SACJ 36(1) July 2024
Research Article

Understanding the inertial forces impeding dynamic cybersecurity learning capabilities: The case of a South African healthcare software services firm

Lawrence Nyakasoka[a], Rennie Naidoo[a, b]

[a] Department of Informatics, University of Pretoria, Pretoria, South Africa
[b] Department of Information Systems, University of the Witwatersrand, South Africa

ABSTRACT
Healthcare firms need to develop cybersecurity learning mechanisms to respond faster and more proactively to a rapidly changing cybersecurity threat landscape. Many healthcare firms lack the necessary cybersecurity learning capabilities to address ever-changing and unpredictable cyberthreats effectively. In this case study, we investigate the challenges faced by a major South African healthcare software services firm that offers software as a service (SaaS) solutions. We analyse the inertial forces that impede the firm's cybersecurity learning capabilities by integrating concepts from dynamic cybersecurity learning capability (DCLC) and IS-enabled organisational learning perspectives. Furthermore, we identify strategic and operational level inertial forces through interviews with the organisation's experts and examination of cybersecurity documents. We then present actionable recommendations for industry practitioners to overcome these inertial forces and strengthen their cybersecurity learning capabilities. Our suggested interventions include implementing proactive leadership structures, enhancing user learning capabilities, and adopting novel risk management approaches. Additionally, we propose further directions for scholars to research the impact of inertial forces on dynamic cybersecurity learning capabilities in healthcare firms.

Keywords case study, cybersecurity, dynamic capabilities, organisational learning, organisational inertia, healthcare, software as a service

Categories • **CCS ~ Security and Privacy, Human and societal aspects of security and data privacy, Privacy**

Email
Lawrence Nyakasoka – lnyakasoka@gmail.com (CORRESPONDING)
Rennie Naidoo – rennie.naidoo@wits.ac.za

Article history
Received: 31 January 2023
Accepted: 17 October 2023
Online: 31 July 2024

1 INTRODUCTION

Cybercriminals are working with increased sophistication, constantly learning new ways to target and evade detection by healthcare organisations (Martin et al., 2017). The repercussions

Nyakasoka, L. and Naidoo, R. (2024). Understanding the inertial forces impeding dynamic cybersecurity learning capabilities: The case of a South African healthcare software services firm. *South African Computer Journal* 36(1), 105–132. https://doi.org/10.18489/sacj.v36i1.18877

SACJ is a publication of *SAICSIT*. ISSN 1015-7999 (print) ISSN 2313-7835 (online)

of cyberattacks on healthcare institutions are gaining prominence within the cybersecurity domain (Renaud & Ophoff, 2019). The escalating awareness of these consequences underscores the urgency for healthcare organisations to adopt proactive measures to safeguard against cybersecurity threats (Renaud & Ophoff, 2019). However, the inherent challenges of improving existing systems due to inertial forces are hindering the ability of healthcare organisations to respond effectively to cybersecurity threats (Frumento, 2019).

Healthcare organisations must proactively adapt and reinforce their cybersecurity capabilities to safeguard against cybercriminals who continuously develop sophisticated cyberattack techniques (Appari & Johnson, 2010). Cybercriminals take advantage of the interconnected nature of modern healthcare organisations to launch lateral movements to gain access to other vulnerable systems (Graham, 2021). Moreover, cyberattackers often operate from systems not directly under their control, making detection and prosecution arduous (Papastergiou et al., 2021). It is, therefore, imperative for healthcare organisations to adapt cybersecurity capabilities to counter advanced cybercriminals.

As the healthcare sector adopts wearable devices, telehealth, and Internet of Things (IoT) technologies, these give rise to distinct attack vectors, wherein cyberattacks on life-saving devices could have severe and life-threatening consequences, especially for patients with chronic illnesses (Graham, 2021; Sparrell, 2019). Consequently, cyberattacks within the healthcare sector have escalated into a life-and-death phenomenon, emphasising the importance of adopting proactive cybersecurity measures.

Novel multi-stage attacks, such as Advanced Persistent Threat (APT) attacks, further exacerbate the challenges of combating cyberthreats (Papastergiou et al., 2021). Additionally, the barriers to entry for cybercriminals have significantly lowered, as they now have access to malicious tools and services through the dark web (Papastergiou et al., 2021). In the face of this dynamic cybersecurity threat landscape, static industry standards and frameworks, like the NIST Cybersecurity Framework and ISO 27000 series, struggle to keep pace with evolving threats and rapidly changing technology (Scofield, 2016).

To fortify their cybersecurity defences and effectively counter ever-changing cyberattackers, healthcare organisations should adopt a dynamic approach. We propose integrating concepts from dynamic capabilities theory, organisational learning, and organisational inertia to supplement and inform the development of existing cybersecurity standards and frameworks. Emphasising the need for a dynamic cybersecurity learning framework, we contend that healthcare organisations that embrace these principles will be better prepared to withstand rapidly evolving cyberattacks.

We assert that a deeper understanding of inertia is the first crucial step to addressing the inertial forces that impede the building and implementation of Dynamic Cybersecurity Learning Capabilities (DCLC). By comprehending the forces of inertia that hinder the development of DCLC in a South African healthcare software services firm, the firm can proactively counteract these inertial forces and foster a more responsive cybersecurity culture. Therefore, we propose the following research questions to guide our investigation:

What are the major inertial forces that can impede the building of dynamic cybersecurity

learning capabilities in a South African healthcare software services firm, and how can these inertial forces be effectively counteracted by key cybersecurity learning drivers?

The remainder of this article is structured as follows: We provide an overview of the cybersecurity challenges facing South African healthcare organisations. Subsequently, we outline the theoretical foundations for our healthcare software as a services case study, drawing upon key concepts from organisational learning, organisational inertia, and dynamic capabilities theories. We then present our research methodology and findings, followed by a discussion of our research's contributions, implications, and limitations.

2 CYBERSECURITY CHALLENGES IN SOUTH AFRICA

The African continent is experiencing a significant upsurge in cybersecurity threats. Notably, a 2018 report by Symantec Incorporation highlighted that cybercrime increased faster in Africa than on any other continent (Walker et al., 2021). The economic impact of cybercrime in South Africa alone is estimated to range between R8.5 billion and R10 billion (Adomako et al., 2018; Gopal & Maweni, 2019). In 2020, cybercrimes ranked fourth in the most frequently reported criminal activity and exhibited the most rapid growth rate in South Africa (Walker et al., 2021). The COVID-19 pandemic further exacerbated the situation, with numerous healthcare institutions falling prey to coordinated cyberattacks, including those in South Africa. Table 1 offers a glimpse of some significant cyberattacks that have targeted healthcare organisations since the onset of the COVID-19 pandemic.

Table 1: Cybersecurity breaches in the healthcare sector since the onset of COVID-19

Date of cyberattack	Country/ Institution	Reported details
30 July 2020	South Africa – Life Healthcare	A coordinated cyberattack disrupted IT services. However, the complete extent of the attack was not publicly disclosed (Pieterse, 2021).
17 August 2020	South Africa – Momentum Metropolitan	A third party unlawfully accessed a limited portion of data of a subsidiary of the group (Moyo, 2023).
14 March 2020	World Health Organization (WHO)	A malicious website was created, imitating the WHO internal email system, with the primary intention of stealing employee passwords (Chigada & Madzinga, 2021).
16 March 2020	United Kingdom – Hammersmith Medicines Research Group	Ransomware attacks resulted in the disruption of patient care and a halt in healthcare service provision (Goodwin, 2022).
22 March 2020	United States – Health and Human Services (HHS)	Ransomware attacks resulted in the publication of patients' personal details and a failed attempt to disable the network (Kiser & Maniam, 2021).

https://doi.org/10.18489/sacj.v36i1.18877

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 (Chuma & Ngoepe, 2022; Ngoepe & Marutha, 2021). Hospitals in South Africa are frequently targeted for two primary reasons: the absence of a robust regulatory framework governing personal health information and inherent vulnerabilities stemming from poor cybersecurity posture (Chuma & Ngoepe, 2022).

