Received 21 September 2021
Revised 19 April 2022
23 July 2022
Accepted 12 October 2022

A service lens on cybersecurity continuity and management for organizations' subsistence and growth

Godwin Thomas
Department of Computer Science, University of Jos, Jos, Nigeria, and
Mary-Jane Sule
Abdus Salam International Centre for Theoretical Physics, Trieste, Italy

Abstract

Purpose – This paper proposes a holistic, proactive and adaptive approach to cybersecurity from a service lens, given the continuously evolving cyber-attack techniques, threat and vulnerability landscape that often overshadow existing cybersecurity approaches.

Design/methodology/approach – Through an extensive literature review of relevant concepts and analysis of existing cybersecurity frameworks, standards and best practices, a logical argument is made to produce a dynamic end-to-end cybersecurity service system model.

Findings – Cyberspace has provided great value for businesses and individuals. The COVID-19 pandemic has significantly motivated the move to cyberspace by organizations. However, the extension to cyberspace comes with additional risks as traditional protection techniques are insufficient and isolated, generally focused on an organization's perimeter with little attention to what is out there. More so, cyberattacks continue to grow in complexity creating overwhelming consequences. Existing cybersecurity approaches and best practices are limited in scope, and implementation strategies, differing in strength and focus, at different levels of granularity. Nevertheless, the need for a proactive, adaptive and responsive cybersecurity solution is recognized.

Originality/value – This paper presents a model that promises proactive, adaptive and responsive end-to-end cybersecurity. The proposed cybersecurity continuity and management model premised on a service system, leveraging on lessons learned from existing solutions, takes a holistic analytical view of service activities from source (service provider) to destination (Customer) to ensure end-to-end security, whether internally (within an organization) or externally.

Keywords Cybersecurity, Information security management, Service system, Standards, Frameworks, Risk, Threats, Vulnerabilities, Countermeasures, Capabilities, Resources, Processes

Paper type Research paper

1. Introduction

The advent of the Internet or cyberspace has had a positive impact on the way organizations and businesses perform their functions and services. Platforms for e-commerce, banking and government among others exist to ensure greater reach, engage with and provide services for customers and citizens alike (Kitsing, 2017; Pawar and Palivela, 2022). More so, because of the Internet's reach, individuals continue to take advantage as entrepreneurs to reach customers that cut across international boundaries, thus contributing to a nation's economy and poverty mitigation. For instance, the network marketing industry continues to leverage Internet technology for its reach and services (Jones *et al.*, 2013; Dwivedi *et al.*, 2021).

Organizational Cybersecurity Journal: Practice, Process and People
Vol. 3 No. 1, 2023
pp. 18-40
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-09-2021-0025

While the Internet and the corresponding information and communication technology (ICT) tools continue to provide great value for different entities, they are not without risks (Jang-Jaccard and Nepal, 2014; Fonseca-Herrera *et al.*, 2021). The activities of cybercriminals continue to threaten this new way of life, limiting the trust levels in Internet-driven services. Cybercriminals take advantage of the available tools on the darknet, users' lack of knowledge/awareness and the anonymity the Internet platform offers to run cyberattacks whether through hacking or social engineering among others (Kobielus, 2020; Pawar and Palivela, 2022). More so, the current COVID-19 pandemic has made the world more reliant on the Internet and the digital economy. Cyberspace continues to see increasing and evolving threats and vulnerabilities associated with the continuous adoption and evolving nature of cyberspace.

According to the 2020 global risks report by the World Economic Forum, cyberattacks on critical infrastructure are rated the fifth top risk in 2020 which continues to prevail across the energy, healthcare and transportation industries among others (Cremer *et al.*, 2022). The report maintains that cybercrime-as-a-service is a growing business model, especially with the increase of sophisticated tools on the darknet that is making malicious services affordable and more easily accessible to anyone. More so, organized cybercrime entities continue to evade detection and prosecution where the likelihood of this happening in the USA, for instance, only stands at an estimated low of 0.05%. The impact of insufficient cybersecurity has been estimated to have cost US$ 945 bn to the global economy in 2020 increasing to about $6 tn in cybercrime damages worldwide in 2021 (Cremer *et al.*, 2022; Pitchkites, 2022). The prediction is that the cost of cybercrime will hit $10.5 tn by 2025 (Kerner, 2022). As such, taking proactive measures, subscribing to security standards/frameworks and meeting regulatory compliance become a most for an organization to address cybersecurity challenges and increase/improve digital trust levels geared to protect businesses, institutions and individuals alike; thus, governments, organizations and businesses continue to invest in ways to ensure cyberattacks are mitigated.

