The African Journal of Information Systems

Volume 13 | Issue 3 Article 3

August 2021

Evolving Information Security Governance Practices from Evolving Technologies: Focus on Covid-19 Lockdowns

Cosmas Ngwenya
University of Johannesburg, cosmo4n@yahoo.com

Kennedy Njenga
University of Johannesburg, knjenga@uj.ac.za

The African Journal of Information Systems

Evolving Information Security Governance Practices from Evolving Technologies: Focus on Covid-19 Lockdowns

Research Paper

Volume 13, Issue 3, August 2021, ISSN 1936-0282

Cosmas Ngwenya
University of Johannesburg
cosmo4n@yahoo.com

Kennedy Njenga
University of Johannesburg
knjenga@uj.ac.za

(*Received January 2021, accepted July 2021*)

ABSTRACT

This paper contemporizes evolving information security (IS) governance practices during the coronavirus pandemic (Covid-19) in South Africa. Using post-structuralism as a lens, we offer distinct insights regarding how information systems and technologies are evolving and the impact they present to the governance of IS systems during intermittent lockdowns. An online self-administered questionnaire was designed and distributed using Google forms to elicit data around evolution. A link was emailed to 160 respondents fitting pre-defined criteria. Data was exported to a statistical analysis software for analysis. Our results present an important relationship between technology evolutions and IS threats and that changes in technology as well as IS threats lead to changes in work routines and notably, IS governance. The model presented by this study helps IS practitioners understand how these important changes can be managed during these uncertain times.

Keywords

Information security, governance, technology, evolution.

INTRODUCTION

As businesses in South Africa embrace digital transformation such as the Internet of Everything (IoE), (Snyder & Byrd, 2017) more pressure has been placed on information security (IS) practitioners who are mandated to protect information hosted by information systems and technologies (Mell & Grance, 2011). Importantly, as technologies evolve, so will the security protocols embedded in IoE evolve (Garzia & Papi, 2016). Evolving technologies display an array of complexity regarding how information across multiple platforms is created, stored, analysed, and processed (Sagiroglu & Sinanc, 2013). Many business devices have evolved, and many are embedded with sensors and advanced software, including but not limited to smartphones, tablets, printers, webcams, navigation systems, and security alarms. All of these can now connect to form a network described as IoE (Stergiou et al., 2018). Software

development has evolved at a similarly rapid rate and developers previously working as isolated silos, are now able to collaborate as remote teams due to better connectivity (Ebert, et al., 2016).

The year 2019 was unique and unprecedented because a global pandemic namely the coronavirus pandemic, led to global lockdowns which have since been intermittent. For the first time, the entire global workforce, except for those providing essential services to the health industry, was required to work from home (Lallie et al., 2021). In order then for businesses to remain operational and coordinated, a concerted effort was necessary, requiring most to heavily rely on connected technologies across multiple regions. Technology evolution became catalysed by the pandemic and technologies such as IoE skyrocketed exponentially and those working from home could now harness the power of these innovations, not only to their advantage but also that of their employers as well. What then followed was that these connected technologies became lucrative targets for cybercriminals and those targeting information infrastructure for nefarious reasons (Sergey et al., 2017). There were reports of scams impersonating public authorities and businesses such as the World Health Organisation and airlines (Lallie et al., 2021). These scams targeted—and continue to target—millions of individuals working from home.

Working from home, therefore, started to create a unique challenge to information security practitioners because cybercriminals were increasingly innovative, and as the technology infrastructure continued to evolve rapidly, so did many of the recently witnessed IS threats. IS governance practitioners as well as those working from home had never experienced such scale and nature of these attacks as witnessed. These attacks also exposed the level of under-preparedness faced by IS governance practitioners of connected global information systems and technologies. Indeed for instance, in the United Kingdom (UK), the highest number of computer viruses were recorded in April 2020, the peak of lockdown when Covid-19 measures were at their strictest (Buil-Gil et al., 2020). Similarly, those South African businesses having advanced technologies across many spheres of operations also became prime candidates for external attacks. Indeed, during the peak of lockdowns in South Africa, a study by Rananga & Venter (2020) suggested that cloud service providers observed a big upsurge in the usage of cloud-based technologies and that the cost-effectiveness and ease of use of mobile cloud computing (MCC) gained traction rapidly. The security around the use of these MCC technologies however remained a challenge (Rananga & Venter, 2020). Moreover, a report by Paton (2019) confirmed that the banking industry in South Africa was hit by a wave of ransom driven distributed denial of service attack (DDoS) that targeted various customers facing services across multiple banks. Paton (2019) also reported a breach to the city of Johannesburg's network that shut down its website and all e-services, some hours after receiving a ransom note demand of 4.0 bitcoins–a similar technique to that used to attack the banks–from a group called Shadow Kill Hacker (Paton, 2019).

Objective of Research

As a result of businesses operating in unprecedented times during the Covid-19 pandemic, this work is motivated by a need to understand the impact of the evolution of technology arising from intermittent lockdowns in South Africa, and how this has impacted the evolution of IS security threats, work routines (routinization), and whether there is a quantifiable impact on institutional goals and importantly the governance of IS. An attempt is therefore made to contemporize evolving IS governance practices during the Covid-19 lockdown as a dependent variable and to model a framework that can predict this.

Addressing the above evolutions is particularly important because of the adverse impact this can have on the proper governance of IS infrastructure. We apply post-structuralism, drawn from interdisciplinary theories of social sciences, information systems, and management as a theoretical lens. By carrying out a

study during the peak of the Covid-19 pandemic beginning March 2020, we draw on this conundrum of evolution. Importantly, we do not simply point out the underlying evolutions that technology has undergone in times of the Covid-19 pandemic, we point to how information technology (IT) governance practitioners' governance practices may be improved upon using our framework.

In doing so, we organise this work as follows; the introduction has provided a background into IS governance practices in light of heavy IT usage during lockdowns caused by the Covid-19 pandemic. A review of literature then follows and presents a discourse on why businesses need to put in measures to improve IS governance practices. We explain the methodology of this research following the literature review and finally, present the data that was collected and analysed, and what this observed data tells us. Implications of findings are presented in the penultimate sections.

LITERATURE REVIEW

As technology continues to evolve, so does its use. In recent times it has not been uncommon to witness new use of technology for the betterment of African businesses, such as the use of cloud computing and the value this has provided to South African businesses (Johnston et al., 2016). Countries like Mozambique have improved on their governance practices using technologies (Macueve, 2008) and importantly service delivery has been greatly enhanced in countries such as Nigeria because of technology (Dahunsi, 2017). Countries like Ethiopia now use advanced technologies for the treatment of diseases such as tuberculosis (Sorsa et al., 2020) and provision of short messaging service as intervening HIV awareness programs (Bandyopadhyay et al., 2018). African countries have also started witnessing technology use for nefarious reasons such as cyberbullying (Oosterwyk & Kabiawu, 2016) and threats to information assets when South African businesses experience compromised passwords (Butler & Butler, 2018).

As South African businesses continue to evolve, the existing IS governance practices and work routines, continue to slowly evolve (Nyoni et al., 2020). It is therefore important for these businesses to evolve and change their work practices more rapidly to remain resilient in mitigating against IS threats. This call is now more urgent particularly during periods of Covid-19 lockdowns when many South African businesses require their workforce to use technology to work from home. What is worrying is that many of those working from home are not immune to cybersecurity attacks. The global Cyber Exposure Index ranks South Africa sixth on the list of most-targeted countries for cyber-attacks according to a report by First Distribution (2019). In this respect, South African businesses are therefore required to have proper IS governance practices to remain competitive. We consider literature regarding evolution and IS governance practices in the sections that follow.

Information Security Governance in South Africa

IS governance is the process of placing proper methods and practices for defending IT resources and data from IS threats (Kaspersky, n.d.). The International Organisation for Standardization (2020) defines IS governance as "guides concepts, objectives, and processes for the governance of information security, by which organizations can evaluate, direct, monitor and communicate the information security-related processes within the organization" (p. 1). IS governance ensures that controls are implemented to mitigate risks and will often involve procedures that influence actions (Sylvan, 2014). Literature shows that existing IS governance practices remain unsustainable because new IS threats continually evolve (Kshetri & Kshetri, 2016). Despite advancements in technology, evolving institutional goals and the role of human agency within organisations makes IS governance challenging.

In South Africa, IS governance is anchored on regulatory frameworks in common law statutes that guarantee the right of protection of personal information as well as information privacy (Ntsaluba, 2018). There are several frameworks such as the National Cybersecurity Policy Framework, the Protection of Personal Information Act, and the Cybersecurity and Cybercrimes Bill which provide a foundation for creating an infrastructure of best practices for information security (Nyoni et al., 2020).

Information Security Governance During Covid-19

Covid-19 which started in early 2019 quickly became a global crisis, occasioning mass lockdowns that affected businesses on a global scale. Most workers were required to work from home. The lockdowns forced many businesses to carry out operations that are heavily technology-centric and reliant on remote internet connectivity for their workers. This was also the time many of these businesses and those working from home witnessed unprecedented external IS attacks and threats on critical infrastructure (Lallie et al., 2021). A recent study by Nyoni et al. (2020) shows that those regulating new and emerging technologies view these technologies as potentially risky. It is due to these revolutionary technologies that it becomes necessary that regulators develop robust laws to help prevent potential violations and IS threats to information (Nyoni et al., 2020).