The ransomware attack in July 2020 at a major hospital in South Africa highlights the critical importance of incorporating cybersecurity learning (Burke et al., 2021). The incident's severe disruption of the hospital's operations for an extended period could have endangered patients' well-being and access to critical medical services. This ransomware attack emphasises the urgency for healthcare organisations to proactively enhance their cybersecurity learning capabilities. Healthcare institutions can better safeguard their essential systems and data by continually adapting and improving their cybersecurity responses, ensuring the uninterrupted delivery of life-saving healthcare services. Mitigating the risks posed by cyberthreats in the ever-evolving digital landscape becomes paramount in protecting patients' safety and well-being, making cybersecurity learning an indispensable aspect of healthcare management and operational resilience.

The enforcement of the Protection of Personal Information Act (POPIA) in South Africa has intensified the imperative for healthcare organisations to enhance their cybersecurity learning capabilities (Olofinbiyi, 2022; Sutherland, 2021; Townsend, 2022). Healthcare organisations face substantial pressure to adhere to data privacy legislation and enhance their cybersecurity learning efforts.

While substantial progress has been achieved in addressing cybersecurity challenges within the healthcare domain, most studies utilise existing cybersecurity frameworks (Akinsanya et al., 2019; Kruse et al., 2017; Thompson, 2017). However, these cybersecurity governance frameworks are inherently static and lack provisions for cybersecurity learning. Consequently, we propose a Dynamic Cybersecurity Learning Capabilities (DCLC) model to improve the agility of cybersecurity initiatives in a healthcare context.

3 THEORETICAL FOUNDATIONS

3.1 Dynamic cybersecurity capabilities

Teece et al. (1997) coined the term "dynamic capabilities" and defined dynamic capabilities as the firm's ability to integrate, build, and reconfigure internal and external competencies to adapt to rapidly changing environments. Eisenhardt and Martin (2000) extended this definition, depicting dynamic capabilities as the organisational processes that utilise resources, particularly those for integration, reconfiguration, acquisition, and release, to match and even create market change. In this vein, dynamic capabilities encompass firms' strategic and organisational routines to achieve new resource configurations as markets emerge, collide, split, evolve, and decline.

https://doi.org/10.18489/sacj.v36i1.18877

An alternative perspective, presented by Helfat et al. (2007), perceives dynamic capabilities as the ability of an organisation to create, extend, or modify its resource base deliberately. Recent research has distilled dynamic capabilities into three fundamental constructs: sensing (identifying opportunities and threats), seizing (orchestrating business design), and transforming (implementing a business model) (Daniel & Wilson, 2003; Zollo & Winter, 2002).

We expand the scope of the dynamic capabilities theory to cybersecurity, introducing the term *dynamic cybersecurity capabilities* (DCC) to describe our focus. Similarly, we adapt the fundamental elements of dynamic capabilities theory and introduce the terms *cybersecurity sensing* (CSn), *cybersecurity seizing* (CSz), and *cybersecurity transformation* (CT) to align with our specific emphasis on cybersecurity.

CSn pertains to continuously monitoring the internal and external healthcare environment, enabling healthcare organisations to identify potential cybersecurity threats and opportunities for enhanced defences. CSz involves adeptly orchestrating cybersecurity initiatives and designing refined defence mechanisms to capitalise on identified opportunities (Daniel & Wilson, 2003; Zollo & Winter, 2002). CT in healthcare refers to the capability to realign and reconfigure cybersecurity routines, processes, structures, and organisational culture (Easterby-Smith, 1997; Teece, 2018).

Healthcare institutions must foster a cybersecurity learning culture, encouraging continuous experimentation, innovation, and skill development to adapt to the dynamic cybersecurity landscape. Investing in employee training and development becomes a strategic imperative to nurture a talented workforce capable of contributing to the development and execution of dynamic capabilities in cybersecurity.

3.2 Cybersecurity learning

Organisational learning is a dynamic process wherein members of the organisation interact and exchange knowledge, leading to the creation of shared knowledge that exceeds the sum of individual knowledge (Curado, 2006). This continual learning process enables people to enhance their capabilities, fostering self-update, flexibility, agility, speed, and innovation within the organisation (Crossan & Berdrow, 2003). Organisational learning emerges as individuals interact, collaborate, and collectively find solutions to challenges (Easterby-Smith, 1997).

Encouraging knowledge sharing, lifelong learning, and fostering a culture of challenging the status quo are key aspects of promoting organisational learning (Curado, 2006; Wang & Ahmed, 2003). Organisations must establish processes that facilitate knowledge exchange among employees at all levels, encouraging them to learn and seek innovative approaches continuously (Visser, 2011). Additionally, learning from failure and incorporating feedback is vital to the improvement and growth of the organisation (Visser, 2011).

To align with our specific focus on cybersecurity, we customise organisational learning and introduce the term “cybersecurity learning” (CL). This term precisely encapsulates our emphasis on the dynamic learning processes related to cybersecurity practices and strategies.

Cybersecurity learning is crucial in the healthcare sector to safeguard patient data, main-

tain trust, comply with regulations, and effectively counter the ever-evolving cyberthreats. It is an essential aspect of modern healthcare management, protecting patients and healthcare organisations from the adverse effects of cyberattacks.

3.3 Cybersecurity inertia

Organisational inertia is an operational phenomenon in which an organisation sticks to its past practices to maintain stability (Ashok et al., 2021). Such inertia can hinder organisational learning, preventing the organisation from adequately responding to a turbulent external environment. If an organisation operates in a volatile environment, maintains the status quo over a long period, and fails to adapt to change promptly, that can be evidence of organisational inertia (Borkovich & Skovira, 2019; Renaud & Ophoff, 2019). Organisational inertia is associated with stable structures and processes that do not change over time (Hur et al., 2019; Yayla & Lei, 2020). Inertia manifests in different ways within organisations, including information suppression, excessive commitment to organisational structure, bureaucracy and rigid rules (Hur et al., 2019). Organisational inertia stifles organisational learning.

We refine the organisational inertia theory to better align with our research and introduce the term *cybersecurity inertia*. Our approach addresses the concept of organisational inertia within the cybersecurity context, providing a more focused lens for our investigation. Cybersecurity inertia results from the stickiness of traditional cybersecurity practices and routines (Borkovich & Skovira, 2019).

Healthcare institutions face significant challenges as they strive to accommodate the ever-evolving and expanding cybersecurity landscape within their organisation and the broader external context (Hur et al., 2019; Renaud & Ophoff, 2019). However, in many instances, healthcare organisations facing a widening threat landscape recognise the need for change but struggle to improve their defensive posture (Hur et al., 2019). Cybersecurity inertia often manifests as a resistance to adaptation, an excessive commitment to rigid structures, and the suppression of information (Ruiz-Mercader et al., 2006).

Next, we present a conceptual framework combining DCC, CL, and CI concepts. Through this synthesis, we theorised a dynamic cybersecurity learning capabilities (DCLC) model, the guiding framework for our case study analysis.

4 CONCEPTUAL FRAMEWORK

Figure 1 shows a direct link between DC and DCC (Besson & Rowe, 2012). Thus, CL helps build the capacity to perceive and accommodate external changes. Conversely, inadequate CL can lead to CI and rigid structures, hindering the development of DCLC (Ferreira et al., 2021).