Cybersecurity represents a way for individuals and organizations to protect their Internet-connected systems, such as computer networks, hardware, software and data from cyber threats (Rouse, 2020; Perwej *et al.*, 2021), thus protecting against unauthorized access to their data centers or other electronic systems. As a subset of information security, cybersecurity efforts aim to protect against malicious attacks or intent that extort an organization or user-sensitive data (Jang-Jaccard and Nepal, 2014; Pawar and Palivela, 2022).

However, this is easier said than done as mitigating cybersecurity risks can be a challenging task. According to Taylor (2021), even the best cyber defense application cannot provide total cyber protection as nearly all systems deemed secured can be vulnerable to some type of cyberattack. More so, cybersecurity is a continuously evolving field, with the development and advancement of technologies that come with novel avenues for cyberattacks (Rouse, 2020; Perwej *et al.*, 2021). Networks are becoming more extended, complex and challenging to monitor. This is especially true for organizations that have moved to remote working and as such have less control over workers' behavior and device security (De Smet and Mysore, 2020).

According to Cremer *et al.* (2022) and Dixon and Singh (2020), the risk of cyber-attacks continues to rise; more so now as the COVID-19 pandemic continues to disrupt global health, economic, political and social systems, the uncertainty of the crisis forces organizations and individuals to embrace new practices such as social distancing, hand washing/sanitizing and remote working and increased reliance on digital tools. Sadly, cybercriminals continue to capitalize on the increasing dependence on digital tools resulting in a rise in cybersecurity risks (Lallie *et al.*, 2020; Weil and Murugesan, 2020).

Deloitte (2020) reports an observed increase in phishing attacks, malicious spam and ransomware attacks as cybercriminals have continued to use COVID-19 as a lure to impersonate known brands, thereby cheating employees and their customers. Given the level of unpreparedness of remote work deployment by organizations and businesses as a result of

the pandemic, new vulnerabilities have been introduced, and cybercriminals around the world undoubtedly are exploiting them (Lallie *et al.*, 2020; Perwej *et al.*, 2021). Unfortunately, the traditional perimeter security approach often employed by organizations to protect and defend crucial system components against known threats remains insufficient. Despite the sophisticated firewalls and antivirus systems installed by organizations, new vulnerabilities come to the fore, and the threat landscape continues to evolve more rapidly than organizations can keep up with.

As the volume and complexity of cyberattacks grow, it is imperative that businesses and organizations, especially those tasked with the duty of protecting information related to health, national security and financial records among others, take a proactive and holistic approach to cybersecurity in order to safeguard sensitive corporate and personnel information. Standards and best practice organizations continue to encourage more proactive, adaptive, applied and data-focused approaches to cybersecurity (NIST CSF, 2014).

However, existing standards and frameworks do not present a one size fits all approach to cybersecurity management as organizations continue to have unique risks with different threats, vulnerabilities and risk tolerance levels (Gordon *et al.*, 2020; Pawar and Palivela, 2022; Al Faruq *et al.*, 2020). As such, they have varying customized practices based on different frameworks with activities that are deemed important for their service delivery. While existing frameworks provide an overview of how cybersecurity risk management should be approached at a macrolevel, they leave the implementation details to the individual organizations at the microlevel (Fonseca-Herrera *et al.*, 2021; Ibrahim *et al.*, 2018). Existing research and practice have been mostly focused on protecting immediate business environment exploring how standards, best practices and frameworks can be best implemented or integrated to improve an organization's credibility and standing. Thus, this only supports the strategic move by organizations to instill confidence to their stakeholders that risks are adequately managed by getting certified, which is far from realizing absolute security.

