing a crime low.

2.1.4 Protection Motivation Theory (PMT)

From a psychological standpoint, PMT speaks of how individuals and organisations protect themselves from perceived threats. The theory proposes that when there is an identified threat, there are two types of cognitive appraisal that can be applied as a basis for actions. These include threat appraisal, assessing the seriousness of the threat, vulnerability assessment (one's vulnerabilities), and coping appraisal or the capacity to cope with the threat and what can be done (Sulaiman et al., 2022).

In the case of cybersecurity measures at councils in the UK, PMT may thus explain whether the council wants to invest in some specific security controls. Cyber-attack: This is perhaps the most familiar case. When the council's leaders think that a cyberattack would have terrible effects (severe perceived severity, such as shutting down all public services for weeks), and when the council itself becomes a high-probability target (high perceived vulnerability, meaning that most attacks have been on coworkers), that might be the right time for a threat assessment to come to the conclusion that there should be some reason to act. With respect to response efficacy, the council's decision-makers will study what countermeasures, such as multi-factor authentication, staff training, or firewall installation, will accomplish. A self-efficacy evaluation will then follow as the decision-makers assess whether they can afford the upgrades, whether they have competent staff, and whether they have the resolve to implement such improvements (Sulaiman et al., 2022).

In some cases, the council may assess whether the ransomware is likely to hit them and, by enhancing the backup system and applying network segmentation, respond with a declaration to the effect of upgrading being made by a skilled team (self-efficacy), thus motivating further implementation of protection mechanisms envisaged by the PMT model. If the decision-makers are of the opinion that it would not happen—e.g., "we are a small district; hackers won't bother us"—or feel defeated already due to the sophistication of the attacks, then it is possible that they may regard the cyber threat as not really serious enough to consider further actions.

According to some research, this attitude is dangerous: one-fourth of the councils declared that they had made no improvements to their cybersecurity in the past year (TechInformed, 2024).

Basically, PMT describes how many more breach incidents the councillors will learn about, and higher probabilities for their own employees' exposure to cyberattacks would trigger their further efforts directed at defending mechanisms against cyberspace. Fear appeal and awareness are the drivers pushing for the motivation of the behaviour, according to PMT. For example, they may warn other councils of a breach that happened and tell case studies that may make councils further aware of the severity and vulnerability that would, in turn, encourage them to make a further effort into the protection of cyberspace.

2.1.5 Human Factors Theory

The role of human behaviour in cybersecurity is usually analysed in the light of "human factors." While it is not a single, uniform theory in name, frameworks of human factors in this context, which are more generally discussed in safety sciences and increasingly in the context of cybersecurity research, highlight how human errors, decision-making, and organisational culture contribute to security incidents. In the case of cyber breaches, a human factors theory approach would focus on how it was that certain classes of individuals, such as council employees, IT staff, management, or even the citizens, created or contributed to the conditions in the breach.

Numerous studies and breach reports substantiate that human errors and misjudgments have been a major factor for failure in cybersecurity (Sjouwerman, 2020; Ashford, 2018). Such examples include an employee being tricked by a phishing email, IT personnel not installing important security patches, or poor password practices or decisions in responding to incidents. In UK councils, the human factor abounds: evidence of human factors has revealed the main reason behind successful cyber-attacks on councils, yet only a quarter of local authorities required their staff to undergo mandatory cyber security training some years ago (Ashford, 2018).

For instance, in the case of Hackney Council, the ICO found a dormant account with a guessable password that had not been disabled – a rather minor oversight, yet it provided an opening for attackers (ICO, 2024). This shows an example of improper user account management (a human/process lapse) leading to a serious data breach (Verizon, 2023). The theory about human factors invites us to evaluate such cases systematically: Was the employee overburdened, or was there ignorance of the existing policy? Is there a cultural norm of sharing passwords? Did management enforce the security policy? Councils can mitigate the "human factor" risk through appropriate training, awareness, and user-friendly security policies. It is also important that many breaches could have been averted or contained had the management worked towards the development of a security-conscious culture with regular training simulations (such as phishing exercises) and with systems put in place that reduce the chance of user error, e.g., clear warning prompts or two-step verification.

2.3 Empirical Review

Drawing on recent case studies and empirical analyses (2022–2025), this section examines the common causes of cyber breaches in UK local councils, evaluates how councils have responded to incidents, and discusses the practical challenges they face in managing

cybersecurity. The evidence reveals recurring themes in how breaches occur and how well local authorities can cope in the aftermath.

2.3.1 Common Causes and Contributing Factors

An examination of the events over the last few years has shown that many breaches on the council's side share the same roots. Phishing and social engineering, which exploit the vulnerability of human beings, are the main channels through which breaches occur. The majority of council case studies have cited phishing emails as being responsible for breach entry. The attack on Gloucester City Council in December 2021 was initiated through a spear-phishing email that was cunningly embedded in a supplier's ongoing correspondence (Gloucester City Case Study, 2023). A council staff member, believing it was an honest e-mail, followed the embedded link, which installed malware on Gloucester's system.

This is a clear example of tricking a user into installing malware, which serves as a clear example of the impact of not being vigilant or well-trained on one's behalf. Leicester City Council also had an alleged breach believed to have been executed by a targeted phishing or a similar social engineering tactic to disable systems in 2024 (TechInformed, 2024). Another common cause of the breach would be the use of unpatched software or system vulnerabilities. Many local councils are faced with the challenge of maintaining complex IT environments that include legacy applications (sometimes built specially for government services) which may not be patched up to date. The Hackney attack probe identified that not applying critical security patches on systems was a clear enabling factor that enabled the attackers to access Gloucester's network (ICO, 2024).

Attackers took advantage of well-known weaknesses that had not been patched; this further underlined the importance of serious patch management. An associated weakness is poor access control and credential management. In the case of Hackney, an old user account with a default password that remained unchanged was active on the server, and the attackers exploited this for privilege escalation (ICO, 2024). This particular negligence (unused accounts not being disabled, weak passwords) unfortunately is not uncommon and reflects failings in IAM processes. Other councils point out problems with network architecture as contributors to breaches.

2.3.2 Incident Response Effectiveness

The response of councils towards a breach that is either being undertaken or has been completed and the effectiveness of that response is mixed, ranging from some councils that demonstrate some resilience to others that struggle during the recovery process. An example that works in its favour is that of St Helens Council, which was attacked by cyber attackers in August 2023, resulting in data exfiltration (a form of double-extortion ransomware attack). St Helens foresaw most of its data (66%) would be in the cloud; importantly, none of the cloud backups had been accessed by the attackers (Member, 2024). So, it could therefore recover its on-premises systems that had been hit and then taken offline but retrieve data from the cloud to start the restoration. St Helens was able to restore its systems fully in around 10 weeks, which is comparatively quick for the magnitude of a modern ransomware incident.

The St Helens case stands as an example of the efficiency of well-advanced business continuity planning (with the backup offsite and cloud) and how helpful quick containment is. St Helens' leadership switched to its incident response protocols upon detection of the breach: critical

systems were turned off to stop the further spread of the attack, while communication channels for affected services were made alternative (Member, 2024). A similar containment process was applied by Leicester City Council in 2024, shutting down systems in expectation of the major cyber incident, thus establishing communication channels (WAQAS, 2024). By doing so, Leicester could have possibly minimised damage, but that meant short periods of interruptions in services. Other aspects of the incident response included collaboration with outside entities.

According to the post-attack review for Gloucester, it sought out the National Cyber Security Centre (NCSC) and National Crime Agency (NCA) for guidance on investigation and recovery just days after the breach was detected. The LGA and central government (DLUHC) also offered financial and technical assistance for Gloucester's reconstruction of systems. This multi-agency support model seems efficient for expertise sharing and reduction of recovery burden on a council. On the contrary, there have been responses to breaches that were unattractive. In Hackney's case (2020), much effort went into restoring services which faced disruptions for a lot of time, with certain functions reverting back to normal in early 2021 and even in 2022 (ICO, 2024). This indicates that both the initial response and the contingency plans could have gotten overwhelmed with the attack's severity. A great number of citizen service delays had to be processed (for example, a backlog of requests from citizens) through a laborious restoration and decryption of surviving backups.