Scholars have applied dynamic capabilities, organisational learning and inertia to business functional units such as information technology and cybersecurity (Mehra & Dhawan, 2003; Naseer et al., 2018; Ruiz-Mercader et al., 2006). In our study, we adopt dynamic capabilities,

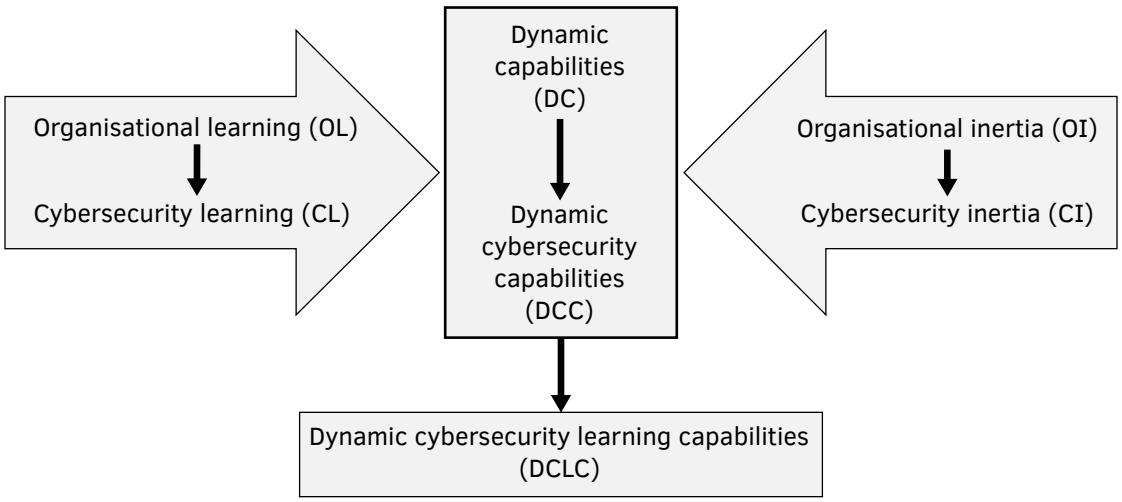

Figure 1: Conceptual framework

organisational learning, and organisational inertia concepts as a guiding framework to theorise a novel DCLC model. We aim to enhance the understanding of how dynamic cybersecurity learning can be incorporated into organisational practices to foster adaptive, responsive and resilient cybersecurity strategies.

5 METHODOLOGY

This section outlines the research methods employed in this study. Firstly, we provide a background of the case study and offer a rationale for selecting the specific case. Subsequently, we detail the data collection process utilised in this research. We present an overview of the data analysis approach employed to derive insights from the collected data. Finally, we outline principles that we followed to comply with research ethics.

5.1 Case description

We adopted an interpretive case study approach because it is suitable for investigating complex social contexts (Baškarada, 2014; Walsham, 1995; Yin, 2018). Our case study explores the cybersecurity practices at HSSP (pseudo-name), a healthcare software services provider. The study examines the inertial forces to dynamic cybersecurity learning capabilities at HSSP and offers solutions to overcome the inertia.

HSSP, a healthcare software service provider based in Johannesburg, South Africa, founded in 1999, offers software as a service solutions to medical practitioners and hospitals. Their platform includes billing, clinical, and bureau services, streamlining medical practices' workflows and improving revenue management. The solutions integrate with medical funders, providing automated benefit checks and real-time electronic claims processing. They also offer electronic

medical record (EMR) and electronic health record (EHR) solutions, storing patient information and enabling electronic scripts, sick notes, and referrals. In response to the COVID-19 pandemic, HSSP developed a vaccine administration solution used by medical aid funders.

HSSP, a custodian of sensitive healthcare information, is potentially an attractive target for cybercriminals seeking valuable personal health information (PHI) (Appari & Johnson, 2010; Soomro et al., 2016). Consequently, HSSP should embrace robust information security practices that can guarantee the confidentiality, integrity, and availability (CIA) of the data entrusted to its care. Moreover, HSSP should exhibit resilience, adaptability, dynamism, agility, and responsiveness in the face of ever-evolving cybersecurity threats that persistently affect the healthcare sector. By fostering these capabilities, HSSP can proactively navigate the dynamic cybersecurity landscape, safeguard critical healthcare information, and preserve the continuity of its services.

HSSP places a significant emphasis on cybersecurity. The policy declaration within a cybersecurity document affirms cybersecurity as a focus area:

> *HSSP is committed to understanding and effectively managing risks related to Information Security to provide greater certainty and confidence for our stakeholders, employees, patients, partners, suppliers and the communities in which we operate. Finding the right balance between information security risk and business benefit enhances our business performance and minimises potential future exposures*
>
> [Information Security Policy, Chief Executive Officer, May 2022, p. 1]

5.2 Data collection

The researchers employed purposive sampling as their sampling method to select research participants deliberately and strategically. The data collection process encompassed both primary and secondary sources. Primary data was gathered through twenty-five interviews. All were conducted online via Google Meet as a precautionary measure in response to COVID-19 concerns. Each interview was digitally recorded and subsequently transcribed. The interview duration varied, ranging from 34 minutes to 67 minutes, with an average duration of 47 minutes.

The sample group of research subjects (Table 2) comprised external cybersecurity consultants who directly interacted with HSSP and technical teams serving specific customers. Diverse roles were represented among the research subjects, including Executives, Development Leads, Information Security Consultants, Product Specialists, Information Security Specialists, IT professionals, and finance professionals. To ensure the systematic collection of relevant information, we utilised an interview guide during the interviews.

Apart from conducting interviews, we also utilised document analysis as part of our data collection. This analysis encompassed various documents, including information security policies, strategy documents, business plans, roadmaps, budget reports, product documentation, meeting minutes, and content from the company's website. Document analysis was

Table 2: Research subjects

Department	Role in organisation	# participants
Cybersecurity Specialists	Included external cybersecurity consultants who provide cybersecurity services to HSSP and internal cybersecurity staff.	5
Product Support	Included product owners for the HSSP products, product support staff, and call centre.	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, leads and software engineers.	5
Integration Partners	Included IT and staff from integration partners.	2

used as a supplementary technique to complement, and validate and cross-reference the data we acquired through interviews.

5.3 Data analysis

For the thematic analysis, we followed the four-step guideline proposed by Green et al. (2007). Our study utilised a hybrid approach, combining deductive and inductive coding to develop themes (Fereday & Muir-Cochrane, 2006). Initially, we created a code template that included codes from the literature (Roberts et al., 2012). Initial codes were derived from key concepts from (DCC), (CL) and cybersecurity inertia (CI). Table 3 illustrates the key concepts that served as the foundation for our initial codes.

Table 3: Definition of key concepts

Key concept	Definition	Theory	Example from case
Cybersecurity flexibility	The ability of a firm to quickly and easily adapt its cybersecurity operations to capitalise on the external environment and proactively respond to cybersecurity threats that may affect the organisation's performance (Teece et al., 1997).	DCC	*"You know, we carry out tabletop exercises at least once a year. T-tops help us understand the potential threats we might face and explore various scenarios and permutations. By doing so, we get a better overview of our security risks and overall posture."*

[Continued …]

Table 3: […continued]

Key concept	Definition	Theory	Example from case
Cyber resource orchestration	The capacity of a firm to manage, coordinate and systematically combine its internal resources to position itself advantageously in the cyber environment (Helfat et al., 2007).	DCC	*"I don't think we can get a bigger team than what we currently have. However, we can leverage external consultants to provide backup support to our key team members. This approach should give us some breathing space and additional expertise without the need to hire more permanent security resources, which can be quite expensive."*
Cybersecurity anticipatory orientation	The ability of a firm to actively look for and respond to cybersecurity threats proactively. This is achieved by creating a culture of foresight, using various techniques to identify changes in the threat landscape, such as vulnerability scanning, penetration testing and secondary research (Teece, 2014; Teece et al., 1997).	DCC	*"Absolutely! I believe it's of utmost importance for HSSP (pseudo name) to understand and anticipate the actions of cybercriminals. Conducting vulnerability assessments and penetration tests at least annually can help us stay ahead of potential threats."*
Cybersecurity knowledge creation	Cybersecurity knowledge creation refers to creating, sharing, and storing cybersecurity knowledge within an organisation (Curado, 2006).	CL	*"… so there is need for continuous education and awareness of what's happening around us as far as system security is concerned. So I think that's very key for us as any organisation as HSSP to have those trainings, awareness continuously …"*
Cybersecurity memory	Cybersecurity memory is the process of retaining, sharing and leveraging cybersecurity information from past personal experiences within an organisation. It can be seen as a tool to enhance cyberthreat response within a company and allow for new opportunities (Wang & Ahmed, 2003).	CL	*"We need to continuously educate our users on information security issues. We need to educate users and carry out some random phishing assessments where we can identify users that potentially need additional training."*
Socio-techno inertia	Socio-technical inertia is the tendency of people and organisations to maintain the status quo when confronted with a new technology or process. This can include a reluctance to change, even when changes could offer significant benefits (Rowe et al., 2017).	CI	*"… 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."*