Similarly, outside of South Africa and in response to emergent IS threats, on 8th of April 2020 the UK's National Cyber Security Centre as well as the United States Department of Homeland Security Cybersecurity and Infrastructure Security Agency published a joint advisory on how cybercriminals and advanced persistent threat groups were exploiting the current COVID-19 pandemic (Lallie et al., 2021). Issues discussed by the advisory considered how businesses needed to be alerted to IS threats such as phishing and malicious software (malware) attacks on compromised communications platforms such as Zoom and Microsoft Teams to those working from home. Buil-Gil et al.'s (2020) UK study likewise carried out during the peak of Covid-19 lockdown measures between May 2019 and May 2020 noted as follows:

> most cyber-dependent and cyber-enabled crimes have experienced an increase between both years, and this increase is remarkably large and statistically significant in the case of hacking of personal computers, hacking of social media and email, and online fraud. (p. 7)

The overall number of cybercrimes increased during the peak period of lockdown in the UK with only three distinct types of cybercrime decreasing (Buil-Gil et al., 2020). This is shown in Table 1.

Table 1

Cyber-Dependent Crime and Online Fraud Recorded in May 2019 and May 2020

Incident type	Count in May 2019	Count in May 2020	Relative change (%)
Computer virus/malware/spyware	742	648	-12.67*
Denial of Service attack	14	18	28.57
Hacking – Server	24	25	4.17
Hacking – Personal	270	479	77.41***
Hacking – Social media and email	939	1,449	54.31***
Hacking – PBX/Dial Through	9	7	-22.22
Hacking combined with extortion	313	251	-19.81
Online fraud – online shopping and	5,619	8,482	50.95***

Incident type	Count in May 2019	Count in May 2020	Relative change (%)
auctions			
All cybercrimes	7,930	11,359	43.24***

Note. From "Cybercrime and Shifts in Opportunities during COVID-19: A Preliminary Analysis in the UK. European Societies," by D. Buil-Gil, F. Miró-Llinares, A. Moneva, S. Kemp, & N. Díaz-Castaño, 2020, *European Societies*, *23*(S1), p. 8 (https://doi.org/10.1080/14616696.2020.1804973). Copyright 2020 Taylor & Francis.

*** p < .001). **p < .01. *p < .05.

These alarming statistics not only affected global organisations but also people at a personal level, where personal records of those working from home were recorded as having been compromised through illegal remote access. These instances provided new challenges for IS practitioners. Literature proposes that IS practitioners, boards of directors and senior executives must be proactive and understand the nature of IS risks and ensure oversight is prioritized (Katz & McIntosh, 2017). The cost to businesses when there are IS incidents such as breach of personal health information and personally identifiable information is huge, and in many cases, these businesses could potentially be subject to fines or penalties. The rise in IS threats and the types of threats faced by businesses increased and peaked during Covid-19 initiated lockdowns as businesses and people suffered. Because these were unique times and information security was deprioritized, protracted growth in IS attacks and incidents compelled attention (CyberArk, 2019). Research work in the peak periods of lockdowns highlighted a correlation between Covid-19 related events and initiatives with cybersecurity incidents such as phishing, pharming, and financial fraud and extortion as shown by Table 2 (Lallie et al., 2021).

Table 2

Selected Correlations Between Events and Cyber-Criminal Campaigns

Event date	Event	Incident date & type	Incident
21-02-20, 09-03-20	Doctors warn GPs are running out of personal protective equipment, (PPE); Hospitals running out of PPE;	17-04-20 p, ph, f 27-05-20 p, ph, f	Fake PPE offers through email. Link to URLs that capture credit card and other details
11-03-20	Government announces a range of financial assistance packages in the budget	20-03-20 p, ph, f	Smishing campaign promising a COVID-19 financial relief payment. Respondents are directed to a fake gov.uk website which requests credit/debit card details
19-03-20	Government announces a scheme that entitles children who qualify for a free school meal to a food voucher or alternatives if they are not able to continue attending school.	24-03-20 p, ph, f	A smishing campaign which targeted parents with a promise of help with their free school meals in return for banking details. Banking details are defrauded
23-03-20	Lockdown announced. £60 contravention fine, later (10-05-20) increased to £100	27-03-20 p, e	Lockdown contravention SMS
24-03-20	COVID-19 hardship fund enables councils to reduce council tax bills by	15-05-20 p, ph, f	Council tax rebate scam

Event date	Event	Incident date & type	Incident
	£150 for residents of working age and who have had their bill reduced by an award of council tax reduction		
25-03-20	Government announce intention to make home testing kits available	31-03-20 p, f 17-04-20 p, f 27-05-20 p, f	Phishing campaigns in England and Scotland direct victims to fake websites that claim to sell PPE equipment
17-04-20	Government announces job retention scheme	19-04-20 p, f	Fake job retention scheme phishing campaign.

Note. p = phishing; ph = pharming; f = financial fraud; e = extortion. From "Cyber Security in the Age of Covid-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks During the Pandemic," by H. S. Lallie, L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, C. Maple, & X. Bellekens, 2021, *Computers & Security*, *105*, p. 10. (https://doi.org/10.1016/j.cose.2021.102248). Copyright 2021 Elsevier.

While in the pre-Covid-19 era, IS threats seemed to originate from thrill-seekers or government-sponsored spy agents, Table 2 shows that IS threats are evolving following changes in socio-organisational and cultural dynamics. Evolving external attackers are progressively innovative and present unique challenges to IS practitioners.

As long as IS governance continues to be viewed as the domain of the IT staff and IS threats continue to evolve, ordinary people will remain vulnerable (Andre, 2017) and IS attacks will continue unabated. It is critical that organisations re-strategize and prioritise IS governance investment initiatives, by continued monitoring and revising existing security controls and training their skilled personnel to always be prepared to combat innovative threats and IS attacks in particular (CyberArk, 2019).

Undeniably, the evolving nature of IS governance is driven by the ever-increasing, advanced and challenging IS threat landscape catalysed by a majority of people now working from home in the era of Covid-19. Implementing and enforcing the existing IS governance measures has not been effective for many organisations lately, hence the demand for an improved and more robust approach to cybersecurity risks.

Post-Structuralism and Evolution

Structuration theory (ST) brings new intrinsic importance into understanding the post structuralism approach. The central concept in ST is that of human agency which affirms that people's activities matter and that practice needs studying as it influences different outcomes (Whittington, 2010). Most significantly the ST brings together enablement and constraints within the notion of both social structure and agency to not only provide flow continuity but also cater for possible structural changes (Cohen, 1989). Van Assche et al. (2014) acknowledge post-structuralism as a constructivist epistemology and is seen as a critique of structuralism ideals. Post-structuralism holds ideals of post-modernism which posits events from a point of destabilization of hierarchies, systems of knowledge, ideas, meanings, categories, classification, and labels (Chang, 1993). Post-structuralism challenges entrenched ideas of language, subjectivity, and meaning (Moisander et al., 2009). Prominent post-structuralists such as Foucault (2013) have developed substantial literature across different disciplines that can best explain discourse regarding how for instance the evolution of systems and technologies challenges and destabilizes traditional technology usage. Furthermore, this discourse encourages the development of new structures at different levels, which can migrate, gain prominence, and modify contexts. Broadly speaking, governance comprises multiple discourses that also compete and change over time colliding and struggling for primacy, and then recombine and transform (Eugen & Petruţ, 2018; Foucault, 2013; Van

Assche et al., 2014). In our literature review, we identified 5 constructs namely, evolution of technology, the evolution of information security threats, the evolution of routinization, evolution of institutional goals, and evolution of information security governance. We show how we were able to develop each from literature in the section that follows. It should be noted that these constructs have not been tested in previous literature. An instrument was therefore designed from scratch for this purpose. We discuss how this instrument was constructed in the methodology section.

Evolution of Technology

Technology is itself complex and has been undergoing rapid evolution with businesses and notably IS practitioners needing to keep abreast of the next IS threat. From an ST perspective, technology's origin is functionalist and control is a necessary feature that guides how people think and use it. Post-structuralism seeks to reverse this perception by proposing a "think forward" approach to individual's everyday lives (Verbeek, 2010). Technology should be seen as "things–in–use", neutral mediators of the relationships between humans and the world involved in actively co-shaping lives, actions, experience, perceptions, and existence. As a result, what people do is co-shaped by the "things–they–use".