Thus, the success of a council's response to an incident is largely based on preparation before the breach: having offline backups, testing its disaster recovery plans, and training its incident response teams. Once cybersecurity had been conducted and resilience built by councils like Gloucester – with cyber drills and staff training before an attack – the councils got hacked but maintained some continuity by working around with some help from outside. Conversely, those councils with no tested plan had to scramble with ad hoc solutions and saw their outages extended. Rapid communication and openness to residents have become critical lessons emerging from such recent incidents, since the quicker the message was spread out about the incident, the better they were equipped to respond. Councils like Leicester issued public updates and temporary contact numbers when systems were down (Leicester City Council, 2024) as an attempt to reassure the citizens.

2.4 Research Gap

This literature review indicates that although cyber breaches within UK local councils are slowly beginning to receive attention, the literature thus far still has some considerable gaps. One gap is the limited number of academic publications on incidents of cyberattacks in local government. Most information on cyberattacks available to the public, especially from a research point of view, comes from industry reports, government surveys, and case studies on specific instances. There are very few academic studies that conduct extensive analysis into breaches of UK councils, and they tend to draw conclusions and lessons from post-incident reviews, which remain few and far between. The review identified very few peer-reviewed studies on local government lessons from cybersecurity that had emerged in the last few years (some required extrapolations from related fields such as healthcare or public sector IT).

This may indicate that the scenarios of local governments do not represent the broader context of research on cybersecurity. It may be noted that there are nuances that have been missed: in particular, local councils have some different constraints and community-facing duties when

compared to private companies or even central government agencies; however, literature usually broadens generalisation in public sector cybersecurity without paying more specific focus on councils. More empirical studies or comparative analyses of case studies that focus on the particular cases of breach experiences of local councils in the UK should be conducted. Other gaps include research on recovery and learning from an incident, which is often limited to reporting the immediate impacts and remedial steps after a breach, rather than the changes that happen in councils over a span of months or years.

The literature does not adequately address whether councils actually embrace "lessons learnt" from a post-incident review or if these changes effectively prevent future incidents. For example, the lessons learnt by Gloucester were documented in a detailed report, but little published research exists to determine how often similar in-depth post-mortems are conducted by all councils or how they get translated into better sector-wide policy responses. Another area of gaps involves connecting theoretical perspectives with practice. The theories applied included RAT, PMT, and human factors. Besides that, literature so far has mainly described the problems (what went wrong), while the successes or near misses have attracted much less research. It provides an opportunity for research on successful strategies for local council cybersecurity. The present study intends to propose the identified solutions in what works well using the comparative studies.

2.5 Conclusion

In conclusion, this review provides additional information in a sense of reassertion regarding the basic premise that local authorities within the UK suffer cyber-related losses to a greater degree and that breaches can be devastating in a social context. Both the literature and cases generally agree upon three key lessons: a) the importance of prevention and preparedness (e.g. basic cyber hygiene: patching, multi-layer access management, and staff awareness training that would avoid breaches that could be explained as occurring because of obvious oversights (ICO, 2024; Ashford, 2018); b) resilience in planning (reliable backup storage, incident response drills, and networks of mutual support between councils) significantly reduces the extent of damage that could be caused by incidents (Member, 2024) and people as the center of things-cultivate a culture of security awareness among council staff and leaders is as important as any technical fix (Ashford, 2018; Lance , 2024).

Findings, thus, are aligned with the research objectives of understanding how breaches of cyber in councils are perpetrated and what could be learnt going forward to minimise the potential risks. The outcome is quite clear: even if cyberattacks may be inevitable ("a matter of when, not if", as Gloucester's Director noted), local councils can dramatically improve their defensive posture and response capability by learning from past incidents (Gloucester City Case Study, 2023). The continued improvement of cybersecurity within local government will need continuous learning, investment, and potentially even greater centralised support. Yet, it is an essential endeavour to protect citizens and to build public trust in the digital public service system.

The findings from this review provide valuable insights and lessons that can serve both practitioners charged with the security of IT in councils and researchers striving to close the gap in this critical area of cybersecurity. The following chapter lays out the methodological framework guiding the proposed solutions to address the cyber problem.

3. Methodology

This study provides a brief overview of the systematic approach employed to conduct the research. This study discussed the research philosophy, research approach, methods of data collection, method of data analysis, limitations on the data, reliability and validity of the study and ethical considerations.

3.1 Methodological Approach

A methodical approach known as a systematic literature review was utilised to carry out this study. A systematic literature review follows a transparent and thorough process to find, select, and evaluate pertinent papers that are relevant to a certain topic (Hiebl, 2023). This methodology guarantees that the results are all-encompassing, impartial, and grounded in the most reliable and up-to-date evidence within the respective field (Mahat and Kandel, 2023). Through the implementation of a methodical methodology, this study aims to enhance the credibility and validity of its findings pertaining to the lessons learned from post-incident reviews of cyber breaches in the UK local councils.

3.1.1 Philosophy

The concept of research philosophy is related to a framework of concepts and principles that form the fundamental basis for understanding the nature of the phenomenon being studied (Khatri, 2020).

The underlying research philosophy informing this review is pragmatism. The philosophical stance of pragmatism is deemed suitable for this study due to its emphasis on the practical implications of research and its aim to effectively address the research question by integrating diverse perspectives (Kaushik and Walsh, 2019). The selection of this research philosophy aligns with the notion that post review of cyber breaches can serve as a valuable instrument for mitigating against future attacks in UK local councils (Lee et al., 2023). Thus, factors that warrants post-incident review in UK local councils' compliance was discussed is this study. Within the framework of this research, the pragmatism research facilitates the incorporation of diverse research methodologies and paradigms (Shannon-Baker, 2016), thereby enabling a comprehensive exploration of the lessons learned from post-incident reviews of cyber breaches in the UK local councils.

3.1.2 Research Approach

The fundamental purpose of a research approach within a study is to establish a structured framework for the methodical gathering and examination of data (Tobi and Kampen, 2018). The choice of study methodology significantly influences the type of data to be collected, the methods employed for data collection, and the subsequent analysis (Opoku et al., 2016). Consequently, the selection of a research approach is contingent upon the specific research question being posed (Krehl and Weck, 2020). The study employed a desk-based research methodology, as its research approach. Desk-based research is a form of inquiry that relies on the utilisation of existing data sources, commonly referred to as secondary data (Nyathi and Mathwasa, 2022). The selection of this research methodology was based on its appropriateness for investigating the lessons learned from post-incident reviews of cyber breaches in the UK local councils. Hence, the utilisation of desk-based research facilitates the examination of an extensive array of data within a condensed timeframe.

3.1.2.1 Search Strategy

A comprehensive search was conducted for the literature review, which involved compiling a set of keywords related to the lessons post-incident reviews of cyber breaches in the UK local councils. The procedure started with creating a keyword inventory, which was then input into the research databases. The primary focus of the search process was on scholarly literature pertaining to the post-incident reviews of cyberbreaches of UK local councils, the challenges and benefits associated with its utilisation, and the factors that influence its adoption. Table 3.1 displays the search phrases that emerged throughout the process of fine-tuning the search strategy. The study employed these keywords to obtain entry into Scopus and Pubmed, with the purpose of locating research studies and journal articles pertaining to the given topic.

Table 3.1. Database search keywords and queries.

SN	Database	Search keywords or queries
1	Scopus	*cyber AND breaches AND in AND UK (36)*
2	Scopus	cyber AND breaches AND in AND UK
3	Science Direct	*cyber breaches of UK (1,014)*
4	Science direct	*cyber breaches of UK local council (519)*
5	Science direct	*post review incidence of cyber breaches of UK local council (37)*

3.2 Methods

The research methodology utilised in this systematic literature review is in a qualitative nature. Although systematic reviews typically prioritise quantitative studies (Campbell et al., 2020; Edwards et al., 2018), it is relevant to employ a qualitative approach in this study to facilitate an in-depth exploration of the lessons learned from post-incident reviews of cyber breaches in the UK local councils (Hennessy et al., 2022). This study employed a qualitative systematic literature review methodology in order to consolidate and evaluate studies pertaining to the research topic.