[Continued …]

Table 3: […continued]

Key concept	Definition	Theory	Example from case
Cybersecurity sensing	Refers to monitoring the external cybersecurity environment for possible opportunities and threats (Teece et al., 1997).	DCC	*"I think that as an organisation, we should do regular penetration testing of our systems so that we can identify loopholes before malicious hackers identify them. So, in other words, we should be proactive in identifying those loopholes."*
Cybersecurity seizing	This means the business must have the vision, insight and strategic foresight to identify and act upon cyberthreats (Teece et al., 1997).	DCC	*"Once we identify any vulnerabilities or weaknesses, we should be proactive and create a clear remediation plan before any incidents occur. This way, we can respond swiftly and effectively to any cyberthreats."*
Cybersecurity transforming	Refers to the ability to anticipate and adapt to changes in cyberthreats and to use resources and capabilities to shape and react to the cybersecurity environment (Teece et al., 1997).	DCC	*"We have started a process of migrating all our systems from on-premises to online, that is, to the cloud, which is a way of promoting high availability because you find that the cloud systems that we are using, some of them are in the US, some are in the UK and so forth. So it ensures high availability and allows us to recover when there is a disaster."*

The subsequent phase entailed validating the suitability of the initial codes by coding the documents and applying the deductive codes from the code template (Teece, 2014). The researcher meticulously analysed the interview transcripts line by line, resulting in the emergence of inductive codes when the deductive codes were insufficient in capturing meaning – these new insights led to the creation of new codes or extensions of existing ones (Rowe et al., 2017). The codes were consolidated into categories, where the relationships between the codes were examined to establish linkages and coherence. The final step encompassed identifying the overarching themes. ATLAS.ti and Microsoft Excel were used to code, categorise, and store themes.

5.4 Research ethics

We implemented multiple measures to adhere to research ethics. Firstly, the researcher obtained permission from HSSP's senior management. The researchers obtained permission to access relevant cybersecurity documents and interview key cybersecurity staff members. They also ensured strict compliance with privacy and confidentiality ethical guidelines at all times. Secondly, the University's ethics committee reviewed and approved the interview guide. Additionally, explicit consent was obtained from all participants, ensuring voluntary participation and respecting their autonomy. Furthermore, anonymity was preserved, protecting parti-

cipants' identities. Further, transparency was maintained through overt observations, where participants were informed in advance, and the study's purpose was communicated. These measures upheld ethical guidelines and safeguarded participants' rights and welfare, fostering an environment of trust and credibility (Soomro et al., 2016).

6 DYNAMIC CYBERSECURITY LEARNING DRIVERS AND CYBERSECURITY INERTIAL FORCES

We identified and analysed the cybersecurity inertia drivers, which are the forces that resist changes to the status quo in cybersecurity practices. These inertia drivers significantly hinder the development of dynamic cybersecurity learning capabilities (DCLC) within HSSP. To foster effective DCLC, addressing and mitigating these cybersecurity inertia drivers is imperative.

We also explored the dynamic cybersecurity learning drivers that push HSSP towards adopting and embracing dynamic cybersecurity learning capabilities. These drivers challenge the conventional cybersecurity norms and encourage organisations to seek adaptive and innovative solutions to overcome the inertia that impedes the implementation of dynamic cybersecurity learning capabilities. By understanding and leveraging these dynamic cybersecurity learning drivers, HSSP can actively drive transformative changes in its cybersecurity strategies and practices.

As dynamic cybersecurity capabilities strengthen, they weaken cybersecurity inertia (Chiu et al., 2016; Rowe et al., 2017). Dynamic cybersecurity capabilities collectively reduce the inertia caused by the socio-technological factors that impede organisational change. Similarly, we posit that dynamic cybersecurity capabilities are pivotal in weakening cybersecurity inertia.

Figure 2 reveals the antagonistic nature of two main factors influencing DCLC (Dynamic Cybersecurity Learning Capabilities): the dynamic cybersecurity learning drivers, which challenge the status quo, and the cybersecurity inertia drivers, which strive to maintain the current state. In Sections 7 and 8, we explore these antagonistic factors in depth.

7 CYBERSECURITY INERTIA DRIVERS

Cybersecurity inertia drivers encompass the factors that hinder cybersecurity learning within HSSP. These drivers create resistance to change, hamper adaptive cybersecurity practices, and elevate the risk of cyberattacks.

7.1 Strategic level inertia

Strategic inertia is the tendency of senior and middle-level management to remain with the status quo and resistance to strategic renewal outside the frame of current strategies (Hopkins et al., 2013). Senior management plays a critical role in the development of DCLC. Senior

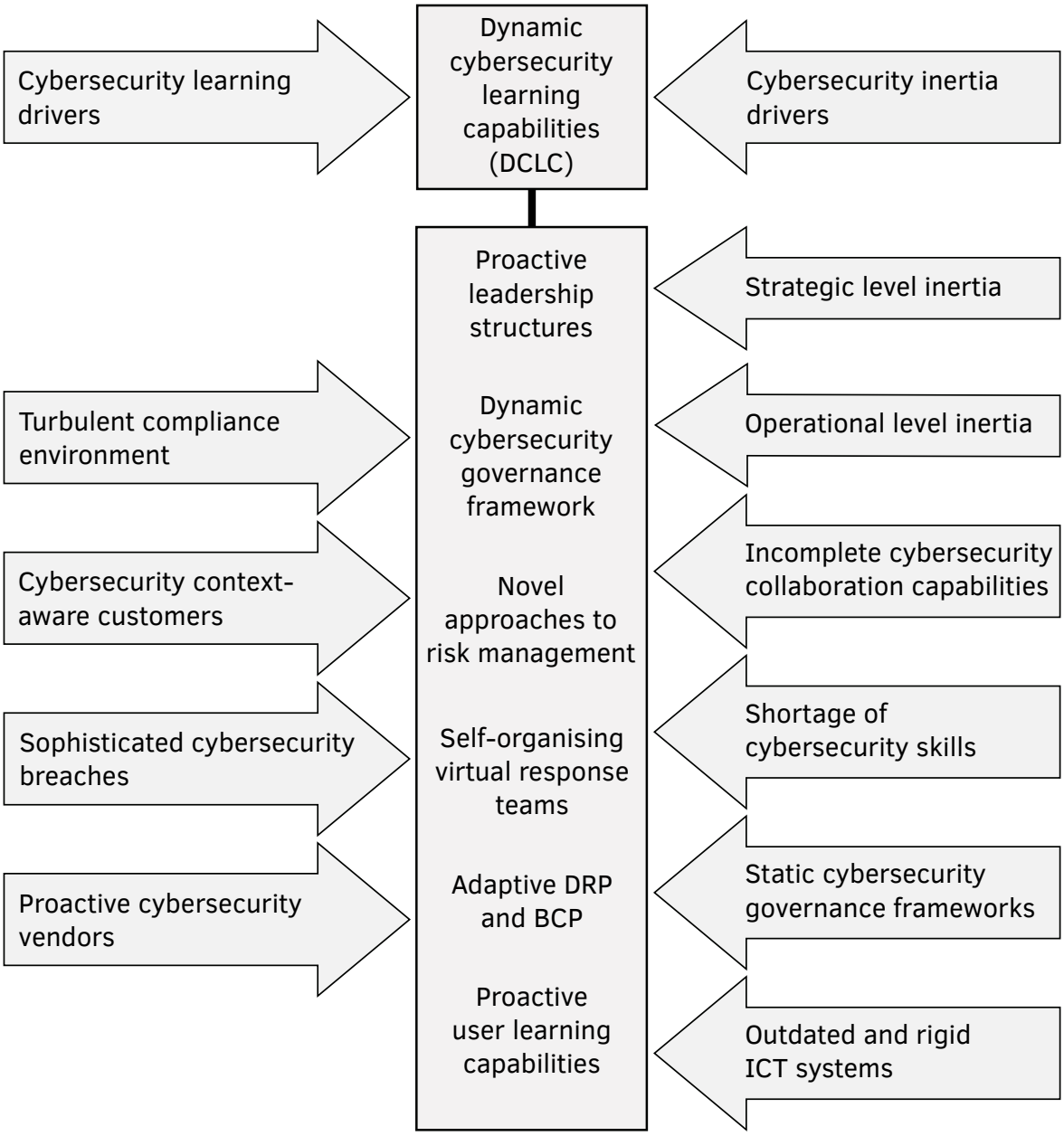

Figure 2: Dynamic cybersecurity learning drivers, cybersecurity inertial forces and DCLCs.

https://doi.org/10.18489/sacj.v36i1.18877

management is responsible for setting the tone and creating agile structures that create an enabling DCLC environment.

