EPiC Series in Computing

Volume 85, 2022, Pages 231–242

Proceedings of 43rd Conference of the South African Institute of Computer Scientists and Information Technologists


# Barriers to dynamic cybersecurity capabilities in healthcare software services

Lawrence Nyakasoka[1], and Rennie Naidoo[2]
[1]University of Pretoria, Lynnwood Rd, Hatfield, Pretoria, 0002, South Africa
[2]University of Pretoria, Lynnwood Rd, Hatfield, Pretoria, 0002, South Africa
lnyakasoka@gmail.com, rennie.naidoo@up.ac.za

**Abstract**

Healthcare firms need to respond faster to the rapidly changing threat landscape. Risks to patient privacy and safety are increasing due to recent cyber-attacks. Healthcare firms are lagging in building cybersecurity capabilities prescribed by best practice approaches. The purpose of this case study is to identify the barriers to building a dynamic cybersecurity capability within a South African healthcare software services firm. The firm is a major provider of cloud-based software as a service (SaaS) solutions to medical practitioners and hospitals. The study used interviews and document analysis as primary data collection methods. Thematic analysis guided by a dynamic capability perspective was used to identify the internal and external barriers that could impede building a dynamic cybersecurity capability at a healthcare software services firm. The research recommends interventions to address cybersecurity barriers in healthcare software services firms.

## 1 Introduction

Cybersecurity risk is among the most complex problems the healthcare sector faces (Appari & Johnson, 2010; Martin et al., 2017; Muthuppalaniappan & Stevenson, 2021). Information technology solutions such as electronic health records (EHRs) have transformed patient care. EHRs have made it easier for healthcare practitioners to store, process and transmit medical records (Appari & Johnson, 2010). The use of information technology and interconnectivity in healthcare, on the other hand, has introduced cybersecurity risks. Privacy breaches were still a primary concern before the adoption of EHRs. Before EHRs, medical records were only accessible through physical access to filing cabinets. EHRs and interconnectivity provide multiple access gateways to medical records from across the globe. The confidentiality, integrity and availability (CIA) of EHRs is no longer guaranteed (Kruse et al., 2017; Ross et al., 2016).

Cyber attackers target the healthcare sector for two main reasons: it is a source of valuable personal data, and its cyber security defences are generally weak (Coventry & Branley, 2018). Cyberattacks in

healthcare can reduce patient trust, cripple health systems and potentially threaten human life (Martin et al., 2017). Cyber security challenges are exacerbated by attackers using artificial intelligence (AI) powered tools to perpetrate attacks while healthcare organisations reactively respond with manual, slow and uncoordinated tools (Sparrell, 2019).

This research aims to identify the key barriers impeding the development of cybersecurity capabilities at a healthcare software service firm. To achieve these aims, the study draws on a dynamic capabilities perspective to better understand the barriers impeding the development of a cybersecurity capability at a healthcare software services firm in South Africa. The key contribution of this paper is to improve the understanding of the challenges of cybersecurity in healthcare services using a dynamic capability model as a theoretical framework (Li & Chan, 2019). Additionally, this paper addresses two weaknesses in extant literature: Firstly, cybersecurity in the context of healthcare services in South Africa has been under-researched (Cilliersa & Wrightb, 2018; Ngoepe & Marutha, 2021). Secondly, few studies to date have applied an IT-enabled dynamic capabilities framework within cyber security research in healthcare services.

This study has practical applications as it assists practitioners in identifying the impediments to addressing cyber security challenges, thereby providing an essential step in resolving cyber security challenges in the healthcare sector. The study also proposes solutions to improve cybersecurity in the healthcare sector.

This narrative aims to explore the following questions:

1. What are the key barriers to building dynamic cybersecurity capabilities at a healthcare firm in South Africa?
2. How can the healthcare firm improve its dynamic cybersecurity capabilities by overcoming these cybersecurity barriers?

This paper builds on prior literature that explores the internal and external cybersecurity barriers in healthcare by focusing on the healthcare software services context. The internal barriers to dynamic capabilities in healthcare software services include inadequate management support, isolation between information security and other functions, inability to attract or retain skilled cybersecurity staff and complex legacy systems. The external barriers include ongoing legal and regulatory changes, evolving threat landscape and the COVID-19 pandemic.

The rest of the article is organised as follows: Next, we provide a brief review of healthcare cybersecurity challenges in South Africa. Then, we outline the dynamic capabilities perspective, which we use as a conceptual framing for our healthcare software services case study. Following this, we present our method and our results and discuss the contributions, implications and limitations of our research.