3.2.1 Data collection

The PRISMA (Preferred Reporting Items for Systematic Review and Meta-Analyses), inclusion, and exclusion criteria served as a guide for this phase of the study's data extraction (O'Dea et al., 2021; Page et al., 2021). The process of choosing the relevant literature for this study was also explained using a PRISMA flowchart. The data collection procedure employed in this systematic literature review entails conducting an exhaustive search for relevant scholarly literature. The following procedures were adhered to:

3.2.1.1 Literature Search and Review: A comprehensive exploration was undertaken utilising electronic databases including Scopus and Pubmed. The selection of search terms was conducted with meticulous consideration in order to encompass all relevant research pertaining to the lessons learned from post-incident reviews of cyber breaches in the UK local councils.

3.2.1.2 Inclusion criteria

The inclusion criteria were utilised to make certain that the research papers that were incorporated into the systematic review were relevant to the specific research questions that have been stated (O'Dea et al., 2021). The inclusion criteria for this study are peer-reviewed articles, published in the last 5 years (i.e. between 2019 and 2023), studies specifically conducted within Nigeria and its diaspora, and research that specifically examines the lessons learned from post-incident reviews of cyber breaches in the UK local councils.

3.2.1.3 Exclusion criteria

The researcher employed exclusion criteria to eliminate studies that were deemed irrelevant to the research inquiries or lacked sufficient quality (Cheung et al., 2017). Research articles failing to meet the inclusion criteria will be excluded from the analysis. Furthermore, exclusion may arise in the context of studies that exclusively concentrate on the lessons learned from post-incident reviews of cyber breaches in the UK local councils. In addition, it is imperative that the research papers possess written content that has been published in English language.

3.2.1.4 Quality Assessment: The studies that have been chosen was subjected to a comprehensive evaluation of their methodological rigour and validity (Pati and Lorusso, 2018). The analysis will assign greater importance to studies of superior methodological quality, while studies with inherent limitations was removed.

3.2.2 Method of data analysis

The explanatory variables on the variables were evaluated using thematic and critical analysis.

3.2.2.1 Thematic analysis: Thematic analysis was employed for the data analysis in this systematic literature review. Thematic analysis is a qualitative data analysis technique that entails the identification, coding, and categorization of themes within the dataset (Castleberry and Nolen, 2018). The identified themes in the collected information were subsequently utilised to enhance the lessons learned from post-incident reviews of cyber breaches in the UK local council (Xu and Zammit, 2020). The present study aims to identify and synthesise themes derived from the selected literature, thereby facilitating the systematic organisation and presentation of findings pertaining to the lessons learned from post-incident reviews of cyber breaches in the UK local councils.

3.2.2.2 Critical Analysis: During data analysis, a rigorous critical examination will be conducted to assess the merits, limitations, and ramifications of the studies that have been incorporated (Lawless and Chen, 2019). This will necessitate the examination of various factors, including the sample's representativeness, the research design employed, the methods used for data collection, and the limitations inherent in each study.

3.2.3 Evaluation of Research Studies: The PRISMA Structure

The PRISMA framework, known as the Preferred Reporting Items for Systematic Reviews and Meta-Analyses, offers a comprehensive and methodical outline of the process involved in conducting a review (Page et al., 2021). The PRISMA guidelines were adhered to by following the following steps.

1. Identification: The preliminary exploration of electronic databases and scholarly journals yielded a total of 1,607 articles that could potentially be relevant to the research topic.

2. Screening: Screening was conducted by evaluating the titles and abstracts of the articles that remained, furthermore screening was done in accordance with the predetermined inclusion and exclusion criteria, quality assessment and then duplicate removal. After completing this procedure, a total of 25 articles were chosen for a comprehensive evaluation of their full texts.
3. Eligibility: The assessment of the full text was performed in order to ascertain the eligibility of the 25 articles. The systematic literature review included studies that satisfied the specified inclusion criteria. Consequently, a total of 5 articles were incorporated.
4. Inclusion: The 5 articles included in this study offer valuable insights into the lessons learned from post-incident reviews of cyber breaches in the UK local councils
5. Exclusion: From the initial retrieved 1,607 articles from database search a total of 1,602 were excluded at different point of the search flow (See Figure 3.1).
6. Data Extraction: The process of data extraction involved the identification and retrieval of pertinent information from the studies included in the analysis. This information was then systematically organised and compiled into a synthesis table (See Appendix B), which served as a tool for the analysis and presentation of the research findings.
7. Quality Assessment: The assessment of the methodological quality of the studies included in the analysis was conducted in order to gauge the robustness and dependability of the results.

The primary investigation was carried out on two prominent electronic publication databases, Scopus and ScienDirect, and scholarly journals focused on computer data. The search strategy employed a hybrid approach incorporating both keywords and subject terms pertaining to the topics of "post review incidence," "data breaches,". A comprehensive examination resulted in the identification of a total of 1,607 prospective articles.

3.2.4 Limitations on the data

The systematic literature review process encountered various limitations that can potentially affect the breadth and depth of the findings (Williams et al., 2021), they include;

3.2.4.1 Bias: It is possible that the existing literature on the lessons learned from post-incident reviews of cyber breaches in the UK local council is influenced by publication bias, wherein studies with positive or significant findings are more likely to be published, which may result in an incomplete representation of these attitudes (Marks-Anglin and Chen, 2020).

3.2.4.2 Quality: The heterogeneity in the quality of the studies included in the analysis may affect the reliability and relevance of the results (Mokkink, et al. 2020).

3.2.4.3 Literature Availability: The review may be impacted by the limited availability of literature pertaining to the specific topic of interest (Mokkink, et al. 2020).

3.3 Ethical consideration

The fundamental principle underlying ethical considerations in research is to guarantee that the research being conducted is carried out in a manner that upholds the rights and well-being of all individuals involved (Sherwood and WeCare, 2020). Ethical considerations hold significance as they serve to safeguard participants against potential harm and exploitative behaviour, while also enabling researchers to uphold responsible and ethical conduct

throughout their work (Różyńska, 2021). The researcher took measures to ensure the appropriate citation and acknowledgement of all sources utilised to prevent instances of plagiarism.

3.4 Conclusion

The chapter's conclusion provides a summary of the methodological approach employed in this systematic literature review, which encompasses data collection, analysis approaches, restrictions, and ethical considerations. In light of the data breaches in UK local council, the study adheres to stringent requirements to provide a comprehensive and ethical examination of the lessons learned from post-incident reviews of cyber breaches in the UK. The technique and ethical considerations mentioned here are crucial for generating reliable and ethically sound study findings, which can shape future policies and actions

4. Design and Implementation

This chapter focuses on the result of the systematic literature review, analysis and the development of the proposed framework solution for the research project. Then the results of the analysis are discussed concerning the research objectives.

4.1 The SLR Process: PRISMA FLOW

The PRISMA diagram presented (see Figure 4.1) outlines the systematic process of literature selection for the research, detailing the flow of information through the various stages of the review starting from the database search down to the inclusion of the required research articles for analysis. As shown in Fig. 4.1, at the end of the literature search process only 5 articles were deemed relevant to be included in the research analysis.