The deployment of the 5th generation mobile network (5G), capable of leveraging IoE by connecting virtually everyone and everything including machines, objects, and devices, has revolutionized communication at unparalleled speeds across cellular networks and private networks respectively. This is expected to present unique challenges to IS practitioners and interesting opportunities to cyber-criminals. Historically, cyber-attacks such as the DDoS, concentrated on the disruption of services and systems to crash the website (Green, 2015) and with the introduction of 5G, these threats are now magnified in unimaginable proportions. Ahmad et al. (2018) systematically outline the evolution of mobile network communication as follows:

> In 1st generation mobile networks (1G), mobile phones and wireless channels were targeted for illegal cloning and masquerading. In 2nd generation mobile networks (2G), message spamming became common for not only pervasive attacks but injecting false information or broadcasting unwanted marketing information. In 3rd generation mobile networks (3G), IP-based communication enabled the migration of Internet security vulnerabilities and challenges in the wireless domains. In 4th generation mobile networks (4G), the size and speed of IP-based communication increased and this enabled the proliferation of smart devices, multimedia traffic, and new services into the mobile domain. (p 36-37)

5G has led to a complicated and dynamic threat landscape, where security threat vectors are anticipated to be much bigger, and the privacy concern heightened. IS threats such as semantic information attacks, timing attacks, and boundary attacks that mainly target the location privacy of users are expected to grow (Ahmad et al., 2018).

Verbeek (2010) suggests that as technology evolves, transformation and changes will occur at the point of human-technology relations and that a system will be created which approaches "human beings not as unique individuals but as fulfillers of functions who are in principle interchangeable" (p 18). From a post-structuralist perspective, technology evolution will help shape what is real, for instance, shaping perception regarding IS threats emanating from 5G evolution and IS governance. By analysing the evolution of technology, insights can be drawn regarding what technology can do and how it can co-shape the human-world relationship. We consider that evolution of technology directly impacts both the evolution of IS threats and IS governance and therefore propose the following two hypotheses:

Hypothesis 1 (**H_1**): Evolution in technology leads to evolution in information security (IS) threats.

Hypothesis 2 (**H_2**): Evolution in technology leads to evolution in routinization.

Evolution of Information Security Threats

While technology has become far more sophisticated over the past decade, so has the nature of IS threats and attacks from cybercriminals. The evolution of IoE and 5G also means potentially more devices are exposed to IS threats. A 2014 global risks report published by the World Economic Forum (2014), reports that IS attacks remain at the top quadrant of business. The report further noted that 79% of IT leaders believed that employees had accidentally put business data at risk with 61% believing that this was done maliciously. By implementing post-structural approaches to evolving IS governance strategies, IS practitioners would move from minimizing IS data breaches to potentially stopping these from happening in the first place. The Economist Intelligence Unit (EIU, 2016) reported that cyber-criminals prioritize personal information as much as organizations do. Banks remain a highly attractive target by having their customers' personally identifiable information and detailed records of their past spending. IS-related attacks targeting banks include fraud related to payment cards, disruption of websites, and network infiltrations to steal money (Kshetri & Kshetri, 2016). Increasingly, phishing emails targeted at individuals with privileged access to sensitive data, corporate banking accounts, and other critical enterprise assets have also emerged (Verizon, 2017). These are new kinds of monetised attacks targeting vulnerabilities that exist within the email authentication mechanisms.

Malware has also evolved to be more sophisticated, targeting specific applications or systems that evade anti-malware and traditional defence mechanisms. Malware threats are similar to those affecting traditional IT networks, and these often compromise access to sensitive data across IoE devices (Sharmeen, et al., 2018). Businesses must therefore evolve from old ways of protection by, for instance, using advanced endpoint malware detection and response tools that use signature-based approaches (Vijayan, 2019).

Another example of evolving IS threats was observed in late 2017 and early 2018, when Google's Project Zero identified a significant hardware vulnerability, namely Meltdown and Spectre, which allow programs to steal data processed by computers (Vijayan, 2019). These vulnerabilities were said to be present on most modern central processing units (CPUs), such as Intel and AMD.

Data theft is now not restricted to the CPU space, and toolkits such as Torii use up to six techniques to target infected connected mobile devices. Any of these techniques could be used as attacks remain persistent. Businesses are now advised to be vigilant of these IS attacks which have evolved and extend beyond malicious software attacks. Vijayan (2019) reported that the primary reason cybercriminals have become persistent is that many of the devices they target contain exploitable vulnerabilities. IS practitioners are expected to adopt new practices to IS governance in light of these threat advancements. As new practices evolve, new sets of policies will be created which can enable proper governance of information resources necessary to mitigate effects from IS attacks (Van Assche et al., 2014). We consider that evolution of IS threats directly impacts IS governance and therefore propose the following hypothesis:

Hypothesis 3 (**H_3**): Evolution in IS threats leads to evolution in institutional goals.

Evolution of Routinization

The evolution of work routines (routinization) by IS practitioners is necessary in light of innovative technologies that have arisen during lockdowns for businesses to be more effective. When routinization is considered from a post-structuralist perspective, the changing of routine is seen as a means to replace

traditional structure and agency by co-shaping routine in many new ways, known as a 'quasi-transcendental approach' (Verbeek, 2010). Giddens (1984, as cited in Whittington, 2010) highlights three forms of routinization, that is communication, the exercise of power, and sanction. Therefore, whenever employees interact (work), they constantly ask questions such as:

- Why did that not happen?
- What made that possible?
- How does that change what is possible in the future?

We postulate that the interaction of agency and of questioning routine work in light of intermittent Covid-19 lockdowns would require businesses to readjust and change their institutional goals and priorities. Since routinization is concerned with the time and space of human interaction, with routine practices stemming from skilled accomplishments of knowledgeable agents, new routines may be bound to happen and these may alter existing social systems and goals since social stability and order are not permanent (Whittington, 2010). We therefore consider that evolution of routinization directly impacts IS governance and propose the following hypothesis:

Hypothesis 4 (**H_4**): Evolution of routinization leads to evolution in institutional goals.

Evolution of Institutional Goals

As humans erect institutions, they also establish norms, reciprocity, and corporation to achieve low costs, stability, and predictability for interaction in society (Duit & Galaz, 2008). In the advent of Covid-19 lockdowns, unexpected changes in businesses and institutions have been observed. These changes have brought uncertainty and those working from home, and businesses, now need to employ flexible goals. Many of these goals need to adopt and be aligned to:

- disruptive IS threat events
- working from home network challenges
- jolts or discontinuities of old methods of work
- performance measures, that affect organisational stability

Establishing new institutional goals is necessary and will require businesses to adapt to certain measures such as changing their value. These include how they view those who work from home, the security measures anchored by control objectives and practices related to information and its security at home, to strengthen and overcome these cyber-risks (Kshetri & Kshetri, 2016). For example, some organisations may consider using secure virtual private networks and make these available to all those working from home.

The Covid-19 pandemic and resulting lockdowns have catalysed business evolution with many businesses such as banking and retail adopting to lockdown regulations faster than others. Many businesses are now critically dependent on the Internet and their IT infrastructure but are still struggling with how to integrate IS goals into their organisation-wide risk management processes. We therefore consider that evolution of institutional goals directly impacts IS governance and propose the following hypothesis:

Hypothesis 5 **(H_5):** Evolution of institutional goals leads to evolution in IS governance.

Evolution of Information Security Governance

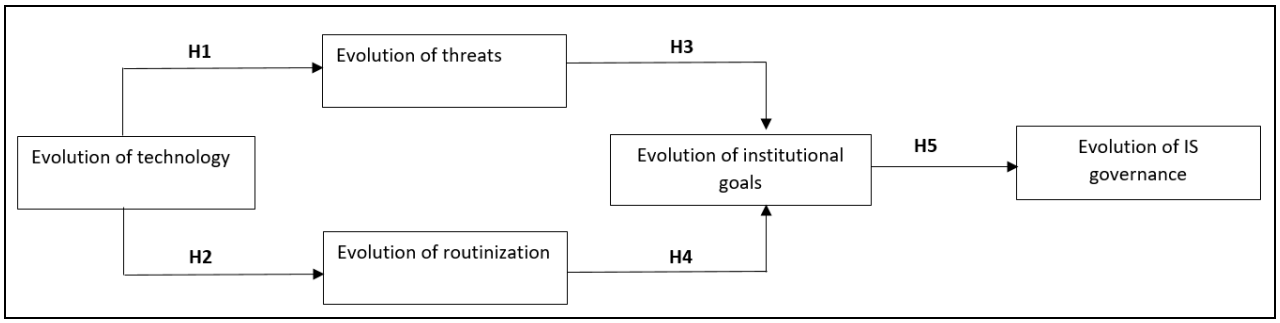
A study by EIU (2016) revealed that over 60% of executives believe that there will be an increase in severe and successful attacks on their businesses. This pessimism is explained by Yahoo having reported to have suffered two significant data breaches between the periods 2013 and 2014, compromising over 1 billion user accounts and over 500 million user accounts respectively (Trautman & Ormerod, 2016). As IS threats continue to grow in sophistication and numbers, so does the need for IS professionals, board members and senior executives to become more involved and proactive in their defence against these attacks. Most boards are however still taking a "head in the sand approach" with the belief that it cannot happen to them (North et al., 2016). Evolutionary IS governance practices call for different theoretical approaches that recognize that IS governance and its elements of IS threats, IS practitioners and businesses are constantly changing and are at interplay with each other. It emphasizes the co-evolution between discourses, actors, and institutions (Ostrom, 2014).

In our earlier discourse, we have proposed that changes in technology, IS threats, routinization, and institutional goals may have a direct impact on IS governance. It is therefore necessary that IS governance involves a unified and coordinated approach at the organizational, regional, and global levels. Organisations experiencing Covid-19 lockdowns must be able to clearly define their IS risk management policies, strategy, and goals, if they are to establish effective IS governance programs. This will require assessing existing IS risk management practices before defining pragmatic strategies and goals. Some elements that are key when developing new and effective IS strategies and goals include understanding how IS risks relate to business operations, determining resource requirements, determining the risk appetite, and developing objectives for continuous monitoring (Swinton & Hedges, 2019).