# 2 Cybersecurity Challenges in South Africa

South African healthcare institutions are increasingly becoming targets of coordinated cyberattacks such as ransomware, theft of personal health information, denial of service attacks and malware (Burke et al., 2021; O'Brien et al., 2021). According to Chuma & Ngoepe (2021), the healthcare sector in South Africa is targeted for two primary reasons: lack of a sound regulatory framework governing personal health information and inherently poor cybersecurity posture. To date, little is known about the dynamic cybersecurity capabilities that is required to overcome these challenges.

# 3 Dynamic Capabilities

According to Teece et al. (1997), dynamic capabilities refer to a firm's "*ability to integrate, build and reconfigure internal and external competencies to address rapidly changing environments*." IS scholars have used the dynamic capability perspective to help explain how dynamic IT-enabled capabilities can help firms respond to fast-changing environments (Li & Chan, 2019; Daniel and Wilson, 2003). Building dynamic IT-enabled capabilities in response to a fast-changing cybersecurity threat landscape also calls for reconfiguring the firm's tangible and intangible assets. This often means altering the firm's organisational structures, processes and competencies to adapt to a changing environment (Li & Chan, 2019). Dynamic capabilities may be used to reconfigure resources or combine existing resources innovatively, resulting in new significant capabilities (Kogut & Zander, 1992; Zahra et al., 2006). Dynamic information security capabilities enable a firm to take action based on cybersecurity insights. Cybersecurity analytics capabilities help management make informed decisions based on existing threats and vulnerabilities (Naseer et al., 2016). Dynamic cybersecurity analytics capabilities result in effective organisational structure, productivity and alignment between business and IT (Melville et al., 2004; Nevo & Wade, 2010; Wade & Hulland, 2004).

This study assumes that an IT-enabled dynamic capabilities perspective can be used to explore how firms attempt to overcome external and internal barriers that impede the development of a dynamic cybersecurity capability. We posit that dynamic capabilities help a firm identify, prevent, detect, respond and recover from cyber-attacks.

# 4 Methodology

## 4.1 The Case Description

We adopted an interpretive case study approach because it is suitable for investigating complex social contexts (Yin, 2018; Baskarada, 2014; Walsham, 1995). Our case study explores the cybersecurity practices at a healthcare software service provider (Meditech). The study examines the barriers to dynamic cybersecurity capabilities at Meditech and proffers solutions to overcome the barriers. Meditech was founded in 1999 and has its head office in Johannesburg, South Africa. The operations of Meditech are limited to the South African market, and it has a presence in all the provinces of South Africa. The primary purpose of Meditech is to transform healthcare and lives by accelerating healthcare information processing and interchange.

Meditech provides cloud-based software as a service (SaaS) solutions to medical practitioners and hospitals. The solutions include billing, clinical services and bureau services. Meditech provides medical billing solutions that assist in billing and collecting directly from medical funders. Meditech also provides healthcare practitioners with health management systems (HMS) and outsourced administration functions. Meditech plays a critical role in the healthcare value chain.

Meditech is a custodian of healthcare information for all the medical practices and the hospitals which use its services. Meditech stores, processes, and transmits medical information to its clients. The information under the custody of Meditech includes personally identifiable information (PII), patient diagnosis, clinical notes, medical aid details and financial information. Given the nature of the information kept by Meditech, it can be classified as a lucrative target for valuable personal information. Meditech needs to adopt sound information security practice that ensures the CIA of the information under its custody.

## 4.2 Data Collection

The researchers used purposive sampling to choose research subjects. Data was collected using primary and secondary sources. The primary data sources included twenty-five interviews. All the interviews were conducted online using google meets due to covid concerns. All the interviews were digitally recorded and transcribed. The interviews ranged from 34 minutes to 67 minutes, averaging 47 minutes. Research subjects who had at least two years within the organisation were preferred. External cybersecurity consultants with direct contact with the organisation and technical teams for some integration partners were interviewed. Research subjects included an Executive, Development Leads, Information Security Consultants, Product Specialists, a former Information Security Specialist, IT professionals and finance. An interview guide was used to gather information from the informants. To supplement interviews, secondary data was collected from information security policies, strategy documents, business strategy, roadmaps, budgets, product documentation, minutes of meetings and the company website. We employed participant triangulation by obtaining the views of different members of organisation.