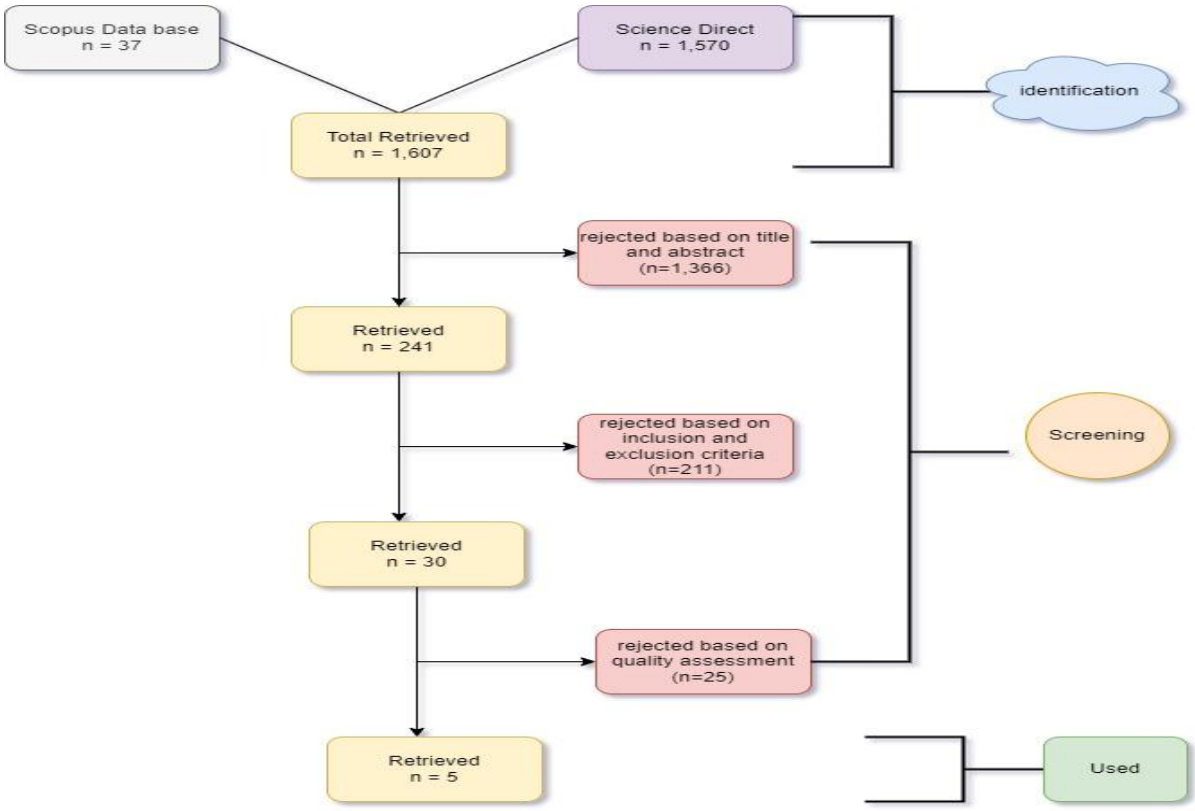

Figure 4.1. PRIMAS flow research process.

4.2 Data Extraction

Table 4.1 in the publication is a crucial element in the systematic review, illustrating the process of gathering data from the selected studies that are pertinent to the research objectives. Each study undergoes rigorous scrutiny to discover and evaluate key components of management that contribute to an understanding of the research issue. The table provides a concise summary of study references, encompassing their objectives, techniques, important findings, and the reasons for data breaches in UK local councils.

Table 4.1 Data extraction

Author/Year	Title	Findings	Key implication
Pool et al. (2024)	Challenges of organisation control in healthcare information security.	- behavioural patterns of management, lack of compliance, and employee attitudes were leading factors that prompts hackers access to firm data. - As such, firms are faced with constant privacy intrusion, DDoS attacks and ransomware attack	- lack of coordination and communication between different departments emerged as a major barrier in the organisation.
Patel et al. (2023)	Ways in which companies control and manage the data security of healthcare in the light of the instantaneous world of technology	- healthcare organisations should strengthen their policies - practice good procedural approaches in information security	- Issues with implementation, - enforcement of information security, - poor organisational policies, - managing third-party vendors, and - inaccurate responding to security incidents
Nifakos et al. (2021)	Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review	The study resolve into some commonly cyberthreats classification like - attacks that exploit IT infrastructure, vulnerabilities resulting from misconfigurations of network components, such as firewalls, overwhelming digital services by flooding requests (denial of service (DoS), DDoS), software bugs in the system (SQL) injections, man-in-the-middle (MITM) or eavesdropping; - ransomware attacks being launched against healthcare organisations, with the intention of causing service disruption and holding the healthcare organisation data hostage for economic gains; - the emerging threat of exploiting human vulnerability in gaining access to healthcare infrastructure are common threats evidence in the study	The review pointed out a lot of issues like; - unprofessional social media access by organisation staff, economical and societal issue, - incessant attacks like Distributed Denial of Service (DDoS), add to the complexity of IAM among healthcare firms.
Ghadge (2024)	Enhancing threat detection in Identity and Access Management (IAM) systems	The research presented issues such as; - poor organisational guidelines - ransomware attacks - bad policy change, and	The study found that healthcare organisations should focus on;

		- traditional network system are prevalent among firms as the obstacles to the successful implementation of IAM among healthcare information security	- the training and education of their staff for the sake of awareness and to guarantee the successful implementation of IAM.
Kessler et. al (2019)	information security climate and the assessment of information security risk among healthcare employees	The researchers aver that; - the organisation culture, - control of legal compliance - employee attitudes and were associated with the issue of information security challenges	- Improved organisational culture/climate - Employee trainings
da-Veiga et al. (2020)	Social aspects of organisation control in the field of healthcare information security	The study found that organisations are faced with constants - ransomware attacks, - DDoS Which was resulted due to poor organisational culture, inadequate leadership support, and poor employee attitudes are significant challenges and practices of information security in the operations of healthcare firms	- the research showed a sparing security in the health sector - and that health organisations should instigate a practice of security awareness.
Dong et al. (2019)	Organisation control of data security in a healthcare setting.	- The study found a security strategy which in turn could be aligned with their business goals, - apply risk management practices that are both robust and capable of addressing any weaknesses, and - discipline employees who may be responsible for security breaches.	- The study uncovered primary issues of the control of the organisation - the failure to follow an efficient security strategy and - the absence of accountability for security breaches
Zhou et al. (2019)	The challenges of organisation control in healthcare information security	- health institutions should develop a security strategy that aligns with their business objectives - implement robust risk management practices - and take a strict approach at the individual level to security breach	- It was shown that the fast pace of advancement in the technology of the healthcare sector was one of the major factors allowing for the problems of security breeches - Poor risk management practices - Constant surfing of social media
Yeng et al. (2019)	The challenges of organisation control in the field of healthcare information security	The study concludes that healthcare organisations have; - a difficulty in devising and enforcing information security policies, - managing third-party vendors, and - difficulty in handling security incidents	Lapses in information security policies through implementation of the correct procedures

Source: Researcher's compilation (2025)

4.3 Data Extraction and Analysis

Table 4.2 presents the methodical procedure employed to gather relevant data from the chosen studies. The data extraction process involves analysing each study to identify and collect

pertinent information such as the authors, publication year, study context, research techniques, participants, findings, and significant conclusions. This procedure guarantees that every literary work contributes to a logical and full integration of data. The techniques of extracting and coding data are crucial for improving the transparency and credibility of the synthesis. Additionally, they offer stakeholders clear and practical insights into the study's emphasis.

Table 4.2 Data extraction and Coding

Author/Year	Theme	Sub-theme	Code	Quote	Pages
Pool et al. (2024)	A systematic analysis of failures in protecting personal health data: A scoping review	Personal health data breaches; a challenge to healthcare providers and clients	Data shortcomings	"Personal health data breaches are particularly consequential and can cause serious harm to individuals"……	p. 1, 2, 11
Ghadge (2024)	Enhancing threat detection in Identity and Access Management (IAM) systems	automated reasoning techniques for threat detection in IAM systems	IAM and threat detection	"Traditional network security solutions cannot adequately detect and prevent these attacks"…	p. 2
Aboukadri et al. (2024)	Machine learning in identity and access management systems: Survey and deep dive	the fusion of machine learning (ML) techniques to fortify IAM	ML-based solutions	"…..Identity is a digital representation formed by combining the unique attributes of an individual"…..	p.2
Nifakos et al. (2021)	Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review	commonly encountered factors of cybersecurity postures of a healthcare organisation	Cyber Security	"At every step of the systematic review process, all the information was stored in the Rayyan platform. Rayyan is an online collaborative platform that supports the filtering process carried out among the researchers "…..	p.2,7
Singh et al. (2023)	IAM identity access management—importance in maintaining security systems within organisations	The importance of IAM and Security Systems within Organisations	IAM and information security	" 'Okta' is such an IAM platform that can be used easily and neutrally with all relevant existing solutions, which selects the best technologies"….	p.2

Source: researcher's compilation (2025)

4.4 Quality Assessment

This process involves appraising and documenting the literature used for this study by doing quality assessment to each research paper used. Using JBI critical appraisal questions (table 4.4), it was shown in the literature reviewed that there was congruity between the research objectives and the methodology in the study of Pool et al. (2024); Ghadge (2024); Aboukadri, (2024) Nifakos et al. (2021) and Singh et al. (2023). Also, the data extraction methods, were appropriate for all the studies used in addition to the thematic findings which were supported by the data quoted by all the study.