New and evolved processes must be put in place to enforce requirements or IS governance initiatives will fail. Businesses need to embrace the fact that IS governance is an enterprise concern, and that focus and direction must come from top management. Senior leadership must remain engaged for the entire lifecycle of IS programs to ensure that the entire business understands its commitment to implementing high IS governance standards. Finally, as suggested by Kshetri and Kshetri (2016), IS governance enablers such as technology vendors, private sector organisations, cybersecurity practitioners, and regulators must be drawn together towards coordination, collaboration, and communication to encourage public-private sector interactions in policy-making processes. It is from this discourse that we propose the following model, that integrates our proposed hypotheses, and to test this model to determine whether indeed evolving IS governance can be determined by the mentioned constructs. We present this model in Figure 1. We highlight the methodology adopted to test this model in the section that follows.

Figure 1

Post-Structuralism IS Governance Model



RESEARCH METHODOLOGY

We followed the quantitative research approach to test the five constructs shown in Figure 1 which we elicited from our literature review (Goertzen, 2017). These five contemporize technology and IS threat evolution and innovative trends. The quantitative research approach was preferred in this study because it applies measurable data and is effective in answering quantifiable "what" and "how" type questions (Hjalmarson & Moskal, 2018).

Population Sampling

Our population sample was centred on IT experts and practitioners working in the information technology industry in the city of Johannesburg, South Africa with a minimum of one year of experience. According to data available from Annual Report 2019/20 of the Institute of Information Technology Professionals South Africa (IITPSA, 2020), its membership countrywide stands at 10,875. Of these, 62.1% are based in Gauteng province which consists of the cities of Pretoria and Johannesburg.

We targeted a population of around 250 IITPSA members currently working in companies in the immediate precincts of our research institution in the northern Johannesburg metropole. It was important to incorporate experts possessing special knowledge in the field to obtain useful data (Creswell & Creswell, 2017). Our budget would allow us to reach this number. We computed the sample size using Raosoft Software as a sample size calculator (Raosoft, 2004) based on the following formula:

$$x = Z(c/100)^2 r(100-r) \quad (1)$$

$$n = \frac{N x}{((N-1)E^2 + x)} \quad (2)$$

$$E = \mathrm{Sqrt}\left[\frac{(N-n)x}{n(N-1)}\right] \quad (3)$$

In our case, N was the population size needed to determine our sample, from a margin of error E. We estimated E at 5% margin of error. The fraction of responses we were interested in is r and Z (c/100) is the critical value for the confidence level c. We used a confidence interval of 95% with a population, N of 250. We used a response distribution of 50%. Based on calculations, the recommended sample size was 152. In addition, in order to gauge our model fitness, we applied a ratio of 5 observations to 1 per parameter, using ratio 5:1 proposed by Bentler and Chou (1987) in our determination of sample size for model fitness. According to Bentler and Chou (1987) "the ratio of sample size to number of free parameters may be able to go as low as 5:1 under normal and elliptical theory" (p. 91).

Our model consisted of 19 parameters (see Appendix A) and based on these parameters, we estimated a sample size of 95 (5 x 19) as a minimal acceptable size. It should be noted that some studies have proposed a ratio of 10:1 (Schreiber, et al., 2006), depending on model and parameters. In total we analysed a sample size of 160 which was a size falling within the limits of our calculations. An online survey was the best alternative to use during the Covid-19 pandemic period. Purposive sampling was used as a guide in targeting sampled experts and responses were anonymous and ethical considerations followed to ensure the privacy of participants' data (Bryman, 2016). Data elicitation and analysis was done using online platforms and technologies since at the time of the research, the researchers, as well as respondents, were under Covid-19 instituted lockdown in South Africa.

Instrument Design

We designed a close-ended 5-point Likert scale online questionnaire designed and distributed online via a web link (see Appendix B). The online questionnaire was divided into six main sections. The preliminary first two questions were to filter out vulnerable participants who for ethical purposes must be protected during research. These are participants less than 18 years of age and those older than 65 years of age.

We used literature to guide us in formulating original questions found in the questionnaire. According to Krause (2002) questions may essentially come from three sources. Some questions could be taken directly from existing scales, some from existing scales and modified, and some mostly developed from scratch because these measures may not be found in literature. In our case, we developed questions from scratch. In doing so we used the discourse in post-structuralism and evolution in our literature review to create a list of all facets that emerged and designed questions. This step is called concept analysis (Oosterveld et al., 2019).

We then set an upper limit of between four or five items as a general guideline on the instrument in the scale construction step (Andrews, 1984). Since the goal was to determine existing relationship between evolution of technology and organizational changes, items were designed to reflect this. In the last step of evaluation, we incorporated the assistance of an expert to review these items and the expert provided invaluable input in reshaping these items by proposing revisions. Changes were made to reflect these suggestions. After evaluation, we tested our questionnaire with peers for the instrument to be validated. We statistically analysed datasets using a computerised statistical analysis software called SPSS. Missing data (a few respondents failed to complete their responses) was excluded from the analysis as it made up a small percentage.

Ethical Clearance and Collection of Data

We obtained ethical clearance granted by the university where the study was domiciled before sending the online questionnaire to target participants. A web link was then made available to respondents once consent was obtained. The entering of data on the online questionnaire was automated and self-administered with data populating automatically as each respondent filled-in the questionnaire. The questions inferred temporal order about past, present, and future structural behaviour, experiences, characteristics, and attitudes of IS professionals. Participants were free to stop answering questions and they were under no obligation to complete the questionnaire. However, the importance of the research study was communicated to encourage them to participate, and their anonymity was guaranteed.

DATA ANALYSIS AND RESULTS

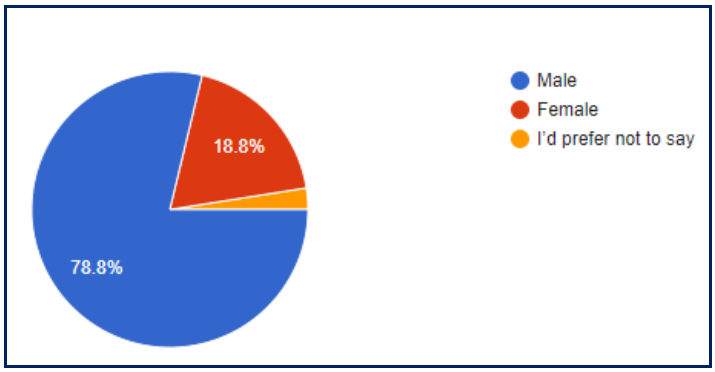
Descriptive Statistics

Section A of the questionnaire sought to collect demographic data of participants such as gender, age, level of education, and details about their organisations. The profiles and demographics of the respondents are presented in the data that follows which addresses the gender, age, level of education, as well as the number of employees in the organisations sampled.

The gender distribution from the sample size of 160 respondents who participated in the survey shows that males contributed 78.8% of the sample while 18.8% were females. This is presented in Figure 2. Of those who responded, 2.4% preferred not to mention their gender. This shows that males still dominate the workforce in South Africa.

Figure 2

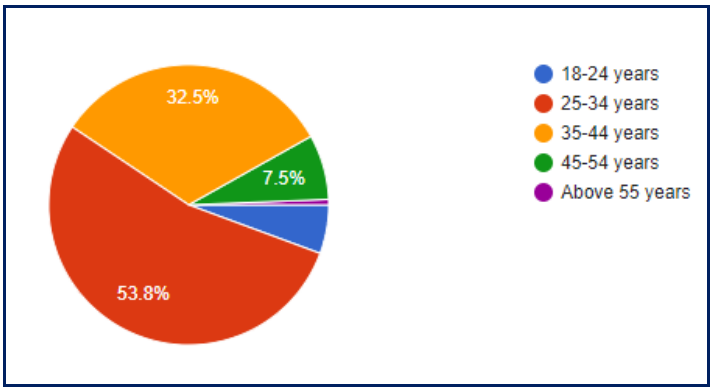
Gender



The majority of participants were between the ages of 25 and 34, representing 53.8% of the respondents, with 32.5% in the age group of between 35 and 44 years as shown by Figure 3. The age distribution is presented as follows: 5.6% of the respondents were between 18 and 24, 7.5% were between 45 and 54 and 0.6% were above the age of 55.