| **Department** | **Role in Organization** | **Number of Participants** |
|---|---|---|
| Cybersecurity Specialists | Included external cybersecurity consultants who provide cybersecurity services to Meditech and internal cybersecurity staff. | 5 |
| Product Support | Included product owners for Meditech's products and product support staff and call centre. staff | 6 |
| IT Operations | Included IT service desk, user support and infrastructure support | 4 |
| Other Shared Services | Included finance, human resources and administrative staff | 3 |
| Software Developers | Included software development managers, soft development leads and software engineers | 5 |
| Integration Partners | Included IT, staff, from organisations which exchange electronic healthcare information with Meditech | 2 |

**Table 1:** Participants by Department

## 4.3 Data Analysis

We employed the Green et al (2007) four-step guideline for conducting thematic analysis. The study employed a hybrid approach to deductive and inductive coding and theme development (Fereday & Muir-Cochrane, 2006). A code template containing codes from literature was used as an initial step (King, 2012). Barriers obtained from literature included funding, skills shortage, lack of management support and human factors.

The next step involved verifying the applicability of the initial codes by coding documents and applying the deductive codes from the code template. The researcher worked through the interview transcripts line by line. Inductive codes emerged where meaning could not be accurately derived from the deductive codes. New insights emerged, constituting new codes or extensions of the existing codes.

The next step involved condensing the codes into categories. The relationship between codes was examined to establish linkages and coherence. The final step involved the identification of themes. ATLAS.ti and Microsoft Excel were used to code, categories and store the themes.

# 5 Results

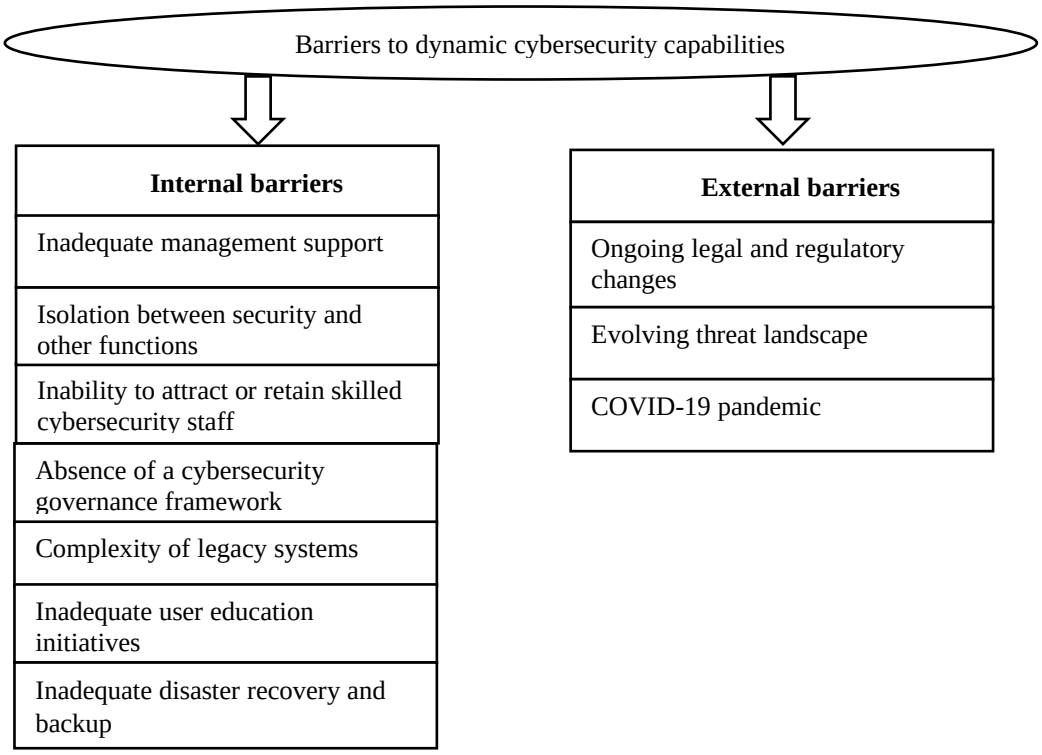


**Figure 1:** Barriers to dynamic cybersecurity capabilities

## 5.1 Inadequate Management Support

Participants agreed that executive management is aware of the consequences of cybersecurity breaches. However, the general sentiment is that executive management can improve cybersecurity posture. Executive leadership provides sponsorship and budgetary support to cybersecurity projects. The budgetary support is corroborated by the 8% budgetary allocation to cybersecurity in 2021, which is higher than the healthcare average of 0-3% (Abraham et al., 2019). A senior IT manager concurred that there was top management cybersecurity buy-in, especially after the introduction of the Protection of Personal Information Act (POPI), when he stated: "*The only strength that I can actually allude to is that when POPI was introduced or when there was talk of POPI, there was a fast reaction to the legislation meaning that there was executive buy-in, the culture for the whole company not really but the executives understood and still understand the implications of privacy and the requirements for security on the network."*