However, it was only the study of Ghadge (2024); Nifakos et al. (2021) and Singh et al. (2023) that met the evidence of saturation for the identified themes and sub-themes, the other studies were limited in findings. Additionally, the study of Pool et al. (2024) and Singh et al. (2023) did not have clear ethical considerations of the original studies addressed and aligned with current criteria, whereas the study of Ghade (2024), Aboukadri et al (2024) and Nifakos et al. (2021) met this criterion.

In view of this, all the studies met the coding scheme consistency which were applied across the studies. Also, the study met necessary participants' quotes that was used to support the themes and sub-themes identified. The page numbers provided for all quotes to ensure transparency in data extraction and the conclusions drawn in the research reports which were align with the themes and sub-themes extracted from the analysis met all the studies criteria.

Table 4.3a. JBI Critical Appraisal

JBI Critical Appraisal Checklist Questions	Study 1 (Pool et al. 2024)	Study 2 (Ghadge 2024)	3 (Aboukadri et al. 2024)	Study 4 (Nifakos et al. 2021)	Study 5 (Singh et al. 2023)
1. Is there congruity between the research objectives and the methodology?	✓	✓	✓	✓	✓
2. Are the data extraction methods appropriate for the research methodology?	✓	✓	✓	✓	✓
3. Is there congruity between the data extraction process and the representation and analysis of data?	✓	✓	✓	✓	✓
4. Are the thematic findings supported by the data quoted in the study?	✓	✓	✓	✓	✓
5. Is there evidence of saturation for the identified themes and sub-themes?	Limited	✓	Limited	✓	✓
6. Is the coding scheme consistently applied across the studies?	✓	✓	✓	✓	✓
7. Are participants' quotes used to support the themes and sub-themes identified?	✓	✓	✓	✓	✓
8. Are page numbers provided for all quotes to ensure transparency in data extraction?	✓	✓	✓	✓	✓
9. Are the ethical considerations of the original studies addressed and aligned with current criteria?	Unclear	✓	✓	✓	Not clear
10. Do the conclusions drawn in the research reports align with the	✓	✓	✓	✓	✓

themes and sub-themes extracted from the analysis?					

Source: Researcher's compilation (2025)

Table 4.3b. Quality Appraisal of Selected Studies

Citation	Author(s)	Year of Publication	Objective of Study	Study Design	Methodological Quality	Relevance
Pool et al. (2024)	Pool et al.	2024	A systematic analysis of failures in protecting personal health data: A scoping review	The study conducted a scoping review, a research approach employed to investigate a broad issue using diverse research methodologies and address extensive research enquiries.	High; utilises robust statistical analysis and targeted surveying	Highly relevant; directly assesses trade-offs of safety protocols
Ghadge 2024	Ghadge	2024	Enhancing threat detection in Identity and Access Management (IAM) systems	machine learning methods using input data to classify or make decisions	Moderate; could benefit from larger sample size but provides in-depth qualitative data	Highly relevant; provides insights into practical challenges of implementation
Aboukadri et al. 2024	Aboukadri et al.	2024	Machine learning in identity and access management systems: Survey and deep dive	ML-based solutions within IAM systems	Moderate to high; substantial sample size	Highly relevant; addresses the gap between knowledge and practice
Nifakos et al. 2021	Nifakos et al.	2021	Influence of human factors on cyber security within healthcare organisations: A systematic review	Qualitative research, semi-structured interviews	High; provides in-depth analysis of cyberthreat challenges	Relevant; suggests structural changes on how to mitigate threats in the healthcare sector and how to improve health and safety
Singh et al. 2023)	Singh et al.	2023	IAM identity access management importance in maintaining security systems within organisations	The importance of IAM and Security Systems within Organisations	High; innovative approach with precise measurement tools	Highly relevant; focuses on AI as a metric to mitigate issues of IAM in any organisation

Source: Researcher's compilation (2025)

4.6 Title Keywords

Figure 4.3 presents a word cloud analysis based on the titles of the selected articles. The research reveals that although "cybersecurity" has the highest frequency, when it comes to common attacks words such as "Wannacry", "DDoS", "phishing", etc are also common. This guides the development of the framework.

Figure 4.3. title keywords word cloud (Source: Researcher Computation, 2025)

4.6 Design Stage

The framework as shown in the Fig. 4.4, showed that there are four major challenges that UK healthcare firms encounter which varies from poor management practices, non- regulatory compliance, attacks due to vulnerabilities and using of traditional security approach. These practices pave way to attacks and vulnerabilities among healthcare firms. However, the study proffer solutions that incorporate user authentication, integration of SSO solutions to simplify authentication and access management across multiple applications among other mitigation measures.

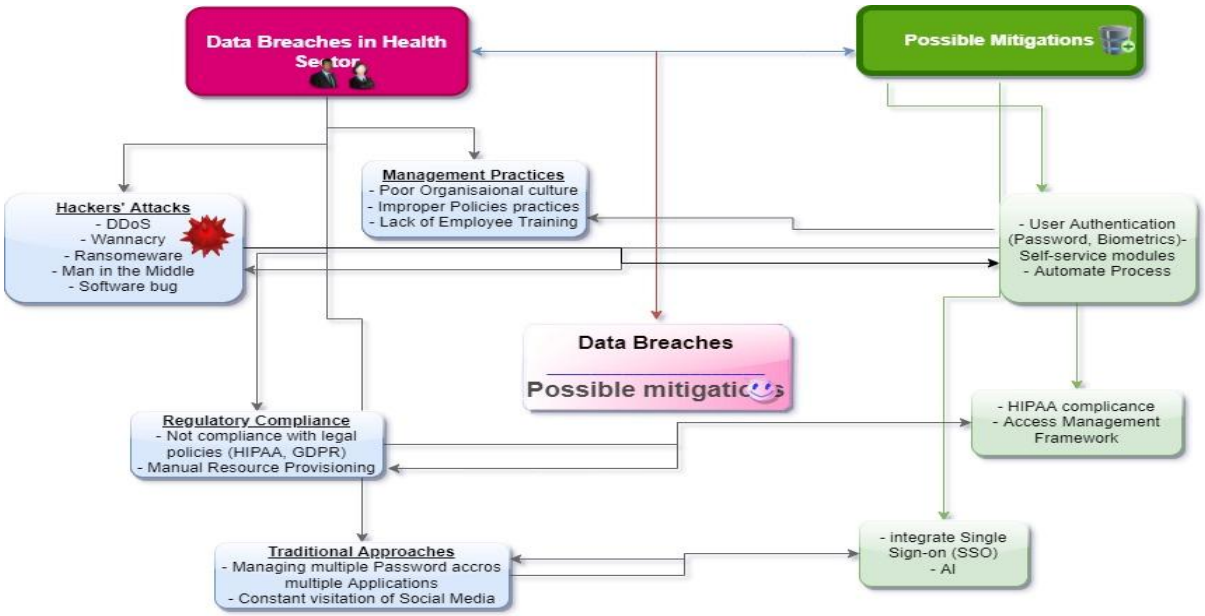

Figure 4.4: framework for data breaches security challenges and mitigations measures (Source: Researcher's design, 2025)

5. Evaluation, Comparative Analysis and Strength of the Framework

This section starts by documenting the conceptual model used in the creation of the proposed framework in chapter 4. Then the results based on each of the research papers were documented which is then proceeded to discuss the findings in relation to the research questions presented in the chapter 4 of this study.

To evaluate the framework in the previous chapter, a hypothetical healthcare named WeCare Hospital was used. Figure 5.1 shows an attempt by an attacker to infiltrate the WeCare hospital. In the figure 5.1 the attacker can bypass the security layer using either of the DDoS, Wannacry, SQL Injection, among others. to infiltrate the company.