Figure 3

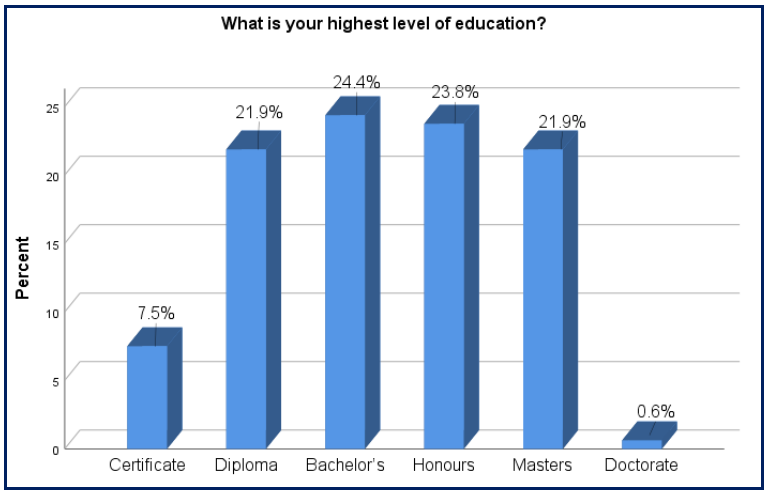
Age



The respondents were asked to indicate their highest level of education and the results are depicted in Figure 4. These results show that the majority of the respondents, 24.4% of the sampled population, had a bachelor's degree. Diploma holders represented 21.9% of the sampled population, those with an honours degree 23.8%, and those with masters level and doctoral qualifications represented 21.9% and 0.6% of the sample size respectively.

Figure 4

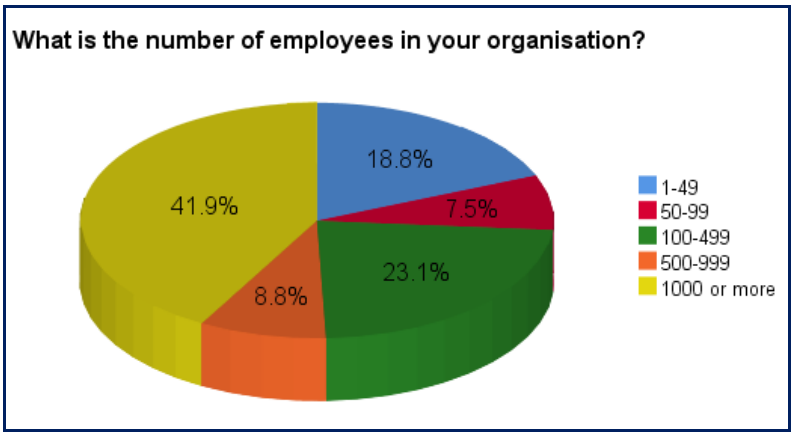
Level of education



Data showing the number of employees within the respondent's organisations are presented in Figure 5. Analysis of Figure 5 shows that the majority of the respondents work in organisations that employ 1 000 or more employees (41.9%), whereas 23.8% of the respondents work in organisations that have between 100 and 499 employees. The remainder of the distribution includes 18.8% of respondents who work for an organisation with 1-49 employees, 500-999 employees (8.8%), and 50-99 employees (7.5%) respectively.

Figure 5

Number of Employees in the Organisation



A cross-tabulation of data was therefore carried out to determine where the majority of respondents were situated concerning positions held in the organisation and the years of experience. The results are displayed in Table 3 below.

Table 3

Cross-Tabulation Between Job Title and Years of Experience in IS Governance

	Years of experience in IS governance						
Current position / role / job title	0-3 years	4-7 years	8-11 years	12-15 years	16-19 years	20 years and above	**Total**
Security Analyst	14	7	9	2	0	0	32
IS Engineer	7	9	4	2	1	0	23
IT Director	1	0	2	1	2	1	7
IT Manager	3	5	1	2	0	0	11
CISO/CSO	0	2	1	1	1	0	5
Systems Administrator	6	1	0	0	0	0	7
Network Engineer	16	3	1	0	0	0	20
IT Auditor	9	4	2	0	0	0	15
Systems Engineer	11	3	1	0	0	0	15
IT Specialist	6	3	1	3	0	1	14
IT Analyst	6	0	0	0	0	0	6
Support Technician	5	0	0	0	0	0	5
Total	84	37	22	11	4	2	160

When comparing the respondent's level of experience with their current job description, the data shows that most of the respondents were network engineers with 0 to 3 years of experience in IS governance. This was followed by security analysts and then systems engineers. Indeed, for most job categories, the majority had less than 3 years' experience suggesting a youthful sample. Cross-tabulation between years of experience and job title not only provides information about the respondents' job descriptions, but also the amount of knowledge the respondents have about IS governance for those roles. This is significant in this research as it ascertains that the data collected is from respondents who are knowledgeable about IS governance and hold different job roles within their organisations.

Reliability Analysis

We carried out a reliability analysis to test our online questionnaire since independent variables were used. This test was necessary since we needed to identify the relationship between the five constructs presented in our literature review. To do this, Cronbach's alpha was used to measure the closeness of and significance of relationships, if any, that these constructs had to each other (Bland & Altman, 1997). For the internal consistency checks, variables not loading onto our component model (principle component analysis, Appendix A) were excluded from the analysis. These included two variables in Section C, question 1 and 2: testing evolution of IS governance and in Section E, question 1 and 2: testing evolution of institutional goals (see Appendix B). The results of the reliability analysis are shown in Table 4 below.

Table 4

Reliability Analysis

Factor item	Cronbach's alpha	*n*
Evolution of technology	0.748	5
Evolution of IS threats	0.769	5
Evolutionary IS governance	0.740	3
Evolution of institutional goals	0.539	2
Evolution of routinization	0.740	4

As a general rule, acceptable levels of reliability must have Cronbach's alpha values between 0.6 and 0.7, whilst a value of 0.8 or higher indicates a very good level (Bland & Altman, 1997). Based on the results, it can be concluded that 4 items had an alpha value greater than 0.6 and can be said to be reliable. Only one item fell slightly below the 0.6 Cronbach's value.

Factor Analysis

As part of data analysis, factor analysis was done on all the constructs. The Kaiser-Meyer-Olkin (KMO) and Bartlett's test of sphericity were also performed. Values reflecting a significant level of less than 0.05 indicated that factor analysis was useful. Table 5 depicts the results from KMO and Bartlett's test of all the variables.

Table 5

KMO and Bartlett's Test

Statistical measures		Evolution of Technology	Evolution of IS threats	Evolution of IS Governance	Evolution of institutional goals	Evolution of routinization
Kaiser-Meyer-Olkin measure of sampling adequacy		.781	.803	.652	.500	.752
Bartlett's test of sphericity	**Approx. X^2**	165.285	185.142	113.575	23.154	139.104
	df	10	10	3	1	6
	p	.000	.000	.000	.000	.000

As the results show, this research obtained a KMO value of more than 0.5 on all variables measured, which indicates that the factor analysis was statistically useful for this research. In addition, Bartlett's test of sphericity is less than 0.05 ($p < .05$), on all variables suggesting that factor analysis was useful.

Regression Analysis

This part of the analysis considered examining and interpreting regression results primarily aimed at testing the proposed model. We were guided by Dhakal (2018) on how to carry out a regression analysis and interpretation. We did this with a caveat that there is no single right way to interpret regression results, but that the interpretation would be objective and based strictly on data. A multiple regression

carried out confirmed our model fitness and that indeed IS governance was dependent on the evolution of institutional goals as shown ($p < .05$) in Table 6 (Dhakal, 2018).

Table 6

Regression Weights

Constructs and relationships			Estimate	*SE*	CR	*p*
Evolution_of_IS_Threats	<---	Evolution_of_Technology	.324	.116	2.781	.005
Evolution_of_Routinization	<---	Evolution_of_Technology	.102	.100	1.027	.305
Evolution_of_Institutional_Goals	<---	Evolution_of_Routinization	.314	.098	3.207	.001
Evolution_of_Institutional_Goals	<---	Evolution_of_IS_Threats	.217	.082	2.644	.008
Evolutionary_IS_Governance	<---	Evolution_of_Institutional_Goals	.349	.074	4.691	***

Note. *CR* = critical ratio.

*** = $p < .001$

Our analysis shows that our proposed model also predicted that evolution in technology would influence evolution in IS threats significantly ($p < .05$). The model however could not predict a significant relationship between evolving technology and routinization ($p > .05$). In other words, peoples' evolving work routines and work habits during the Covid-19 lockdown period were not necessarily influenced by the evolution of technology alone and perhaps other variables could have influenced this. Evolution of routinization could, however, predict the evolution of institutional goals ($p < .05$) and that evolution of IS threats could also predict the evolution of institutional goals ($p < .05$). As depicted in Table 7, we also carried out a standardised regression analysis which provided a more accurate standing of model fitness.