Executive management can ensure that cybersecurity can be a focus area and an agenda item for the board. Participant 2 felt that the absence of a C-Level executive responsible solely for cybersecurity makes the board less able to deal with cybersecurity risks. A senior cybersecurity consultant stated that "*When it comes to security, in most cases executives and technical people are not always on the same wavelength. There is a need for someone to bridge this gap between top management and specialists. I*

*think it would be beneficial to have an executive specifically responsible for security, a CISO or maybe if it is not possible to employ a CISO, there should be a security steering committee of some sort."*

## 5.2 Isolation between Security and Other Functions

Meditech employs a shared services model for service departments such as information technology and information security. An executive stated, "*We adopted the shared service model to allow the business units to focus on their core offerings and reduce non-core services duplication*." The evidence gathered from the interviews suggest that the teams focus on their core responsibilities, and there is little or no input from information security to support their product evolution. The cybersecurity function is not involved in product design and evolution. When asked how information security is embedded in software development, A software development lead said, "*Ok, as developers in my department, we mainly focus on ensuring that we get the functionality right. I think more can be done when it comes to security. Maybe we can have someone who is specifically assigned to security issues when it comes to development.*" Not embedding information security in the operations may result in security-related aspects being overlooked in the product design.

## 5.3 Inability to Attract or Retain Skilled Cybersecurity Staff

From the interviews, it was gathered that cybersecurity personnel prefer to work in sectors such as banking, telecommunications and financial service. Two former Meditech employees confirmed that they left Meditech for the telecommunication and financial services sectors. The participants cited a bigger budget for cybersecurity in the financial services and telecommunications sector. They also highlighted that there is also more exposure and more opportunities for growth in the industries such as financial services and telecommunications compared to the healthcare sector. A former information security specialist said that "*I left after three years mainly because I was looking for growth both financially and career-wise. Remember security is based on what you are trying to protect, so the telecommunications are bigger than Meditech (alias), so they obviously have a bigger budget to spend on security. I also realised that I had reached the ceiling in terms of growth as a security specialist. I was occupying the highest position available.*"

There is a global shortage of skilled cybersecurity professionals, and the estimated global shortfall of cybersecurity skills is 6 million (Burrell, 2020; Crumpler & Lewis, 2019). The global shortage of cybersecurity skills and relatively lower remuneration make it difficult for the healthcare sector to attract and retain skilled cybersecurity professionals (Burrell, 2020).

## 5.4 Absence of Cybersecurity Framework

Cybersecurity frameworks (CSF) helps policymakers to define cybersecurity strategy using a policy template. CSFs allow management to cascade the cybersecurity strategy in clear and non-ambiguous statements (Azmi et al., 2018). CSF provide a basis upon which the implementation of cybersecurity strategy can be tracked and measured (Campos et al., 2016).

A review of all the cybersecurity documentation available does not mention any specific CSF that Meditech uses. Senior managers who were interviewed also admitted that there was no currently used framework or considered for adoption in the short term. When asked about CSFs, an IT executive said, "*We follow the best practices in everything that we do and that includes cybersecurity. Our systems and processes are mature, and we are using top-end technology. Before we disposed Subsidiary-Z (alias) we had PCI audits at least once a year, so our systems and processes are tried and tested.*"

The cyber security practitioners we interviewed concurred that Meditech must consider adopting cybersecurity frameworks. A cybersecurity consultant said, "So in essence, for Meitech(alias), I think

we can look at HIPPA not to adopt it but to pick up the finer aspects of it, so you are storing health care data. We might also want to look at South African Legislation to see whether there aren't any standards, but you find out that many countries do business with America, which is why they adopt certain components that are the same as GDPR. African countries do business with European countries, so we are taking components out of GDPR to make sure that we maintain business, so it's prudent for Meditech(alias) to look at what HIPPA says and try to extract what is really necessary for them."