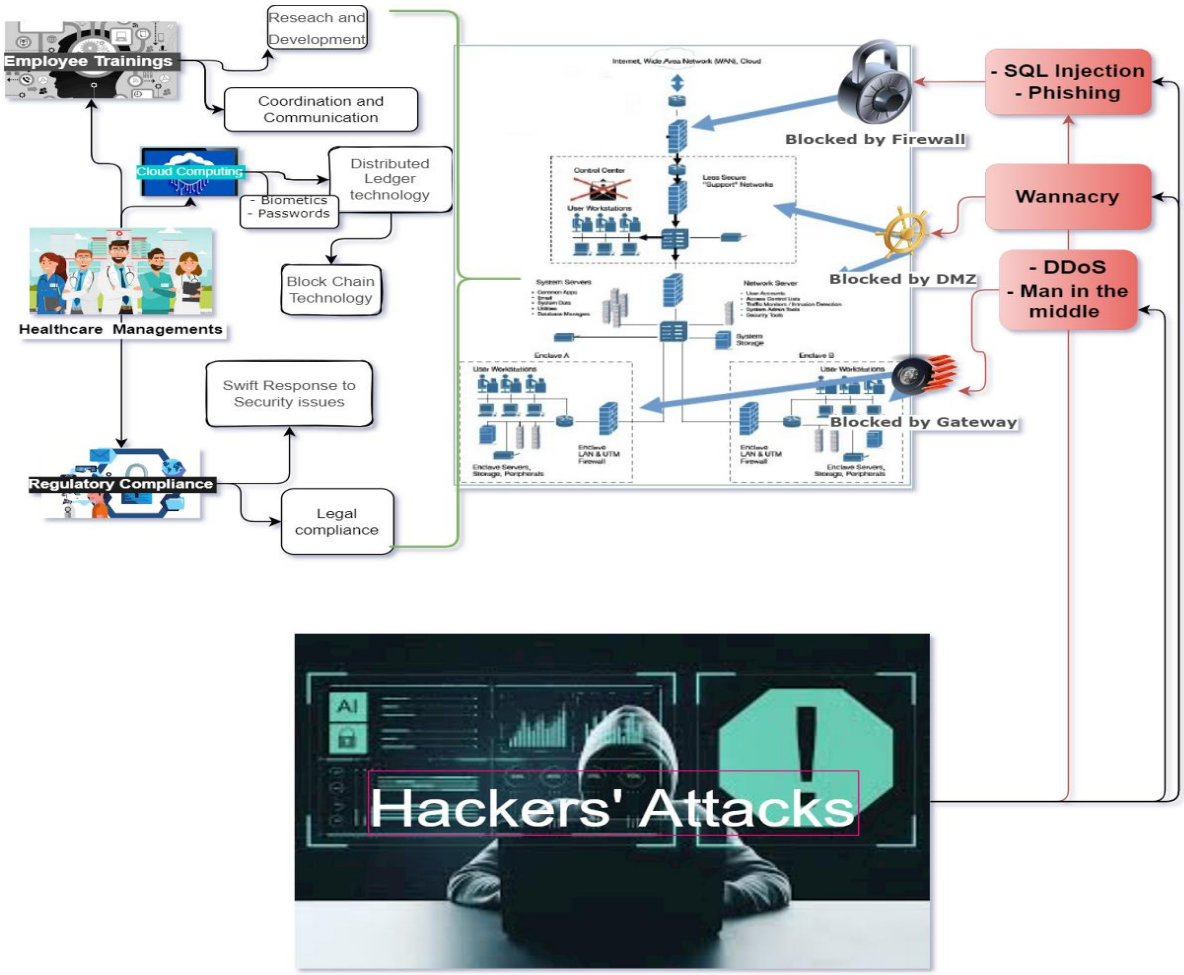

Figure 5.1. Imagined scenario on WeCare's Hospital.

5.1 Framework Evaluation

Mitigations measures in the healthcare sector are vital in the protection of sensitive data and maintaining standards of healthcare according to regulations such as Health Insurance Portability and Accountability Act. In this regard, the framework assessment in healthcare mainly dwells on organizational control effectiveness relating to securing data, prohibiting unauthorized access, and ensuring that access to information is restricted to the right staff. Authentication, Authorization, Access Control Policies, monitoring, and compliance were all assessed. The documentation of this framework is made available in appendix A of this study.

1. Authentication Mechanisms

This study described authentication as the first line of defense in mitigating data breaches, ensuring that only verified users may have access to healthcare systems. There are several ways to check the identity of the user in the healthcare industry among are;

- Single sign-on: This helps users to login to several healthcare applications with credentials from their mobile security app so as to reduce chances of password fatigue and to increase security.

- MFA: Adds more protection to the accounts by implying measures which are more than a combination of a username and password.

- Biometric Authentication: There builds upon unique biology as a foundation, for instance, through fingerprints or retina scans; very pertinent, for instance, in security-sensitive contexts, for instance, in systems involving patients' records or medication.

2. Access Control Policies

Security policies relate to aspects such as rights and privileges of users in relation to healthcare data and systems. Such policies should be such that they secure data and at the same time do not hinder the flow of activities in the healthcare systems.

- Time-Based Access: This means access can be limited at certain time for example for those systems that are not required to be accessed all the time.

- Contextual Access: They can give or deny one permission depending on where they are, which device they use or any other factors.

- Emergency Access (Break-Glass): In emergency conditions there are extraordinary operations that permit certain personnel-defined users to enter into the system despite restrictive measures.

Evaluation: There is a need to ensure that access controls in the frameworks operating in healthcare organizations reflect on ways of managing context and emergencies. These policies should ideally be reviewed periodically so as to suit the current security requirements and standards.

3. Compliance with Regulations

Highly regulated industry whereby treatment of data is strictly controlled based on healthcare standards of data protection and privacy. The regulations highlighted above, ought to be met by the frameworks.

- Data Encryption: To improve data security healthcare sensitive data should therefore be encrypted when in use via the internet as well as when stored.

- Data Minimisation: Makes sure that the organisation only processes, collect and store data that is essential to the functioning of the organization to minimize on data breach incidences in the organization.

5.2 Comparative Analysis of the Data breaches Framework

5.2.1 Comparative Analysis of the Framework

In evaluating the framework developed, it is crucial to examine its performance relative to other frameworks currently used in industry. This analysis focused on the key aspects of authentication mechanisms, and regulatory compliance, while incorporating insights from recent studies in the field.

1. Authentication Mechanisms

The developed framework integrates advanced authentication methods, including single sign-on (SSO), multi-factor authentication (MFA), and biometric authentication, providing a robust security infrastructure. These mechanisms enhance both security and the user experience, addressing issues such as password fatigue prevalent in healthcare settings. However, the implementation of biometric authentication, while offering high security, can be financially challenging for smaller healthcare facilities.

In contrast, recent research by Alamri et al. (2022) explores blockchain-based identity management systems in health IoT applications. This study highlights the advantages of decentralised security systems in healthcare, where blockchain technology is employed to enhance security and reliability in IoT devices used in healthcare environments. While blockchain-based systems offer a forward-looking approach with decentralised control, they currently lack comprehensive security frameworks and require further development to match the practicality of established systems (Alamri et al., 2022). Therefore, while blockchain presents an innovative alternative, the developed framework's focus on mature, albeit costly, technologies like biometrics offers immediate and reliable security benefits.

2. Compliance with regulations

Compliance with healthcare regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), is a critical component of the developed framework. It is designed to meet stringent regulatory requirements, including data encryption, data minimisation, and regular compliance audits. These features are crucial in reducing legal risks and maintaining patient trust, particularly in a heavily regulated industry like healthcare.

The study by Ansari et al. (2022) introduces a privacy-enabling framework for cloud-assisted digital healthcare systems, focussing on ensuring patient and doctor anonymity, unlikability, and data confidentiality through advanced encryption and security protocols. While this framework demonstrates robust security features, it is primarily focused on cloud-based systems, which may not fully address the on-premises and hybrid environments typical in many healthcare organisations (Ansari et al., 2022). The developed framework approach to compliance offers broader applicability across different healthcare IT environments, making it a more versatile solution for immediate implementation.

Adaptive Access Control Policies:

The framework's ability to implement contextual and time-based access controls adds a vital layer of security, ensuring that access is restricted to specific contexts and times that are deemed safe. The inclusion of an emergency access (break-glass) feature is particularly significant, allowing healthcare providers to quickly access critical data during emergencies without compromising overall security. This approach aligns with findings from studies on advanced systems, which advocate for contextual access controls as a means to enhance security while maintaining necessary access during critical situations (Alamri et al., 2022).

Scalability and adaptability:

Designed with scalability in mind, the framework can support organisations ranging from small healthcare practices to extensive hospital networks. Its adaptability ensures continued effectiveness as the healthcare environment evolves, particularly in response to changing regulatory requirements and emerging security threats. This characteristic is supported by evidence from the deployment of systems in diverse healthcare settings, where scalability and adaptability are essential for maintaining security across various operational scales (Ansari et al., 2022).