Table 7

Standardized Regression Weights

Constructs and relationships			Estimate
Evolution_of_IS Threats	<---	Evolution_of_Technology	.215
Evolution_of_Routinization	<---	Evolution_of_Technology	.081
Evolution_of_Institutional_Goals	<---	Evolution_of_Routinization	.241
Evolution_of_Institutional_Goals	<---	Evolution_of_IS_threats	.199
Evolutionary_IS_Governance	<---	Evolution_of_Institutional_Goals	.349

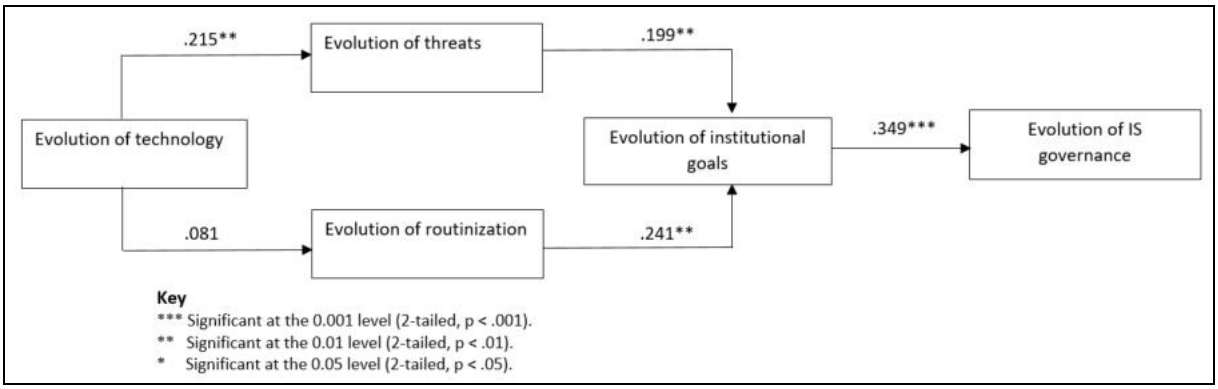
Note. *Group Number 1 - default model*

DISCUSSION

In seeking to contemporize evolving IS governance practices during the Covid-19 lockdown period in South Africa, we used post-structuralism as a theoretical lens and elicited the constructs, evolution of technology, evolution of IS threats, evolution of routinization, and evolution of institutional goals to determine how these influence IS governance. We used multiple regression analysis to determine model fitness and Figure 6 was the outcome of this analysis.

Figure 6

Empirical Model



We observed that the evolution of institutional goals was the strongest predictor of changes in IS governance practices and that these goals were determined by changes in IS threats and routinization. We observed that organisations that use technology are seen as being in a better position to implement effective IS security strategies only if these align with pragmatic goals as well as how people work. Indeed, if people's work routines do not evolve but remain the same, this will drastically influence the nature of goals and ultimately how resources are to be governed. This is indeed an important finding that shows how integrated technology, work practices, and governance practices are all related.

We can therefore predict with a level of certainty that organisations that develop effective IS governance strategies are those that have recognized how work practices have evolved, how technology has evolved, and what measures they should undertake (goals) to align effectively with these changes. IS governance, therefore, demands an organisation-wide approach to protect and eventually enable business success and continuity. It is also essential that institutions position IS governance as an enabler and guarantor of the core business as these strive for business competitiveness in the era of Covid-19 and intermittent lockdowns. Only those organisations that understand the existing IS threat landscape will be able to navigate this treacherous period. As these research findings suggest, the role of human agency and work practices remain core within the contexts of evolution and governance and thus, affirms Giddens' (1984, as cited in Cohen, 1989) structuration theory.

Implications for IS Practitioners

The continued evolution and development of connected technologies across Africa and specifically in South Africa where this study is domiciled, offers unique opportunities for the much-needed leapfrogging of development. It is therefore important to manage these evolving changes at both technological as well as governance and policy levels. Our study offers a compelling need for IS practitioners and professionals to consider persistently revising their existing IS governance approaches in light of such evolution and especially in the wake of the post-Covid-19 pandemic era. This era offers opportunities for new ways of thinking, and new approaches but at the same time consideration of new challenges that include evolving security risks. Many of these new risks and threats have been highlighted in this study.

At first glance, IS technology and governance challenges may seem daunting, but on closer examination, IS practitioners working on the continent can turn this into an advantage. As technology evolution

endures, with noticeable advancements such as 5G and artificial intelligence, African businesses have been lucky not to be encumbered by obsolete technology experienced in more advanced countries. In harnessing this advantage, IS practitioners will need to provide visionary leadership to cherry pick technologies that may help leapfrog the continent into the next level of development. IS practitioners should therefore be more visionary and push for cutting edge technologies that will assist in building new infrastructure tailored specifically for a continent largely endowed with young unemployed and marginalised communities. It will mean learning ways of seeking benefit for these communities from the experience of more developed countries. A call is therefore made for IS practitioners to properly channel technology resources in meaningful ways and design policy response mechanisms towards reskilling labor, realizing that evolving technology may replace traditional forms of human labor and work routines as our work has shown. What matters is the pace of this evolution and if properly managed, African IS practitioners and the broader communities have a fighting chance to adopt to the "new normal". If the evolution is more rapid, not only the businesses and the governance practices they hold, but also the larger communities may be displaced by change and find that they cannot effectively cope or compete. We hope that this work has brought these insights to the fore. It is paramount therefore that all businesses change while being visionary and supportive to the communities these businesses represent. This is an adage that remains true to date.

Contributions to Theory and Knowledge

We offer our framework as instructive and contributing to the body of knowledge by not only presenting an understanding of how evolving information and communication technologies have impacted IS threats, but importantly how governance approaches to IS have and should continue to evolve in equal proportion. When we compare this study with similar work that focuses on information security and governance research on the continent of Africa, Arhin and Wiredu (2018) have presented a deeper understanding on the what, why and how employees react or respond to security-related issues in organizations with emphasis on collaborative analysis. They conclude that without this, response strategies will fail. This study has an internal focus as point of reference to information security issues. Other similar information security studies on the continent with foci on internal information security issues are Ndiege and Okello (2018) on information security awareness as a concern and also Njenga and Jordaan (2016) on neutralisation behaviour by employees as a security concern. Information seeking and gathering has also been flagged as a concern to IS practitioners in studies by Thindwa, Chawinga, and Dube (2019). Finally, Musarurwa, et al., (2018) point to using personal mobile devices in organisational settings as an information security concern.

The findings of our study adds to this understanding by presenting external foci to information security concerns. We show that external shifts such as evolving technology and socio-political changes such as the present day Covid-19 pandemic seem to catalyse evolutions that inform changes in IS governance practices. Indeed, in the pandemic and post-pandemic era, what has been highlighted in this study is the interdependence of many of these external factors (technology evolution, evolutions in work routines, and evolutions in governance) that most of the studies carried out in the continent have not addressed yet. Notably, our study serves as a basis for informed decision making on IS governance matters that should be guided by external matters as well. Our work fills an important void in the literature by particularly focusing on how the Covid-19 pandemic has played a part in catalysing evolving technology and work practices. We feel that these insights are both timely and informative. The results presented can further serve as a benchmark against future work concerned with the governance of information security. As noted, evolving information as well as technology surrogates, such as evolving IS threats, will profoundly impact businesses and society in these uncertain times. Greater knowledge of how IS

threats can be mitigated is of the essence to a society that is currently dependent on IT in the age of information evolution.

Limitations and Recommendations for Future Research

Although the sample taken was from South Africa, we feel this is a good opportunity for future work to replicate this study outside of South Africa and in regions facing similar lockdowns so that comparisons may be made. Furthermore, future research work may consider examining similar studies in countries with less developed economies, where information and technology evolution is yet to make significant inroads.

CONCLUSION

The work was carried out during the peak of the Covid-19 pandemic which began in March 2020. It was grounded on how information and threats to information are evolving, and this evolution was catalysed by heavy use of information technology (IT) in businesses during Covid-19 lockdown. We drew on this conundrum of evolution and modelled constructs drawn from interdisciplinary theories and tested our model for fitness. Our findings suggest that IS governance is significantly related to changes in institutional goals and that these goals are a result of changing IS threats. We established that when work routines (routinization) and institutional goals changed and evolved at a much slower rate, as a result of out-of-date governance practices, businesses were bound to be adversely impacted. These findings are central to organizational work practices and in seeking to be more competitive during lockdowns, it is recommended that these practices would have to change. This was the key contribution this work has hopefully highlighted.

REFERENCES

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2018). Overview of 5G security challenges and solutions. *IEEE Communications Standards, 2*(1), 36–43. https://doi.org/10.1109/MCOMSTD.2018.1700063

Andre, T. (2017). Cybersecurity an enterprise risk issue. *Healthcare Financial Management, 71*(2), 40–46.

Andrews, F. M. (1984). Construct validity and error components of survey measures: A structural modeling approach. *Public Opinion Quarterly, 48*(2), 409–442. https://doi.org/10.1086/268840

Arhin, K., & Wiredu, G. O. (2018). An organizational communication approach to information security. *The African Journal of Information Systems, 10*(4), 261–279.

Bandyopadhyay, T., Meso, P., & Negash, S. (2018). Mobile IT in health–the case of short messaging service in an HIV awareness program. *Information Technology for Development, 24*(2), 359–397. https://doi.org/10.1080/02681102.2017.1363029

Bentler, P. M., & Chou, C.-P. (1987). Practical issues in structural modeling. *Sociological Methods & Research, 16*(1), 78–117. https://doi.org/10.1177/0049124187016001004

Bland, J. M., & Altman, D. G. (1997). Statistics notes: Cronbach's alpha. *BMJ, 314*, 572.

Bryman, A. (2016). *Social research methods.* Oxford University Press. https://doi.org/10.1136/bmj.314.7080.572

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies, 23*(S1), S47–S59. https://doi.org/10.1080/14616696.2020.1804973

Butler, R., & Butler, M. (2018). Some password users are more equal than others: Towards customisation of online security initiatives. *South African Journal of Information Management, 20*(1), 1–10. https://doi.org/10.4102/sajim.v20i1.920

Chang, R. S. (1993). Toward an Asian American legal scholarship: Critical race theory, post-structuralism, and narrative space. *California Law Review, 81*(5), 1241+1243–1323. https://doi.org/10.2307/3480919

Cohen, I. J. (1989). Structuration theory: Anthony Giddens and the constitution of social life. Macmillan International Higher Education.

Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches. Sage Publications.

CyberArk. (2019). *CyberArk global advanced threat landscape 2019 report*. https://www.cyberark.com/resource/global-advanced-threat-landscape-2019/#download-resource

Dahunsi, F. (2017). Conceptual framework of community based location specific services for improved service delivery. *The African Journal of Information Systems, 9*(1), 62–76.

Dhakal, C. (2018). Interpreting the basic outputs (SPSS) of multiple linear regression. *International Journal of Science and Research (IJSR), 8*(6), 1448–1452.

Duit, A., & Galaz, V. (2008). Governance and complexity—emerging issues for governance theory. *Governance, 21*(3), 311–335. https://doi.org/10.1111/j.1468-0491.2008.00402.x

Ebert, C., Gallardo, G., Hernantes, J., & Serrano, N. (2016). DevOps. *IEEE Software*, *33*(3), 94–100. https://doi.org/10.1109/MS.2016.68

Eugen, P., & Petruţ, D. (2018). Exploring the new era of cybersecurity governance. *Ovidius University Annals, Economic Sciences Series*, *18*(1), 358–363.

First Distribution. (2019, June 5). Whitepaper: Go phish-How to prevent your business from becoming another cyber security statistic. *ITWeb*. https://www.itweb.co.za/content/rW1xLv55a95vRk6m

Foucault, M. (2013). *Archaeology of knowledge*: Routledge. https://doi.org/10.4324/9780203604168

Garzia, F., & Papi, L. (2016). An Internet of Everything based integrated security system for smart archaeological areas. In W. R. Claycomb (Ed.), *2016 IEEE international Carnahan conference on security technology (ICCST) proceedings* (pp. 56–63). Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/CCST.2016.7815684

Goertzen, M. J. (2017). Introduction to quantitative research and data. *Library Technology Reports, 53*(4), 12–18.

Green, J. (2015). Staying ahead of cyber-attacks. *Network Security*, *2015*(2), 13–16. https://doi.org/10.1016/S1353-4858(15)30007-6

Hjalmarson, M. A., & Moskal, B. (2018). Quality considerations in education research: Expanding our understanding of quantitative evidence and arguments. *Journal of Engineering Education, 107*(2), 179–185. https://doi.org/10.1002/jee.20202

Institute of Information Technology Professionals South Africa. (2020). *Annual report 2019/20*. https://www.iitpsa.org.za/wp-content/uploads/2020/08/IITPSA-Annual-Report-2019-20.pdf

International Organisation for Standardization. (2020). *ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection — Governance of information security* [Standard]. https://www.iso.org/standard/74046.html

Johnston, K. A., Loot, M., & Esterhuyse, M. P. (2016). The business value of cloud computing in South Africa. *The African Journal of Information Systems, 8*(2), 1-20.

Kaspersky. (n.d.). *What is cyber security?* https://www.kaspersky.co.za/resource-center/definitions/what-is-cyber-security

Katz, D. A., & McIntosh, L. A. (2017, August 17). Cybersecurity board basics: prep, watch, react & report. *Directors and Boards*. https://www.directorsandboards.com/articles/singlecybersecurity-board-basics-prep-watch-react-report

Krause, N. (2002). A comprehensive strategy for developing closed-ended survey items for use in studies of older adults. *The Journals of Gerontology: Series B, 57*(5), S263–S274. https://doi.org/10.1093/geronb/57.5.S263

Kshetri, N., & Kshetri, D. N. (2016). *Quest to cyber superiority*: Springer. https://doi.org/10.1007/978-3-319-40554-4

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of Covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*. *105*, Article 102248, 1–20. https://doi.org/10.1016/j.cose.2021.102248

Macueve, G. (2008). e-Government for development: A case study from Mozambique. *The African Journal of Information Systems, 1*(1), 1–17. https://doi.org/10.1504/IJEG.2008.022067

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

Moisander, J., Valtonen, A., & Hirsto, H. (2009). Personal interviews in cultural consumer research–post-structuralist challenges. *Consumption, Markets and Culture, 12*(4), 329–348. https://doi.org/10.1080/10253860903204519

Musarurwa, A., Flowerday, S., & Cilliers, L. (2018). An information security behavioural model for the bring-your-own-device trend. *South African Journal of Information Management, 20*(1), 1–9. https://doi.org/10.4102/sajim.v20i1.980

Ndiege, J. R., & Okello, G. (2018). Information security awareness amongst students joining higher academic institutions in developing countries: Evidence from Kenya. *The African Journal of Information Systems, 10*(3), 204–221.

Njenga, K., & Jordaan, P. (2016). We want to do it our way: The neutralisation approach to managing information systems security by small businesses. *The African Journal of Information Systems, 8*(1), 42–63.

North, J., Pascoe, R., & Westgarth, C. C. (2016). Cyber security and resilience — it's all about governance. *Governance Directions*, (3), 146–151.

Ntsaluba, N. (2018). *The cyber security legislative and policy framework in South Africa* [Mini dissertation, University of Pretoria]. UPSpace. http://hdl.handle.net/2263/65706

Nyoni, P., Velempini, M., & Mavetera, N. (2020). Emerging internet technologies and the regulation of user privacy. *The African Journal of Information Systems, 13*(1), 1–32.

Oosterveld, P., Vorst, H. C., & Smits, N. (2019). Methods for questionnaire design: A taxonomy linking procedures to test goals. *Quality of Life Research, 28*(9), 2501–2512. https://doi.org/10.1007/s11136-019-02209-6

Oosterwyk, G. W., & Kabiawu, O. (2016). The nature of mobile bullying & victimisation in the Western Cape high schools of South Africa. *The African Journal of Information Systems, 8*(2), 45–69.

Ostrom, E. (2014). Do institutions for collective action evolve? *Journal of Bioeconomics, 16*(1), 3–30. https://doi.org/10.1007/s10818-013-9154-8

Paton, C. (2019, October 25). City of Joburg, banks under cyber attack. *BusinessDay*. https://www.businesslive.co.za/bd/national/2019-10-25-city-of-joburg-banks-under-cyber-attack/

Rananga, N., & Venter, H. (2020). Mobile Cloud Computing Adoption Model as a Feasible Response to Countries' Lockdown as a Result of the COVID-19 Outbreak and Beyond. 2*020 IEEE conference on e-learning, e-management and e-services (IC3e)*, 61–66. IEEE. https://doi.org/10.1109/IC3e50159.2020.9288402

Raosoft. (2004). *Sample size calculator*. http://www.raosoft.com/samplesize.html

Sagiroglu, S., & Sinanc, D. (2013). Big data: A review. *2013 International conference on collaboration technologies and systems (CTS)*, 42 – 47. IEEE. https://doi.org/10.1109/CTS.2013.6567202

Schreiber, J. B., Nora, A., Stage, F. K., Barlow, E. A., & King, J. (2006). Reporting structural equation modeling and confirmatory factor analysis results: A review. *The Journal of Educational Research, 99*(6), 323–338. https://doi.org/10.3200/JOER.99.6.323–338

Sergey, M., Nikolay, S., & Sergey, E. (2017). Cyber security concept for Internet of Everything (IoE). *2017 Systems of signal synchronization, generating and processing in telecommunications (SINKHROINFO)* (pp. 1–4). Institute of Electronics Engineers. https://doi.org/10.1109/SINKHROINFO.2017.7997540

Sharmeen, S., Huda, S., Abawajy, J. H., Ismail, W. N., & Hassan, M. M. (2018). Malware threats and detection for industrial mobile-IoT networks. *IEEE Access, 6*, 15941–15957. https://doi.org/10.1109/ACCESS.2018.2815660

Snyder, T., & Byrd, G. (2017). The Internet of Everything. *Computer, 50*(6), 8-9. https://doi.org/10.1109/MC.2017.179

Sorsa, A., Jerene, D., Negash, S., & Habtamu, A. (2020). Use of Xpert contributes to accurate diagnosis, timely initiation, and rational use of anti-TB treatment among childhood tuberculosis cases in south central Ethiopia. *Pediatric Health, Medicine and Therapeutics, 11*, 153–160. https://doi.org/10.2147/PHMT.S244154

Stergiou, C., Psannis, K. E., Kim, B.-G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems, 78*(3), 964–975. https://doi.org/10.1016/j.future.2016.11.031

Swinton, S., & Hedges, S. (2019, July 25). Cybersecurity governance, part 1: 5 fundamental challenges. *SEI Blog*. https://insights.sei.cmu.edu/insider-threat/2019/07/cybersecurity-governance-part-1-5-fundamental-challenges.html

Sylvan, D. (2014). Global internet governance: Governance without governors. Springer. https://doi.org/10.1007/978-3-642-45299-4_2

The Economist Intelligence Unit. (2016, March 22). Protecting the brand: Cyber-attacks and the reputation of the enterprise. *VMware*. https://www.vmware.com/radius/cyber-attacks-and-the-reputation-of-the-enterprise/

Thindwa, T., Chawinga, W. D., & Dube, G. (2019). Information-seeking behaviour of security studies students: A case study. *South African Journal of Information Management, 21*(1), 1–10. https://doi.org/10.4102/sajim.v21i1.1048

Trautman, L. J., & Ormerod, P. C. (2016). Corporate directors' and officers' cybersecurity standard of care: The Yahoo data breach. *American University Law Review, 66*, 1231–1291. https://doi.org/10.2139/ssrn.2883607

Van Assche, K., Beunen, R., & Duineveld, M. (2014). Evolutional governance theory: Theory and applications. In K. Van Assche, R. Beunen, & M. Duineveld (Eds.), *Evolutional governance theory: An introduction*, 1–95. Springer. https://doi.org/10.1007/978-3-319-00984-1

Verbeek, P.-P. (2010). What things do: Philosophical reflections on technology, agency, and design. Penn State Press.