Participants agreed that it is necessary to use CSF to guide the organisation and track the implementation of cybersecurity strategy. The point is not to certify against a specific framework but use it internally as a form of guidance as a starting point.

## 5.5 Complexity of Legacy Systems

Legacy systems were also identified as a barrier to addressing cybersecurity challenges in the healthcare sector (Langer et al., 2016). An information technology executive stated that "*I am sure you will also find some areas which we are not doing right; for instance, we have some legacy applications that are not using the latest operating systems. It's not only up to the tech team to do it, it's also actually a business problem. So we have to look at it from that perspective*." Some key clients still use the legacy applications and cannot be sunset for genuine business reasons. Legacy applications present a significant security risk. Legacy systems may not support the latest encryption standards and modern security features like multifactor authentication, role-based access and single sign-on (Abraham et al., 2019). Security flaws for legacy applications are documented in blogs and journals to update security professionals, giving hackers access to rich information to perfect their tools (Langer et al., 2016).

The wanna-cry ransomware of 2017, which crippled several hospitals across the globe, resulted from attackers exploiting vulnerabilities in Microsoft Windows 2003, a software for which Microsoft had ceased to provide support at the time (Martin et al., 2018; Mattei, 2017). Product documentation of applications like B and K (pseudo names) revealed that these applications use insecure protocols like File Transmission Protocol (FTP), Lightweight Directory Access Protocol (LDAP) and Simple Message Transmission Protocol (SMTP). Insecure protocols like LDAP, FTP and SMTP send data in plain text and in the event of an eavesdropping attack, the attacker will be able to read through the data (Corey et al., 2002).

## 5.6 Inadequate user education initiatives

Most employees interviewed were aware of the basic cyber hygiene and the possible impact of cybersecurity attacks on the organisation. Most employees were mindful of risky behaviours and acceptable behaviour. Employees were generally familiar with cybersecurity terms such as malware, virus, trojan and ransomware. However, there was a general belief among employees that cybersecurity is a technical issue and is the responsibility of the information technology team. Employees confirmed no formal information security awareness training program in place. Staff members also professed ignorance about the contents of the information security policies. A software development lead mentioned, "*I lead a team of developers, and I am quite sure that they will be able to recognise information security threats. I don't remember attending any scheduled information security awareness training, but I think it would be helpful to have such training just to refresh knowledge as well as to help us keep such issues at the top of our minds.*"

The human resource team was unaware of the information security awareness training programs. The human resource team confirmed that as part of the onboarding of new employees, they sign to acknowledge that they have read, understood and agree to be bound by information security policies. A human resource participant said, "*We try by all means to ensure that all new starts go through all the policies during the onboarding process. Besides, we do not put pressure on employees to sign and return the policy, and we give them seven days to go through all the policies. I believe that is enough time to*

*read through.*" The employees who read information security policy have been found to have better information security culture compared to those who do not read (Da Veiga, 2016). Therefore, it is important to ensure that employees read and understand the contents of information security policies.

## 5.7 Inadequate disaster recovery and backup plans

Backup and disaster recovery plans are controls of last resort. Controls of last resort give an organisation a lifeline if all the other controls have failed (Budiman et al., 2020). Controls of last resort are significant because they result in cyber resilience. In the event of successful cyber-attacks that compromise the availability or integrity of critical data, backup, disaster recovery, and business continuity plans offer an additional layer of protection (Tchernykh et al., 2019).

Meditech has backup and disaster recovery plans in place, however from a review of documentation, there was no evidence of regular testing of the backup and disaster recovery plans. Most interviewed participants were not confident that the business would continue to operate normally in the event of a significant cyber security breach or a natural disaster.

## 5.8 Ongoing legal and regulatory changes

Most participants agreed that the Protection of Personal Information Act (POPI) was a wake-up call for executives and senior management. One senior manager said, "*I think we will be doing POPI assessments. In South Africa, I think we are one of the early adopters of POPI and really making sure that we are compliant. I think we take it quite seriously*." The enactment of POPI came with a threat of regulatory fines and personal liability for directors and senior management. The fear of regulatory penalties and being in the newspaper headlines for the wrong reasons has seriously induced boards to focus on cybersecurity.