A cybersecurity expert argued that there is a gap between technical people and senior management. Cybersecurity experts mentioned,

> *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.*

Strategic level inertia contributes to cybersecurity inertia. Senior management sets the broad strategy for the organisation, including cybersecurity.

7.2 Incomplete cybersecurity collaboration capabilities

HSSP 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 offering and reduce non-core services duplication.*

The evidence gathered from the interviews suggests collaboration gaps as teams focus on their core competencies. The cybersecurity function is not involved in product design and evolution. When asked how cybersecurity is embedded in software development, a software development lead said,

> *Okay, 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.*

By cultivating a collaborative environment, HSSP can enhance its ability to detect cybersecurity threats proactively and devise cutting-edge countermeasures to combat them effectively.

7.3 Shortage of cybersecurity skills

The interviews showed that cybersecurity personnel prefer to work in the banking, telecommunications and financial service sectors. A former information security specialist said,

> *I left after three years mainly because I wanted financial and career growth. Remember, security is based on what you are trying to protect, so telecommunications are bigger than HSSP, 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.*

https://doi.org/10.18489/sacj.v36i1.18877

There is a global shortage of skilled cybersecurity professionals, and the estimated global shortfall of cybersecurity skills is 6 million (Burrell, 2018; Lewis & Crumpler, 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. A lack of cybersecurity skills makes it difficult for healthcare firms to cope with unpredictable cybersecurity threats. To address cybersecurity skills needs, organisations should strive to create an approach to cybersecurity that is actively monitored and regularly updated to meet the changing threats.

7.4 Static cybersecurity governance frameworks

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

An IT executive said,

> *We follow the best practices in everything we do, including 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.*

CSFs and best practices offer stability and predictability. However, CSFs are too rigid and may fail to give protection against adventurous cyberattackers developing exploits rapidly. There is a need for a dynamic framework which adapts to the ever-changing threat landscape.

7.5 Outdated ICT systems

A senior manager at HSSP mentioned,

> *I am sure you will also find some areas in 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.*

It was evident from the case that some key clients used legacy and vulnerable applications that could not be made obsolete for genuine business reasons. Legacy applications present significant security risks and vulnerabilities. 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). The dissemination of security vulnerabilities through blogs and journals inadvertently exacerbates the challenges posed by legacy applications. Although this documentation is created with the noble aim of keeping the security community informed and updated, it unintentionally provides hackers with novel information that can be used to craft exploits for cybersecurity attacks (Langer et al., 2016).

https://doi.org/10.18489/sacj.v36i1.18877

7.6 Operational level inertia

Operational level inertia refers to the phenomenon in which established routines limit the ability to introduce new processes and changes to the daily operations of an organisation. Operational level inertia often results from limited resources, outdated processes and manual processes that are hard to change.

Cybersecurity scholars agree that employees are the weakest link in the cybersecurity stack (Evans et al., 2019; Nobles, 2018; Streeter, 2015). Operational level inertia in cybersecurity manifests itself in users sticking to insecure information security practices, which puts the organisation at risk of successful social engineering attacks. Changing the insecure practices requires significant time, energy, information security awareness training and reinforcement.

A developer admitted not attending any information security awareness training since joining HSSP.

> *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. Still, 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.*

Information security awareness training reinforces cyber hygiene principles and helps employees proactively recognise and respond to user-side cyberattacks.

8 CYBERSECURITY LEARNING FORCES

In this section, we discuss the main forces for change. The forces or environmental influence that put pressure on organisations to adapt to changes in the cybersecurity environment. Cybersecurity learning forces pressure organisations to embed knowledge creation, retention and modification.

8.1 Turbulent compliance environment

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 senior management to focus more on developing dynamic cybersecurity learning capabilities.

https://doi.org/10.18489/sacj.v36i1.18877

8.2 Sophisticated cybersecurity breaches

There were some highly publicised high-profile cybersecurity breaches in the healthcare sector in South Africa. Life Healthcare hospital group in South Africa was targeted by ransomware attacks that stopped all IT systems in July 2020. At the time of the breach, the Group CEO posted on the Life Healthcare website,

> *We are deeply disappointed and saddened that criminals would attack our facilities during such a time when we are all working tirelessly and collectively to fight the COVID-19 pandemic.*

Cybersecurity breaches have shifted focus among IT and cybersecurity professionals. The cybersecurity breaches in the healthcare sector served as a warning to management. One application engineer mentioned,

> *I am not aware of any cybersecurity incident that has affected HSSP since I started working here. The only incident I remember is when we reimaged all the servers linked to firm Z (pseudo name) following an incident there.*

Cybersecurity breaches at key partners can have significant implications for HSSP.

8.3 Cybersecurity context-aware customers

Organisations the world over are increasingly becoming more conscious of their personal information. Organisations are increasingly demanding that their partners put comprehensive cybersecurity policies in place to avoid data breaches. Customers of Nedbank, a South African bank, were compromised through a third-party service provider, Computer Facilities (Pty) Ltd. The Nedbank compromise exposed the personal information of over 1.7 million customers (Roos, 2023).

The potential loss of data through third parties has resulted in partners of HSSP requesting additional cybersecurity controls. One cybersecurity expert mentioned that some integration partners are asking HSSP to complete annual cybersecurity questionnaires. According to the experts, HSSP's partners also demand cybersecurity assessment reports such as vulnerability analysis and penetration testing reports. A cybersecurity professional stated,

> *Of late, we have been receiving requests to fill in some forms with questions regarding our cybersecurity posture, vulnerability scans, penetration test, encryption and so on. I can say that this started in the last year or two. We have not yet started doing this to our integration partners. I think we may need to look at ourselves in the mirror and ask some questions: are we doing things right? Are we lagging? These are real issues that need genuine answers.*

8.4 Proactive cybersecurity vendors

Vendors of cybersecurity-related solutions trying to create awareness of their products publicise cybersecurity breaches and provide information on how their solutions provide defences

against cybersecurity breaches. Vendors of cybersecurity solutions are creating awareness of cybersecurity risks.

A cybersecurity expert at HSSP mentioned that members of the strategic leadership team are invited to the annual cybersecurity expo by Trend Micro, one of the vendors of cybersecurity solutions. The cybersecurity conference gives a platform for management to understand the key cybersecurity risks and the defences that can be put in place to defend against them. A cybersecurity expert mentioned,

> *I know of Amazon, Microsoft, Fortinet, to name a few. They showcase their solutions which can help us to solve some of our day-to-day challenges, I think the benefits of these exhibitions are two-fold really, first, they help us to introspect and identify some of our potential pain points, and obviously, they also help us to find solutions to our problems. It's like a doctor asking about your symptoms and also prescribing medication.*

9 DYNAMIC CYBERSECURITY LEARNING CAPABILITIES

After identifying cybersecurity inertia as a significant obstacle to DCLC, we propose interventions to overcome this challenge. These interventions aim to assist in the development of DCLC, ensuring a more agile and resilient cybersecurity approach at HSSP. Our argument emphasises that effectively managing cybersecurity inertia will lead to notable improvements in DCLC. HSSP can enhance its ability to adapt and respond proactively to the evolving cyberthreat landscape by addressing and mitigating cybersecurity inertia.

9.1 Proactive leadership structures

Executive management is responsible for setting the tone and disseminating information regarding the organisation's risk appetite. The board of directors (BoD) is ultimately responsible and accountable for cybersecurity (von Solms & von Solms, 2018). The BoD may delegate responsibility for cybersecurity to executive management.