Verizon. (2017). *Data breach digest: Perspective is reality* [Data breach scenarios]. https://enterprise.verizon.com/resources/reports/data-breach-digest-2017-perspective-is-reality.pdf

Vijayan, J. (2019). 5 emerging cyber threats to watch for in 2019. *Tech Digest.* https://twimgs.com/custom_content/DR19_Tech_Digest_February-1.pdf

Whittington, R. (2010). Giddens, structuration theory and strategy as practice. In D. Golsorkhi, L. Rouleau, D. Seidl, & E. Vaara (Eds.), *Cambridge handbook of strategy as practice*. 109–126. Cambridge University Press. https://doi.org/10.1017/CBO9780511777882.008

World Economic Forum. (2014). *Global risks 2014*. http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

Appendix A

Rotated Component Matrix

Constructs rotated	Component				
	1	2	3	4	5
Evolution_of_Threats_4	0.788				
Evolution_of_Threats_2	0.706				
Evolution_of_Threats_1	0.681				
Evolution_of_Threats_3	0.672				
Evolution_of_Threats_5	0.619				
Evolution_of_Technology_A3		0.783			
Evolution_of_Technology_A1		0.705			
Evolution_of_Technology_A2		0.699			
Evolution_of_Technology_A4		0.689			
Evolution_of_Technology_A5		0.562			
Evolution_of Routinization C4			0.791		
Evolution_of Routinization C2			0.758		
Evolution_of Routinization C3			0.721		
Evolution_of Routinization C1			0.511		
Evolution_of_IS Governance_B5				0.817	
Evolution_of_IS Governance_B4				0.764	
Evolution_of_IS Governance_B3				0.746	
Evolution_of_Institu_Goals_4					0.772
Evolution_of_Institu_Goals_3					0.634

Note. Rotation converged in 6 iterations. Extraction method: principal component analysis. Rotation method: Varimax with Kaiser normalization

Appendix B

Information Security Governance Questionnaire

Dear participant,

My name is ** *[deleted to keep authors anonymous*]. You have been invited to participate in this research study that [ ]…You have been identified as an expert in information security or otherwise having been involved in information security-related aspects of your organisation.

Should you choose to participate, you will be requested to provide your insights on several aspects relating to information security governance. This questionnaire should not take up more than fifteen minutes of your time. Participation is completely voluntary and there is no personal obligation on yourself to complete the questionnaire. You may also choose to withdraw at any time should you feel uncomfortable answering any of the questions.

Please note that your participation may benefit the discipline of information security governance by providing insights into current policies and practices and how they can be improved in light of the evolutionary nature of various elements that affect them.

This questionnaire does not solicit information that can be used to identify a particular individual and measures will be taken to keep the information secure and encrypted. The information will ONLY be used for academic work and may help the scholarly community when results are presented in outlets such as journals, books, chapters, or conference proceedings. If you have any concerns or questions related to the study in general or the items in the questionnaire, please contact the project leader [*deleted to keep authors anonymous*].

Thank you for taking the time to participate in this study.

We are working on a project the concerns information security governance. If you are older than 18 and below 65 and prefer to use English as your primary mode of communication, you are invited to participate in this study.

I hereby consent to my responses being used as outlined above.

Note: When you answer NO to the below question, you do not have to take part in the survey.

Yes	
No	

Are you over 18 and under 65 years of age? *

Note: When you answer NO to the below question, you do not have to take part in the survey.

Yes	
No	

SECTION A: PARTICIPANT'S DEMOGRAPHICS

This section of the questionnaire is aimed at getting participants' demographics.

A1. Gender

Male	
Female	
I'd prefer not to say	

A2. Age

18-24 years	
25-34 years	
35-44 years	
45-54 ears	
Above 55 years	

A3. What is your highest level of education?

Certificate	
Diploma	
Bachelors	
Honours	
Masters	
Doctorate	

A4. What is the number of employees in your organisation?

1-49	
50-99	
100-499	
500-999	
1000 or more	

A5. What is your current position/role/job title?

Security Analyst	
Cybersecurity Engineer	
IT Director	
IT Manager	
CISO/CSO	
Systems Administrator	
Network Engineer	
Forensic Investigator	
IT Auditor	
Systems Engineer	
IT Specialist	
IT Analyst	
Support Technician	
Other (please specify)	

A6. For how many years has the organisation been in business?

0-5 Years	
6-10 Years	
11-15 Years	
16-20 Years	
21 Years and Above	

A7. How many years of experience do you have in information security governance?

0-3 Years	
4-7 Years	
8-11 Years	
12-15 Years	
16-19 Years	
20 Years and Above	

SECTION B: EVOLUTION OF TECHNOLOGY

This section is aimed at assisting us to understand your perception regarding how technology has evolved.

B1. Using the following scale, please indicate your level of agreement about how IT-based technology has affected information security governance in your organisation.

Evolution of Technology		**Strongly agree 1**	**Agree 2**	**Neutral 3**	**Disagree 4**	**Strongly Disagree 5**
1.	IT-based technology has evolved over the years.					
2.	Ideas and lessons to integrate IT-based technology have evolved over the years.					
3.	IT-based security solutions have evolved over the years.					
4.	Information security and Cybersecurity tools and technologies have evolved over the years.					
5.	Cloud computing and the Internet of Things has evolved over the years.					

SECTION C: EVOLUTION OF INFORMATION SECURITY GOVERNANCE

This section is aimed at assisting us to understand your perception regarding the evolving changes and governance of information in your organisation over time.

C1. Using the following scale, please indicate your level of agreement about how information security governance has evolved.

Evolution of IS Governance *excluded in analysis (See Appendix A)		**Strongly agree 1**	**Agree 2**	**Neutral 3**	**Disagree 4**	**Strongly Disagree 5**
*1.	Growth in automation technology has provided reliable information security governance.					
*2.	Artificial intelligent growth has leveraged information security governance.					
3.	Growth in scalable security dashboards has enhanced the value of information security governance.					
4.	Growth in Cloud-based solutions has made IS governance effective.					

5.	Growth in investments in automation technologies has created successful IS governance practices.					

SECTION D: EVOLUTION OF INFORMATION SECURITY THREATS

This section is aimed at assisting us to understand your perception regarding information security threats and how these have changed and evolved.

D1. Using the following scale, please indicate your level of agreement about how information security threats have evolved and how these have affected governance.

Evolution of Cybersecurity Threats		**Strongly agree 1**	**Agree 2**	**Neutral 3**	**Disagree 4**	**Strongly Disagree 5**
1.	Data security and privacy have changes to become progressively risky.					
2.	Data security warnings are not as effective due to advanced and evolving information security threats.					
3.	Information security threats now target explicit segments of a system framework.					
4.	Information security threats now exceed the capabilities of the current security workforce and administration.					
5.	The information security administration work force is now faced with an expanded number of assaults.					

SECTION E: EVOLUTION OF INSTITUTIONAL GOALS

This section is aimed at assisting us to understand your perception regarding how your organisational goals have changed about the changes in technology as well as information security threats.

E1. Using the following scale, please indicate your level of agreement about how institutional goals have changed.

Evolution of Institutional goals *excluded in analysis (See Appendix A)		**Strongly agree 1**	**Agree 2**	**Neutral 3**	**Disagree 4**	**Strongly Disagree 5**
*1.	My organisation has changed our risk management component and information security administration programme, in accordance with changing technology.					
*2.	My organisation has changed our information security control procedures that outline new dangers related to changing technologies.					

3.	My organisation compels us to regularly update our information security policies.					
4.	My organisation's information security goals have changed since we started working from home.					

SECTION F: EVOLUTION OF ROUTINIZATION

This section is aimed at assisting us to understand your perception regarding how your work routine has changed because of technology and importantly working from home.

F1. Using the following scale, please indicate your level of agreement about how your work routine has changed because of technology and working from home.

Evolution of Routinization		**Strongly agree 1**	**Agree 2**	**Neutral 3**	**Disagree 4**	**Strongly Disagree 5**
1.	My work routine has changed and I no longer have a regularised way of carrying out my duties.					
2.	Procedures concentrating on access control to work stations no longer apply.					
3.	I no longer have adequate information on guidelines that drive work practices.					
4.	I no longer work the way I used to when I first joined my organisation and this is because of the technology I now find myself using.					