While the POPI is a step in the right direction, some cybersecurity experts felt that the enforcement of POPI may be complicated. Most cybersecurity experts do not believe that the regulator has the capacity to ensure compliance with the POPI act. A cybersecurity consultant said, "*I honestly believe POPI act is a good starting point, but I am not quite sure how the Government will be able to monitor compliance. It is still too early to tell what the impact of POPI will be to Meditech and the industry in general.*"

Cybersecurity experts also felt that the absence of healthcare-specific cybersecurity legislation makes it harder to standardise cybersecurity standards. In the United States of America, the healthcare industry is regulated by Health Insurance Portability and Accountability Act (HIPAA). HIPAA enactment cemented standardised frameworks that control, reduce, and track cybersecurity in healthcare (Patil & Chakrabarti, 2021).

## 5.9 Evolving threat landscape

Cybersecurity threats change rapidly (Armin et al., 2015). Modern attackers utilize automated tools to discover vulnerabilities in real-time. The emergence of cryptocurrencies makes it easy to transfer money peer to peer without paperwork and financial institutions. Cryptocurrencies also make it easier for attackers to receive their ransom payment anonymously, and prosecuting authorities cannot trace. An information security specialist mentioned that "*I think ransomware is going to be a big thing in the next few years. I am told that some organisations are now selling ransomware as a service. In essence, we are talking about readymade exploits being sold on the market, just like apples and bananas. The other challenge is that insurance companies are paying ransoms for clients who take up cyber insurance*."

When asked whether Meditech is likely to pay a ransom, one senior manager mentioned that "I *always want to think like America. We don't negotiate with terrorists. The reality is if you look at the*

*big companies that have been hit by ransomware in the last six months, they have all paid. For instance, in the Netherlands where I am from, the university that got hit by ransomware, they also had to pay. Now, the reality is that paying is the easy way out. And because you are running a business, you have to leverage on your clients.*"

## 5.10 COVID-19 pandemic

The COVID-19 pandemic disrupted the healthcare sector globally. Drastic changes had to be made on the business models in a short space of time. The changes included scaling up remote working capabilities. The Healthcare sector suffered the first-hand effects of the pandemic. Healthcare institutions were victims of high-profile cyber-attacks. A desktop support engineer at Meditech mentioned that "*We struggled to setup users to work from, imagine some of the users were using desktops. Laptop, printers and wifi routers were out of stock for three months or so. To be honest we had to cut corners at times. For some users, laptops were delivered directly to their homes without antivirus software, windows updates and security checks. We were aware of the risks but we were just caught off guard."*

# 6 Discussion

To improve the involvement of senior management in cybersecurity, we are proposing that an IT security steering committee be established. IT security steering committee provides a platform where individuals and departments can discuss cybersecurity (Parekh, 2009). Some of the interviewed cybersecurity professionals supported a need for an executive-level cybersecurity role, such as a Chief Information Security Officer (CISO). While it is a noble idea to have an executive-level information security position, a steering committee will be a good starting point because there are no budget implications. We also analysed the company's strategic focus areas for the next five years. Cybersecurity is not a focus area; therefore, it will be difficult to obtain buy-in for a CISO. An IT security steering committee will also address challenges relating to isolation between cybersecurity and other functions as it will consist of representatives of every team.

Cyber insurance has gained prominence in the last decade due to some high-profile and costly cybersecurity attacks (Woods & Simpson, 2017). Cybersecurity insurance can improve an organisation's security posture because insurance companies often insert a moral hazard clause in the policy document. The moral hazard clause stipulates that insurance claims will be repudiated if the policyholder engages in risky behaviour or becomes negligent (Camillo, 2017). Good cyber security practices are rewarded with lower insurance premiums, and risky practices attract sanctions in higher premiums (Pal et al., 2014).

A cybersecurity governance framework provides an organisation with an all-encompassing, holistic plan for information security (Veiga & Eloff, 2007). It combines technical, procedural, and people-oriented components to reduce cybersecurity risk to an acceptable level (Ohki et al., 2009). Management and executives can use a cybersecurity governance framework to plan, track, and control the cybersecurity function (Schlienger & Teufel, 2003). Without a cybersecurity framework, it is difficult to assess the performance of the cybersecurity function. All interviewed cybersecurity professionals concurred that a cybersecurity governance framework is a necessary tool for managing the cybersecurity function. We propose that Meditech should adopt a cybersecurity governance framework. Frameworks to choose from include ISO 27001, which offers an opportunity for Meditech to be certified and accredited.