5.3 Answers to the research questions

i. Identify the common causes and contributing factors of cyber breaches in UK local councils.?

Healthcare organisations in the UK are challenged by the inherent complexity of integrating various systems and technologies. Healthcare institutions typically operate numerous, often incompatible, information systems, each requiring distinct access protocols. This complexity creates potential security gaps, as inconsistencies in implementations across different platforms can lead to vulnerabilities. Ensuring seamless integration and uniform security standards across all systems remains a significant obstacle, particularly in large healthcare organisations where multiple departments may use disparate systems.

Human factors also present a critical factor to healthcare settings. The effectiveness of any solution is heavily dependent on user compliance, yet healthcare staff often prioritise convenience over security, leading to risky behaviours such as sharing passwords or bypassing multi-factor authentication for expedience. Moreover, a general lack of cybersecurity awareness among healthcare workers exacerbates this issue, making the organisation more susceptible to social engineering attacks and other forms of cyber threats.

Finally, financial and resource constraints significantly impede the implementation of advanced systems in healthcare. While large institutions may have the resources to invest in comprehensive security solution, smaller organisations often struggle with the costs associated with deploying and maintaining such systems. This financial burden can result in the adoption of less effective security measures, leaving these organisations more vulnerable to breaches.

ii. How effective are the incident response strategies employed by local councils in the aftermath of a breach?

Local councils need to build complete organisational frameworks which specify the security breach response procedures and protocols. A prepared plan should permit staff to identify breaches followed by containment measures and establish protocols to notify stakeholders and lead response efforts. The influence of the framework on lowering security breaches and enhancing general information security helps one to evaluate its efficiency in the healthcare industry. A well-made framework should cause a clear decrease in unauthorised access rates, therefore safeguarding private patient information and preserving the integrity of healthcare information systems.

For example, models including dynamic multi-factor authentication are especially successful in stopping breaches by guaranteeing that only authorised users have access to vital systems and data. Crucially, another indicator of the framework's success is its capacity to guarantee

adherence to healthcare standards. Following rules like HIPAA not only shields the company from legal fines but also builds patient confidence by securing their confidential medical records. Features that automate compliance activities—such as regular audits and real-time access log monitoring—will be part of an efficient security system, therefore guaranteeing constant conformity to legal obligations.

iii. What are the key challenges and barriers to effective cybersecurity in local councils?

Local councils currently face strong challenges because their cyber security budget remains inadequate. Local councils usually handle their operations while operating under constrained budget restrictions which restrict their ability to establish strong cyber security measures. Local councils become exposed to cyber-attacks because they lack sufficient detection and prevention technology despite their vulnerable situation. Local health care councils in UK face important challenges because of the complex advancement of cyber threats. Local health care councils in UK struggle to protect their security systems because cyber criminals continuously invent new methods to penetrate systems. The cyber security threat to local councils is worsened by their high dependency on third-party contractors and need to connect with suppliers from multiple parties. The sharing of council data with external partners creates additional risks since poor security protection at those partners could result in breaches of protected data. The limited control that councils have over third-party security practices becomes an obstacle to maintaining their data protection.

Local councils need to make cyber security a fundamental operation framework due to existing challenges and obstacles. To safeguard their data local councils must purchase required protective resources and technologies together with implementing complete staff training and awareness programs. Local councils operating in UK territory should schedule periodic assessments of their security programs which must include updates to counter fresh threats along with developing weaknesses in their systems.

5.4 Summary of Findings

Organisations in the local council alongside all other sectors face major risks from cyber breaches. The United Kingdom council health sector experienced multiple major cyberattacks during recent years which resulted in the unethical access of sensitive patient information and service disruptions in critical healthcare operations. Post-incident reviews establish that organizations performed investigations about the breach sources and developed preventive solutions against future incidents.

The UK council health sector revealed through post-incident reviews that strong cybersecurity practices remain an essential element to handle cyber breaches. The sector shows numerous organizations possess poor cybersecurity defenses because they maintain outdated systems as well as weak password protections and they lack encryption system protocols. The established vulnerabilities enable cyber attackers to access unauthorized critical information and control systems.

The outcome of post-incident reviews demonstrates that organizations need to enhance their training initiatives for staff alongside increasing their cybersecurity literacy. Human mistakes cause most cyber breaches when employees allow attackers to phish them or download malicious software by accident. Organizations decrease successful cyber assault chances when

they conduct frequent cybersecurity education for their staff members and show them the dangers of cyber threats.

Post-incident reviews confirm that organizations must perform frequent security assessments together with audits for their systems. Organizations across the UK council health sector exhibit poor capability to detect and respond to cyber threats because they lack proper monitoring systems.

6. Conclusion

This research successfully achieved the goal of assessing the lessons learned on the post incidence review of data breaches in UK council for healthcare information security. Starting with the systematic literature review (SLR), the most often occurring hackers' attacks encompasses Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, man-in----middle attacks, and malware injections were fully understood. These results prepared the way for the creation of a new framework on how management can mitigate these threats.

The framework, which leverages real-time processing and adaptive learning, demonstrated significant strengths during its evaluation. In data security solution, where security breaches can quickly spread and inflict extensive damage and loss of data, real-time threat detection and response capability is vital.

An effective framework is vital for the security and privacy of healthcare information. By implementing robust identification, authentication, and authorization mechanisms, healthcare organizations can protect sensitive data, comply with regulatory requirements, and enhance operational efficiency. As such, regular risk assessments, policy updates, and staff training are essential to maintaining a secure security environment. Addressing these difficulties and focusing on areas of development in security feedback for healthcare information are essential for safeguarding sensitive health data and ensuring compliance with regulatory requirements. By investing in advanced technologies, standardizing practices, and fostering a culture of security awareness, healthcare organizations can significantly enhance their security capabilities and overall information security posture.

6.1 Future Work and Insights

Looking ahead, the framework may be strengthened in a few spots. Integration of the framework in the healthcare industry is one of the main areas that has to be improved. Many sectors, including healthcare, still depend on more antiquated systems that might not be completely compliant with the most recent security regulations. Its use would be much expanded by developing lightweight versions of the framework or modular components that could be readily connected with current systems.

The next step would be doing thorough real-world testing of the framework across several security contexts with more time, money, resources, and partners. This would offer insightful analysis of its performance in several settings and assist to improve the framework to handle any constraints found during these testing. Further improving the efficacy of the framework would be the inclusion of the most recent developments in cybersecurity and identity and access technologies by means of cooperating with other researchers and industry professionals.

References

1) Al Kinoon, M. (2024). A Comprehensive and Comparative Examination of Healthcare Data Breaches: Assessing Security, Privacy, and Performance. Graduate Thesis and Dissertation 2023-2024. [online] Available at: https://stars.library.ucf.edu/etd2023/110/.
2) AlGhamdi, A.A., Niazi, M., Alshayeb, M. and Mahmood, S. (2024). Organizations' readiness for insider attacks: A process-oriented approach. Software Practice and Experience, 54(8), pp.1565–1589. doi:https://doi.org/10.1002/spe.3327.
3) Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A. and Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics, [online] 12(6), pp.1–42. doi:https://doi.org/10.3390/electronics12061333.
4) Beretas, C. (2024). Information Systems Security, Detection and Recovery from Cyber Attacks. Universal Library of Engineering Technology, [online] Volume 1(Issue 1). Available at: https://ulopenaccess.com/ulpages/fulltextUlete?PublishID=ULETE20240101_005.
5) Bose, B., Avasarala, B., Tirthapura, S., Chung, Y.-Y. and Steiner, D. (2017). Detecting Insider Threats Using RADISH: A System for Real-Time Anomaly Detection in Heterogeneous Data Streams. IEEE Systems Journal, 11(2), pp.471–482. doi:https://doi.org/10.1109/jsyst.2016.2558507.
6) Brett, M. (2022). Enabling cyber incident collaboration in UK local government thro...: Ingenta Connect. [online] Ingentaconnect.com. Available at: https://www.ingentaconnect.com/content/hsp/jcs/2022/00000005/00000003/art00006 [Accessed 22 Feb. 2025].
7) Butt, U.J. (2023). Developing a usable security approach for user awareness against ransomware. [online] bura.brunel.ac.uk. Available at: https://bura.brunel.ac.uk/handle/2438/26661.
8) Dasgupta, D., Akhtar, Z. and Sen, S. (2020). Machine learning in cybersecurity: a comprehensive survey. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 19(1), p.154851292095127. doi:https://doi.org/10.1177/1548512920951275.
9) Dib, M. and Pierre, S. (2023). Insider Attack Model Against HSM-Based Architecture. IEEE Access, 11, pp.86848–86858. doi:https://doi.org/10.1109/access.2023.3304994.
10) Elendu, C., Omeludike, E.K., Oloyede, P.O., Obidigbo, B.T. and Omeludike, J.C. (2024). Legal implications for clinicians in cybersecurity incidents: A review. Medicine, [online] 103(39), pp.e39887–e39887. doi:https://doi.org/10.1097/md.0000000000039887.
11) Hallows, R. (2020). Securitisation and the Role of the State in Delivering UK Cyber Security in a New-Medieval Cyberspace. [online] Available at: http://bear.buckingham.ac.uk/557/1/1502910%20Securitisation%20and%20the%20Role%20of%20the%20State%20in%20Delivering%20UK%20Cyber%20Security%20in%20a%20New-Medieval%20Cybersp.pdf.
12) Hossain, S.T., Yigitcanlar, T., Nguyen, K. and Xu, Y. (2023). Cybersecurity in Local Governments: A Review and Framework of Key Challenges. [online] doi:https://doi.org/10.2139/ssrn.4631885.