To improve the involvement of senior management in cybersecurity, we are proposing proactive leadership structures to guide the development and implementation of DCLC. Proactive leadership structures include an IT security steering committee with members drawn from leaders of all the important facets of the business. IT security steering committees are recommended by scholars (Alkhaldi et al., 2017; Parekh, 2009) and the cybersecurity practitioners we interviewed. An IT security steering committee improves collaboration and dissemination of cybersecurity-related, improving the responsiveness against cyberthreats.

9.2 Dynamic cybersecurity governance framework

The cybersecurity governance framework provides an organisation with an all-encompassing, holistic plan for information security (Da 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 the cybersecurity professionals interviewed concurred that a cybersecurity governance framework is necessary for managing the cybersecurity function. Cybersecurity frameworks are static and are updated only after preset intervals. We propose the implementation of a dynamic cybersecurity governance, which builds on continuous sensing of the environment, mobilising internal resources and renewing cybersecurity capabilities.

9.3 Novel risk management approaches

Cybersecurity experts recommended implementing novel approaches to risk management, such as regular vulnerability assessments, penetration tests, security assessments, and cyber insurance (Siegel et al., 2002). Innovative insurance solutions, such as cyber insurance, are a fallback plan, acting as a last resort if other risk management approaches prove insufficient (Woods & Simpson, 2017). Leveraging our dynamic cybersecurity learning capabilities approach, HSSP can swiftly detect and respond to cyberthreats, minimising the risks associated with cyber-attacks and safeguarding their valuable information and reputation.

9.4 Self-organising virtual response teams

PARTICIPANT 8 said,

> *I think maybe if we are to have an application security specialist, that will be great because that person will now have the time to look specifically at security issues associated or which are around the development of software and then another thing that we could also do is maybe to adopt DevSecOps that is to embed security right from the start to ensure that at that moment we are gathering requirements, we also embed security up to the point where we are deploying a system. I think that will give us more secure systems.*

Self-organising teams such as DevSecOps can be used in cybersecurity for greater response and resilience to cyberthreats (Prates et al., 2019). Self-organising teams are composed of highly skilled individuals who can self-manage, adapt and learn new tasks whilst being empowered by the team as a whole (Myrbakken & Colomo-Palacios, 2017). Such teams behave as autonomous units, making decisions collectively and without the need for direct manager input. In this context, the perceived benefits of self-organising teams include reduced decision-making times, greater problem-solving capabilities, a stronger focus on creative solutions and improved organisational performance.

DevSecOps brings together development security and operations. DevSecOps incorporates modern security practices in DevOps's dynamic and agile world (Prates et al., 2019). The DevSecOps model improves the coordination between security and development and ensures security is built into systems design.

9.5 Proactive user learning capabilities

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 study revealed that HSSP's information security education interventions are inadequate. The cybersecurity practitioners interviewed emphasised the importance of information security awareness training. Most cybersecurity practitioners recommended that HSSP invest in online information security awareness platforms. A participant recommended regular penetration tests targeting users to measure information security awareness's effectiveness and identify training needs.

9.6 Adaptive disaster recovery and business continuity planning

The existing business continuity plans (BCP) and disaster recovery plans (DRP) need to be tested regularly to ensure the plans remain effective and relevant (Budiman et al., 2020). From the document review, we deduced that the existing plans had not been subjected to routine testing. We highly recommend conducting tests of business continuity plans at least once a year to prevent disruptions in the event of significant cybersecurity breaches (Budiman et al., 2020). Disaster recovery plan testing is important for two primary reasons: It helps determine whether the existing plan is relevant, complete, and adequate. It helps team members know what to do in a disaster (Cerullo & Cerullo, 2004).

10 DISCUSSION

This study makes several theoretical contributions. The study extends the dynamic capabilities theory (Helfat et al., 2007; Teece et al., 1997; Zollo & Winter, 2002) by introducing a novel dynamic capability, namely dynamic cybersecurity learning capabilities. The study integrates the concepts from dynamic capabilities theory with organisational learning and organisational inertia. We identified how socio-technical inertia can impede the development of DCLC. Organisational learning and organisational inertia theories provide a way to understand the inertial forces impeding dynamic cybersecurity learning. The theories provide a novel understanding of the inertial forces impeding the development of cybersecurity capabilities. Although organisational learning and inertia theories were initially formulated to offer insights at the corporate strategic level (Helfat et al., 2007; Teece et al., 1997), we contend these theories can be adapted and applied to cybersecurity.

This study offers valuable insights for practitioners looking to enhance cybersecurity within their healthcare software service firms. Practitioners often rely on static cybersecurity frameworks such as NIST CSF, ISO 27000, and CIS 20 (Frumento, 2019; Ibrahim et al., 2018).

However, this research goes a step further by expanding the capabilities of these existing frameworks, making them more agile and adaptable to evolving threats.

Additionally, traditional practitioner frameworks typically provide broad recommendations suitable for various organisations, irrespective of their specific contexts. In contrast, our proposed DCLC (Dynamic Cybersecurity Learning Capabilities) model considers the unique context of a healthcare software service firm. By gathering relevant data, we identified the inertial forces hindering the development of DCLC and designed a tailored model to address these challenges effectively. The context-aware approach of our DCLC model aims to optimise cybersecurity measures, enabling practitioners to bolster their organisation's resilience against cyberthreats within the healthcare domain.

Prior research has shown that most cybersecurity breaches result from human error (Evans et al., 2019; Nobles, 2018; Streeter, 2015), and deliberate measures should be taken in employee and management learning. Employees must be continuously reminded of how to prevent, detect, respond to, and recover from cyberattacks. Management should set the tone and provide leadership in developing dynamic cybersecurity learning capabilities. This study encourages practitioners to challenge the status quo and look for ways to create, disseminate, modify and retain new cybersecurity knowledge on an ongoing basis. Practitioners are urged to sense the environment continuously, seize opportunities and transform the organisation's cybersecurity function.

Our study is not a panacea to cybersecurity challenges at HSSP. Our proposed solutions are neither exhaustive nor prescriptive. The proposed solutions should be tested at the HSSP to have an opinion on their efficacy. This study cannot be replicated at other healthcare software service firms; independent studies should be performed.

Future research should test the effectiveness of the proposed initiatives at HSSP. Without testing the initiatives, they remain propositions. Future research could also test the applicability of the findings to other healthcare settings. The theoretically grounded dynamic cybersecurity learning framework provides novel approaches to managing ever-changing cybersecurity threats. Our DCLC model differs from existing studies because it fuses concepts from practitioner-centric cybersecurity frameworks with theoretical aspects from dynamic capabilities, organisational learning and organisational inertia.

11 CONCLUSIONS

In conclusion, this case study pinpointed the inertial forces hindering dynamic cybersecurity learning capabilities within a healthcare software services firm. By conducting semi-structured interviews with experts and analysing corporate documents, we gained valuable insights from these individuals and the existing records of the company. Through thematic analysis, the study uncovered two crucial aspects: the organisational inertia forces that maintain the status quo and hinder cybersecurity learning and the cybersecurity learning forces that drive organisations to proactively adapt to dynamic changes in the cybersecurity landscape by acquiring, modifying, and retaining knowledge.

https://doi.org/10.18489/sacj.v36i1.18877

Identifying these contrasting forces sheds light on the pivotal interplay between organisational inertia and cybersecurity learning, underscoring their significant impact on shaping cybersecurity learning within healthcare software as a service firm. Moreover, the study proposes dynamic cybersecurity capabilities as a plausible solution to counteract the inhibiting effects of organisational inertia.

By cultivating dynamic cybersecurity capabilities, HSSP can effectively overcome the barriers that impede reinvention and fortification, enhancing its cybersecurity posture in the face of persistent threats. The research emphasises the importance of adaptability and continuous learning in fostering a robust and resilient cybersecurity approach for healthcare software services firms.