Numerous studies have shown that information security awareness training and education reduce users 'susceptibility to phishing attempts (Alsharnouby et al., 2015; Kumaraguru et al., 2008; Mayhorn & Nyeste, 2012). Most cybersecurity breaches are a result of unintentional mistakes by users.

Information security awareness training is necessary to reinforce cyber hygiene principles. The interviewed cybersecurity practitioners emphasised the importance of information security awareness training. One participant also recommended regular penetration tests targeted at users to measure the effectiveness of information security awareness and identify training needs.

# 7 Conclusions

This case study explored the barriers to dynamic cybersecurity capabilities in a cloud Saas healthcare firm. Information was gathered through semi-structured interviews and document analysis. Thematic analysis was used to analyse data collected from the interviews. The study identified internal barriers to dynamic capabilities: inadequate executive management support, isolation between cybersecurity and software development, inability to attract or retain skilled cybersecurity staff, absence of a cybersecurity framework, existence of legacy systems, inadequate user education and inadequate disaster recovery and backup plans. The study also identified external barriers to dynamic cybersecurity capabilities: inadequate enforcement of laws and regulations, rapidly evolving threat landscape and the negative impact of the covid-19 pandemic. We proposed possible solutions to address the barriers: formulation of an IT security steering committee, cyber insurance, implementation of a cybersecurity framework, regular user awareness training and regular testing of disaster recovery plans. Our solutions are drawn from literature and input from practitioners. The solutions we proposed are neither prescriptive nor exhaustive. Future research could test the effectiveness of our proposed barrier-based interventions in other healthcare settings. We hope that future research devotes more attention to the development of dynamic cybersecurity capabilities in healthcare settings.

# References

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. *Business Horizons*, *62*(4), 539–548.

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*, 69–82.

Appari, A., & Johnson, M. E. (2010). *Information security and privacy in healthcare : current state of research*. *6*(4),279-314.

Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. *Journal of Cyber Policy*, *3*(2), 258–283.

Baskarada. (2014). Qualitative Research : Case Study Guidelines. *The Qualitative Report*, *19*(40), 1–25.

Bhardwaj, J., Gautam, S., Yadav, H., Tyagi, N., & Abidin, S. (2021). Taxonomy of Cyber Security in Medical Science. *Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2020, Volume 3*, 371–380.

Branley-Bell, D., Coventry, L., & Sillence, E. (2021). Promoting Cybersecurity Culture Change in Healthcare. *The 14th PErvasive Technologies Related to Assistive Environments Conference*,14, 544–549.

Budiman, K., Arini, F. Y., & Sugiharti, E. (2020). Disaster recovery planning with distributed replicated block device in synchronized API systems. *Journal of Physics: Conference Series*, *1567*(3), 32-45

Burrell, D. N. (2020). An exploration of the cybersecurity workforce shortage. In *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 1072–1081)

Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, *2*(1), 53–63.

Campos, J., Sharma, P., Jantunen, E., Baglee, D., & Fumagalli, L. (2016). The challenges of cybersecurity frameworks to protect data required for the development of advanced maintenance. *Procedia Cirp*, *47*, 222–227.

Chuma, K. G., & Ngoepe, M. (2021). Security of electronic personal health information in a public hospital in South Africa. *Information Security Journal: A Global Perspective*, 31(2),1–17.

Corey, V., Peterman, C., Shearin, S., Greenberg, M. S., & Van Bokkelen, J. (2002). Network forensics analysis. *IEEE Internet Computing*, *6*(6), 60–66.

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48–52.

Crumpler, W., & Lewis, J. A. (2019). *The cybersecurity workforce gap*. Center for Strategic and International Studies (CSIS) Washington, DC, USA.

Daniel, E. M., & Wilson, H. N. (2003). The role of dynamic capabilities in e-business transformation. European Journal of Information Systems, 12(4), 282-296.

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information & Computer Security,24(2),*139-151.

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, *5*(1), 80–92.

Gable, G. G. (1994). Integrating case study and survey research methods: an example in information systems. *European Journal of Information Systems*, *3*(2), 112–126.

Green, J., Willis, K., Hughes, E., Small, R., Welch, N., Gibbs, L., & Daly, J. (2007). Generating best evidence from qualitative research: The role of data analysis. *Australian and New Zealand Journal of Public Health*, *31*(6), 545–550

Karakoç, M., Aristigueta, M., & Director, D. P. A. (2017). Understanding the barriers to addressing cybersecurity challenges in american state and local governments.