13) Hossain, S.T., Yigitcanlar, T., Nguyen, K. and Xu, Y. (2024). Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. Applied Sciences, [online] 14(13), p.5501. doi:https://doi.org/10.3390/app14135501.
14) Ibrahim, A., Thiruvady, D., Schneider, J. and Abdelrazek, M. (2020). The Challenges of Leveraging Threat Intelligence to Stop Data Breaches. [online] Semantic Scholar. doi:https://doi.org/10.3389/fcomp.2020.00036.
15) Khattabi, N. (2019). COULD SYSTEM-FOCUSED INCIDENT REVIEW IN HEALTHCARE BRIDGE THE GAP BETWEEN THE 'WORK-AS- IMAGINED' AND 'THE WORK-AS- DONE'? [online] Available at: https://lup.lub.lu.se/student-papers/record/8994089/file/8994090.pdf [Accessed 9 Feb. 2025].
16) Lehto, M. (2022). Cyber-Attacks Against Critical Infrastructure. Computational Methods in Applied Sciences, 56, pp.3–42. doi:https://doi.org/10.1007/978-3-030-91293-2_1.
17) Maasberg, M., Warren, J. and Beebe, N.L. (2015). The Dark Side of the Insider: Detecting the Insider Threat through Examination of Dark Triad Personality Traits. 2015 48th Hawaii International Conference on System Sciences. doi:https://doi.org/10.1109/hicss.2015.423.
18) Mamidanna, S.K., Reddy, C.R.K. and Gujju, A. (2022). Detecting an Insider Threat and Analysis of XGBoost using Hyperparameter tuning. 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), pp.1–10. doi:https://doi.org/10.1109/accai53970.2022.9752509.
19) McCreight, R. (2023). Gauging the Impact of Satellite & Space Systems on Critical Infrastructure[CI]: Risk Management is Neither an Enigma nor a Mystery for CI Systems Security. Journal of Homeland Security and Emergency Management, 20(2), pp.183–208. doi:https://doi.org/10.1515/jhsem-2022-0054.
20) Michail, A. (2020). TACKLING THE CHALLENGES OF INFORMATION SECURITY INCIDENT REPORTING: A DECENTRALIZED APPROACH. [online] Available at: https://repository.uel.ac.uk/download/9c570940f180b4fe5201dd0579a05625d8784d0729bab6aeff1b7676ffd7ac32/5157004/2020_DProf_Michail.pdf.
21) Moore, G., Khurshid, Z., McDonnell, T., Rogers, L. and Healy, O. (2023). A resilient workforce: patient safety and the workforce response to a cyber-attack on the ICT systems of the national health service in Ireland. BMC Health Services Research, 23(1). doi:https://doi.org/10.1186/s12913-023-10076-8.
22) Mott, G., Nurse, J.R.C. and Baker-Beall, C. (2023). Preparing for future cyber crises: lessons from governance of the coronavirus pandemic. Policy Design and Practice, 6(2), pp.1–22. doi:https://doi.org/10.1080/25741292.2023.2205764.
23) Naik, N., Jenkins, P. and Savage, N. (2018). Threat-Aware Honeypot for Discovering and Predicting Fingerprinting Attacks Using Principal Components Analysis. 2018 IEEE Symposium Series on Computational Intelligence (SSCI), IEEE Xplore, pp.623–630. doi:https://doi.org/10.1109/SSCI.2018.8628658.
24) Patterson, C.M., Nurse, J.R.C. and Franqueira, V.N.L. (2024). 'I don't think we're there yet': The practices and challenges of organisational learning from cyber security incidents. Computers & Security, [online] 139(1), p.103699. doi:https://doi.org/10.1016/j.cose.2023.103699.

25) Priya, D.V.S., Sethuraman, S.C. and Khan, M.K. (2023). Container security: Precaution levels, mitigation strategies, and research perspectives. Computers & Security, [online] 135, p.103490. doi:https://doi.org/10.1016/j.cose.2023.103490.
26) Rajesh Kanna, P. and Santhi, P. (2024). Exploring the landscape of network security: a comparative analysis of attack detection strategies. Journal of ambient intelligence & humanized computing/Journal of ambient intelligence and humanized computing, pp.1–18. doi:https://doi.org/10.1007/s12652-024-04794-y.
27) Safitra, M.F., Lubis, M. and Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. Sustainability, [online] 15(18), p.13369. doi:https://doi.org/10.3390/su151813369.
28) Shackelford, S. (2024). Wargames. Routledge eBooks, pp.127–152. doi:https://doi.org/10.4324/9781003344124-8.
29) Shalev, N., Keidar, I., Weinsberg, Y., Moatti, Y. and Ben-Yehuda, E. (2017). WatchIT: Who Watches Your IT Guy? Proceedings of the 26th Symposium on Operating Systems Principles, pp.515–530. doi:https://doi.org/10.1145/3132747.3132752.
30) Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A. and Hutchison, D. (2022). A Cyber Incident Response and Recovery Framework to Support Operators of ICS and Critical National Infrastructure. International Journal of Critical Infrastructure Protection, 37, p.100505. doi:https://doi.org/10.1016/j.ijcip.2021.100505.
31) Tien, C., Huang, T., Tien, C., Huang, T. and Kuo, S. (2019). KubAnomaly: Anomaly detection for the Docker orchestration platform with neural network approaches. Engineering Reports, 1(5). doi:https://doi.org/10.1002/eng2.12080.
32) Valbø, T. (2023). Cloud adoption and cyber security in public organizations: an empirical investigation on Norwegian municipalities. Unit.no. [online] doi:no.uia:inspera:143804570:99658401.
33) Wang, Z.Q. and El Saddik, A. (2023). DTITD: An Intelligent Insider Threat Detection Framework Based on Digital Twin and Self-Attention Based Deep Learning Models. IEEE access, 11, pp.114013–114030. doi:https://doi.org/10.1109/access.2023.3324371.
34) Xiao, H., Zhu, Y., Zhang, B., Lu, Z., Du, D. and Liu, Y. (2024). Unveiling shadows: A comprehensive framework for insider threat detection based on statistical and sequential analysis. Computers & Security, 138, pp.103665–103665. doi:https://doi.org/10.1016/j.cose.2023.103665.
35) Xu, F., Hsu, C., Wang, T. and Paul Benjamin Lowry (2023). The antecedents of employees' proactive information security behaviour: The perspective of proactive motivation. Information Systems Journal, 34(4), pp.1144–1174. doi:https://doi.org/10.1111/isj.12488.
36) Zacharis, A. and Patsakis, C. (2023). AiCEF: an AI-assisted cyber exercise content generation framework using named entity recognition. International Journal of Information Security, 22(5), pp.1333–1354. doi:https://doi.org/10.1007/s10207-023-00693-z