Pursuing Dynamic Cybersecurity Learning Capabilities (DCLC) represents a vital and promising research agenda for cybersecurity scholars, extending beyond the healthcare domain to encompass other critical sectors. By harnessing DCLC, the healthcare sector and other industries could significantly enhance their responsiveness to multifaceted cyberattacks. We believe that adopting the proposed DCLC framework will better enable healthcare organizations to continually adapt, learn, and evolve in response to rapidly emerging cyberthreats. This proactive approach will also help healthcare organizations to strengthen their defences and overcome strategic and operational inertial forces. Finally, we hope that researchers will further develop the dynamic learning capability perspective to advance cybersecurity knowledge, thereby bolstering organizational resilience in the face of rapidly evolving cyberthreats.

References

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, *62*(4), 539–548. https://doi.org/10.1016/J.BUSHOR.2019.03.010

Adomako, K., Mohamed, N., Garba, A., & Saint, M. (2018). Assessing cybersecurity policy effectiveness in Africa via a cybersecurity liability index. *TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy*. https://doi.org/10.2139/SSRN.3142296

Akinsanya, O. O., Papadaki, M., & Sun, L. (2019). Current cybersecurity maturity models: How effective in healthcare cloud? *Proceedings of the 5th Collaborative European Research Conference (CERC 2019)*, 211–222. https://ceur-ws.org/Vol-2348/paper16.pdf

Alkhaldi, F. M., Hammami, S. M., & Uddin, M. A. (2017). Understating value characteristics toward a robust IT governance application in private organizations using COBIT framework. *International Journal of Engineering Business Management*, *9*, 1–8. https://doi.org/10.1177/1847979017703779

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. https://doi.org/10.1016/J.IJHCS.2015.05.005

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. *International Journal of Internet and Enterprise Management*, *6*(4), 279. https://doi.org/10.1504/IJIEM.2010.035624

Ashok, M., Dhaheri, M. S. M. A. B. A., Madan, R., & Dzandu, M. D. (2021). How to counter organisational inertia to enable knowledge management practices adoption in public sector organisations. *Journal of Knowledge Management*, *25*(9), 2245–2273. https://www.emerald.com/insight/content/doi/10.1108/JKM-09-2020-0700/full/html

Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: Context and shared concepts. *Journal of Cyber Policy*, *3*(2), 258–283. https://doi.org/10.1080/23738871.2018.1520271

Baškarada, S. (2014). Qualitative case study guidelines. *The Qualitative Report*, *19*(40), 1–18. https://doi.org/10.46743/2160-3715/2014.1008

Besson, P., & Rowe, F. (2012). Strategizing information systems-enabled organizational transformation: A transdisciplinary review and new directions. *The Journal of Strategic Information Systems*, *21*(2), 103–124. https://doi.org/10.1016/J.JSIS.2012.05.001

Borkovich, D. J., & Skovira, R. J. (2019). Cybersecurity inertia and social engineering: Who's worse, employees or hackers? *Issues in Information Systems*, *20*(3), 139–150. https://doi.org/10.48009/3_iis_2019_139-150

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), 032023. https://doi.org/10.1088/1742-6596/1567/3/032023

Burke, I. D., Motlhabi, M. B., Netshiya, R., & Pieterse, H. (2021). Lost packet warehousing service. *Proceedings of the 16th International Conference on Cyber Warfare and Security*, 545. https://researchspace.csir.co.za/dspace/handle/10204/12036

Burrell, D. N. (2018). An exploration of the cybersecurity workforce shortage. *International Journal of Hyperconnectivity and the Internet of Things*, *2*(1), 29–41. https://doi.org/10.4018/IJHIOT.2018010103

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. https://doi.org/10.1016/J.PROCIR.2016.03.059

Cerullo, V., & Cerullo, M. J. (2004). Business continuity planning: A comprehensive approach. *Information Systems Management*, *21*(3), 70–78. https://doi.org/10.1201/1078/44432.21.3.20040601/82480.11

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, *23*, 1–11. https://doi.org/10.4102/SAJIM.V23I1.1277

Chiu, W. H., Chi, H. R., Chang, Y. C., & Chen, M. H. (2016). Dynamic capabilities and radical innovation performance in established firms: A structural model. *Technology Analysis & Strategic Management*, *28*(8), 965–978. https://doi.org/10.1080/09537325.2016.1181735

Chuma, K. G., & Ngoepe, M. (2022). Security of electronic personal health information in a public hospital in South Africa. *Information Security Journal: A Global Perspective*, *31*(2), 179–195. https://doi.org/10.1080/19393555.2021.1893410

Crossan, M. M., & Berdrow, I. (2003). Organizational learning and strategic renewal. *Strategic Management Journal*, *24*(11), 1087–1105. https://doi.org/10.1002/SMJ.342

Curado, C. (2006). Organisational learning and organisational design. *Learning Organization*, *13*(1), 25–48. https://doi.org/10.1108/09696470610639112

Da Veiga, A., & Eloff, J. (2007). An information security governance framework. *Information Systems Management*, *24*(4), 361–372. https://doi.org/10.1080/10580530701586136

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. https://doi.org/10.1057/PALGRAVE.EJIS.3000478

Easterby-Smith, M. (1997). Disciplines of organizational learning: Contributions and critiques. *Human Relations*, *50*(9), 1085–1113. https://doi.org/10.1023/A:1016957817718

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they? *Strategic Management Journal*, *21*, 1105–1121. https://doi.org/10.1002/1097-0266(200010/11)21:10/11<1105::AID-SMJ133>3.0.CO;2-E

Evans, M., He, Y., Maglaras, L., & Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers & Security*, *80*, 74–89. https://doi.org/10.1016/J.COSE.2018.09.002

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. https://doi.org/10.1177/160940690600500107

Ferreira, J., Cardim, S., & Coelho, A. (2021). Dynamic capabilities and mediating effects of innovation on the competitive advantage and firm's performance: The moderating role of organizational learning capability. *Journal of the Knowledge Economy*, *12*(2), 620–644. https://doi.org/10.1007/s13132-020-00655-z

Frumento, E. (2019). Cybersecurity and the evolutions of healthcare: Challenges and threats behind its evolution. *EAI/Springer Innovations in Communication and Computing*, 35–69. https://doi.org/10.1007/978-3-030-02182-5_4

Goodwin, B. (2022). Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack – Computer Weekly [Accessed 30 June 2024]. https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus

Gopal, N., & Maweni, V. (2019). Cybercrime preparedness – a critical snapshot of BRICS countries. *Africa Insight*, *49*(2). https://hdl.handle.net/10520/EJC-197e445801

Graham, C. (2021). Fear of the unknown with healthcare IoT devices: An exploratory study. *Information Security Journal: A Global Perspective*, *30*(2), 100–110. https://doi.org/10.1080/19393555.2020.1810369

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. https://doi.org/10.1111/J.1753-6405.2007.00141.X

Helfat, C. E., Finkelstein, S., W., M., Peteraf, M. A., Singh, H., Teece, D. J., & Winter, S. G. (2007). *Dynamic capabilities: Understanding strategic change in organizations*. Blackwell Publishing. https://www.wiley.com/en-us/Dynamic+Capabilities%3A+Understanding+Strategic+Change+in+Organizations-p-9781405135757

Hopkins, W. E., Mallette, P., & Hopkins, S. A. (2013). Proposed factors influencing strategic inertia/strategic renewal in organizations. *Academy of Strategic Management Journal, 12*(2), 77–94. https://www.abacademies.org/journals/month-december-year-2013-vol-12-issue-2-journal-asmj-past-issue.html

Hur, J. Y., Cho, W., Lee, G., & Bickerton, S. H. (2019). The "smart work"' myth: How bureaucratic inertia and workplace culture stymied digital transformation in the relocation of South Korea's capital. *Asian Studies Review, 43*(4), 691–709. https://doi.org/10.1080/10357823.2019.1663786

Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: A case study. *Journal of Supercomputing, 74*(10), 5171–5186. https://doi.org/10.1007/S11227-018-2479-2

Kiser, S., & Maniam, B. (2021). Ransomware: Healthcare industry at risk. *Journal of Business and Accounting, 14*(1), 64–81. https://www.proquest.com/docview/2667273522?sourcetype=Scholarly%20Journals

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A stematic review of modern threats and trends. *Technology and Health Care, 25*(1), 1–10. https://doi.org/10.3233/THC-161263