King, N. (2012). Doing template analysis. *Qualitative Organizational Research: Core Methods and Current Challenges*, *426*, 77–101.

Kogut, B., & Zander, U. (1992). Knowledge of the firm, combinative capabilities, and the replication of technology. *Organization Science*, *3*(3), 383–397.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2008). Lessons from a real world evaluation of anti-phishing training. *2008 ECrime Researchers Summit*,14, 1–12.

Langer, L., Skopik, F., Smith, P., & Kammerstetter, M. (2016). From old to new: Assessing cybersecurity risks for an evolving smart grid. *Computers & Security*, *62*, 165–176.

Lee, A. S., & Baskerville, R. L. (2003). Generalizing generalizability in information systems research. *Information Systems Research*, *14*(3), 221–243.

Li, T. C., & Chan, Y. E. (2019). Dynamic information technology capability: Concept definition and framework development. The Journal of Strategic Information Systems, 28(4), 101-575.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *BMJ (Online)*, *358*, 4–7. https://doi.org/10.1136/bmj.j3179

Mattei, T. A. (2017). Privacy, confidentiality, and security of health care information: lessons from the recent wannacry cyberattack. *World Neurosurgery*, *104*, 972–974.

Mayhorn, C. B., & Nyeste, P. G. (2012). Training users to counteract phishing. *Work*, *41*(Supplement 1), 3549–3552.

Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Information technology and organizational performance: An integrative model of IT business value. *MIS Quarterly*, 283–322.

Muthuppalaniappan LLB, M., & Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care*, *33*(1).

Naseer, H., Shanks, G., Ahmad, A., & Maynard, S. (2016). Enhancing information security risk management with security analytics: A dynamic capabilities perspective. *Proceedings of the 27th Australasian Conference on Information Systems, ACIS 2016*, 1–12

Nevo, S., & Wade, M. R. (2010). The formation and value of IT-enabled resources: antecedents and consequences of synergistic relationships. *MIS Quarterly*,34(1), 163–183

Ngoepe, M., & Marutha, N. (2021). A Framework to Integrate Healthcare Records in the South African Public Hospitals Using Blockchain Technology, *African Journal of Library, Archives and Information Science*,31(1),29-38

O'Brien, N., Ghafur, S., & Durkin, M. (2021). Cybersecurity in health is an urgent patient safety concern: We can learn from existing patient safety improvement strategies to address it. *Journal of Patient Safety and Risk Management*, *26*(1), 5–10

Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T., & Kagaya, T. (2009). Information security governance framework. *Proceedings of the First ACM Workshop on Information Security Governance*, 41,1–6.

Pal, R., Golubchik, L., Psounis, K., & Hui, P. (2014). Will cyber-insurance improve network security? A market analysis. *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, 28,235–243.

Parekh, B. (2009). Information Security Steering Committee. *2009 Information Security Curriculum Development Conference*, 148–150.

Patil, A. P., & Chakrabarti, N. (2021). A review into the evolution of HIPAA in response to evolving technological environments. *Journal of Cybersecurity and Information Management*, *4*(2), 5–15.

Ross, R. S., Feldman, L., & Witte, G. A. (2016). Rethinking Security through Systems Security Engineering, *National Institute of Standards and Technology,, 6(4), 101-119.*

Schlienger, T., & Teufel, S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture. *14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings,14*, 405–409.

Sparrell, D. (2019). Cyber-Safety in Healthcare IOT. *2019 ITU Kaleidoscope: ICT for Health: Networks, Standards and Innovation (ITU K)*,27,1–8.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Management Journal, 18(7), 509-533.

Veiga, A. Da, & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management*, *24*(4), 361–372.

Wade, M., & Hulland, J. (2004). The resource-based view and information systems research: Review, extension, and suggestions for future research. *MIS Quarterly*, 107–142.

Walsham, G. (1995). Interpretive case studies in IS research: nature and method. *European Journal of Information Systems*, *4*(2), 74–81.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, *88*, 101-140.

Woods, D., & Simpson, A. (2017). Policy measures and cyber insurance: A framework. *Journal of Cyber Policy*, *2*(2), 209–226.

Yin, R. K. (2018). *Case study research and applications*. Sage Publications. California, USA.

Zahra, S. A., Sapienza, H. J., & Davidsson, P. (2006). Entrepreneurship and dynamic capabilities: A review, model and research agenda. *Journal of Management Studies*, *43*(4), 917–955.