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*, 1–12. https://doi.org/10.1109/ECRIME.2008.4696970

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. https://doi.org/10.1016/J.COSE.2016.07.008

Lewis, J. A., & Crumpler, W. (2019). The cybersecurity workforce gap [Accessed 2 April 2023]. https://www.csis.org/analysis/cybersecurity-workforce-gap

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *BMJ*, *358*(1), 4–7. https://doi.org/10.1136/BMJ.J3179

Mayhorn, C. B., & Nyeste, P. G. (2012). Training users to counteract phishing. *Work (Reading, Mass.)*, *41*(1), 3549–3552. https://doi.org/10.3233/WOR-2012-1054-3549

Mehra, K., & Dhawan, S. K. (2003). Study of the process of organisational learning in software firms in India. *Technovation, 23*(2), 121–129. https://doi.org/10.1016/S0166-4972(01)00089-X

Moyo, A. (2023). Momentum Metropolitan hacked – ITWeb [Accessed 30 June 2024]. https://www.itweb.co.za/article/momentum-metropolitan-hacked/RgeVDqPYBdpvKJN3

Myrbakken, H., & Colomo-Palacios, R. (2017). DevSecOps: A multivocal literature review. In A. Mas, A. Mesquida, R. V. O'Connor, T. Rout & A. Dorling (Eds.), *Software process improvement and capability determination* (pp. 17–29). Springer International Publishing. https://doi.org/https://doi.org/10.1007/978-3-319-67383-7_2

Naseer, H., Ahmad, A., Maynard, S., & Shanks, G. (2018). Cybersecurity risk management using analytics: A dynamic capabilities approach. *International Conference on Information Systems (ICIS 2018) Proceedings*, 4. https://aisel.aisnet.org/icis2018/governance/Presentations/4

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. https://www.ajol.info/index.php/ajlais/article/view/217793

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3), 71–88. https://doi.org/10.2478/HJBPA-2018-0024

Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T., & Kagaya, T. (2009). Information security governance framework. *Proceedings of the ACM Conference on Computer and Communications Security*, 1–6. https://doi.org/10.1145/1655168.1655170

Olofinbiyi, S. A. (2022). A reassessment of public awareness and legislative framework on cybersecurity in South Africa. *ScienceRise: Juridical Science*, *2*(20), 34–42. https://doi.org/10.15587/2523-4153.2022.259764

Papastergiou, S., Mouratidis, H., & Kalogeraki, E. M. (2021). Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures. *Evolving Systems*, *12*(1), 91–108. https://doi.org/10.1007/S12530-020-09335-4

Parekh, B. (2009). Information security steering committee. *Proceedings of the 2009 Information Security Curriculum Development Annual Conference, InfoSecCD'09*, 148–150. https://doi.org/10.1145/1940976.1941005

Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. *The African Journal of Information and Communication (AJIC)*, *28*, 1–21. https://doi.org/10.23962/10539/32213

Prates, L., Faustino, J., Silva, M., & Pereira, R. (2019). DevSecOps metrics. In S. Wrycza & J. Maślankowski (Eds.), *Information systems: Research, development, applications, education* (pp. 77–90). Springer International Publishing. https://doi.org/https://doi.org/10.1007/978-3-030-29608-7_7

Renaud, K., & Ophoff, J. (2019). Modeling inertia causatives: Validating in the password manager adoption context. *Dewald Roode Workshop on Information Systems Security Research, IFIP Working Group IFIP 8.11/11.13*, 1–14. https://rke.abertay.ac.uk/en/publications/modeling-inertia-causatives-validating-in-the-password-manager-ad

Roberts, N., Galluch, P. S., Dinger, M., & Grover, V. (2012). Absorptive capacity and information systems research: Review, synthesis, and directions for future research. *MIS Quarterly: Management Information Systems*, *36*(2), 625–648. https://doi.org/10.2307/41703470

Roos, A. (2023). Data protection principles under the GDPR and the POPI Act: A comparison. *Journal of Contemporary Roman-Dutch Law*, *86*(1), 1. https://collections.concourt.org.za/handle/20.500.12144/38297

Rowe, F., Besson, P., & Hemon, A. (2017). Socio-technical inertia, dynamic capabilities and environmental uncertainty: Senior management views and implications for organizational transformation. *Proceedings of the 25th European Conference on Information Systems (ECIS)*. https://aisel.aisnet.org/ecis2017_rp/27/

Ruiz-Mercader, J., Meroño-Cerdan, A. L., & Sabater-Sánchez, R. (2006). Information technology and learning: Their relationship and impact on organisational performance in small businesses. *International Journal of Information Management*, *26*(1), 16–29. https://doi.org/10.1016/J.IJINFOMGT.2005.10.003

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*, 405–409. https://doi.org/10.1109/DEXA.2003.1232055

Scofield, M. (2016). Benefiting from the NIST cybersecurity framework. *Information Management*, *50*(2), 25–28. https://www.proquest.com/docview/1779940925

Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-risk management: Technical and insurance controls for enterprise-level security. *Information Systems Security*, *11*(4), 33–49. https://doi.org/10.1201/1086/43322.11.4.20020901/38843.5

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/J.IJINFOMGT.2015.11.009

Sparrell, D. (2019). Cyber-safety in healthcare IOT. *11th Academic Conference ITU Kaleidoscope: ICT for Health: Networks, Standards and Innovation (ITU K)*, 1–8. https://doi.org/10.23919/ITUK48006.2019.8996148

Streeter, D. (2015). The effect of human error on modern security breaches. *Strategic Informer: Student Publication of the Strategic Intelligence Society*, *1*(3), 2. https://digitalcommons.liberty.edu/si/vol1/iss3/2

Sutherland, E. (2021). The governance of data protection in South Africa. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3922218

Teece, D. J. (2014). The foundations of enterprise performance: Dynamic and ordinary capabilities in an (economic) theory of firms. *https://doi.org/10.5465/amp.2013.0116*, *28*(4), 328–352. https://doi.org/10.5465/AMP.2013.0116

Teece, D. J. (2018). Business models and dynamic capabilities. *Long Range Planning*, *51*(1), 40–49. https://doi.org/10.1016/J.LRP.2017.06.007

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, *18*, 509–533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z

Thompson, E. C. (2017). *Building a HIPAA-compliant cybersecurity program*. Apress. https://doi.org/10.1007/978-1-4842-3060-2

Townsend, B. (2022). The lawful sharing of health research data in South Africa and beyond. *Information & Communications Technology Law*, *31*(1), 17–34. https://doi.org/10.1080/13600834.2021.1918905

Visser, M. (2011). Constructing organisational learning and knowledge socially: An interactional perspective. *International Journal of Knowledge and Learning*, *6*(4). https://www.inderscienceonline.com/doi/abs/10.1504/IJKL.2010.03865

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Walker, T., Allen, K., Abderrahmane, A., & Yared, T. (2021). Balancing basic freedoms and the need to fight against cybercrime. *ISS Peace and Security Council Report*, *2021*(137). https://hdl.handle.net/10520/ejc-ispscr-v2021-n137-a2

Walsham, G. (1995). Interpretive case studies in is research: Nature and method. *European Journal of Information Systems*, *4*(2), 74–81. https://doi.org/10.1057/EJIS.1995.9

Wang, C. L., & Ahmed, P. K. (2003). Organisational learning: A critical review. *The Learning Organization*, *10*(1), 8–17. https://doi.org/10.1108/09696470310457469

Woods, D., & Simpson, A. (2017). Policy measures and cyber insurance: A framework. *Journal of Cyber Policy*, *2*(2), 209–226. https://doi.org/10.1080/23738871.2017.1360927

Yayla, A., & Lei, Y. (2020). Information technology implementation and organizational change: A dissipative structure theoretical lens. *The Journal of the Southern Association for Information Systems*, *6*(1), 1–21. https://doi.org/10.17705/3JSIS.00011

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.).

Zollo, M., & Winter, S. G. (2002). Deliberate learning and the evolution of dynamic capabilities. *Organization Science*, *13*(3), 339–351. https://doi.org/10.1287/ORSC.13.3.339.2780