Research to aid organizations realize absolute end-to-end security that takes cognizance of the both the service provider environment and the customers is practically nonexistent. There is very little concern about a broader business environment that considers the customers and their environment which can introduce dire threats and vulnerabilities that can be exploited. Since cybersecurity risk management revolves around correctly assessing risk environment, which is not an easy task (Sheehan *et al.*, 2021; Hitchcox, 2020), this paper advocates taking a holistic view of service activities from its source (service provider) to destination (customer) to better fulfill cybersecurity requirements. Thus, what is needed is a holistic analytical approach that takes cognizance of existing frameworks, guidelines and organizations' unique contexts to find their best cybersecurity footing.

This paper argues that by taking a service lens and leveraging on the strengths of existing best practices and standards, a holistic approach to cybersecurity continuity and management can be realized. The following section will highlight more on the challenges associated with cybersecurity, whereafter the paper dwells on the existing approaches employed towards a solution. Next, it delves into the core of the service system frameworks, the Information Technology Infrastructure Library (ITIL), Information Security Management System (ISMS) and the National Institute of Standards and Technology (NIST) security frameworks taking cognizance of their strengths, focus and limitations. Consequently, a conceptual cybersecurity continuity and management model is presented, followed by a discussion on its merits, a conclusion and future work.

2. The cyberspace security issues and challenges

As mentioned in the previous section, cyberspace provides opportunities for organizations, businesses and government agencies to extend their reach and improve their productivity

and service provision even amidst an existential crisis like the COVID-19 pandemic. However, the opportunities presented by cyberspace are not without risks. Cybersecurity continues to remain a challenging task as the threat and vulnerability landscape continues to evolve (Lallie *et al.*, 2020; Weil and Murugesan, 2020; Perwej *et al.*, 2021). Since unauthorized access or exposure to sensitive data can result in negative consequences, organizations continue to look for ways to mitigate threats and effectively respond to security incidents, especially now that digital adoption has become widespread with remote working and increased reliance on IT-driven services. Additionally, customers continue to demand better security services as the ongoing environmental crisis (COVID-19) has introduced more threats and vulnerabilities to individuals and organizations alike (Cremer *et al.*, 2022) As businesses and individuals continue to take advantage of digital technologies and cloud services to emerge ahead of the crisis, the risk and impact of cyberattacks have continued to rise (Weil and Murugesan, 2020; Dalal *et al.*, 2022).

Cyberspace continues to be troubled with highly motivated offenders who take advantage of inadequate security, the lack of security awareness and noncompliance to regulation among others. More so, the rapidly evolving technology landscape comes with new threats and vulnerabilities. For instance, the Internet of Things (IoT) landscape amplifies the potential for cyberattacks. According to the global risk report, attacks on IoT devices have increased by more than 300% in the first half of 2019 and in one instance, taking down Wikipedia through the classic distributed denial of service (DDoS) attack (WEF, 2020). It is expected that such IoT-driven attacks will increase given that there are already over 21 billion active IoT devices in existence, and the number is expected to double by 2025. Thus, cybersecurity continues to remain a big challenge and the scale of the global cyber threat continues to evolve rapidly. The RBS (2019) report revealed that 7.9 billion records were exposed by data breaches in the first nine months of 2019 doubling the number of records in 2018. The report showed that the medical, retailers and public domains experienced the most breaches.

More so, proceeds from cybercrime activities globally were up to $1.5 tn in 2018 (Ismail, 2018), with Juniper Research (Morrow and Crabtree, 2019) estimating cybercrime costs in association with data breaches to soar to over $5 tn in 2024 rising from $3 tn each year (Kerner, 2022). Regulations on data breaches continue to tighten as sensitive data are continuously transmitted across networks and other devices as organizations continue to do business. Ensuring that systems are secure and safe is vital to protecting the business interest and their customers. To improve confidence and trust in products and services for both providers and customers, cybersecurity is dedicated to protecting sensitive information and the systems used to process and store it.

Kapersky (2020) and Perwej *et al.* (2021) define cybersecurity as the practice of protecting computers, mobile devices, electronic systems, servers, networks and data from unauthorized access, malicious attack and destruction. The term also applies to business and mobile computing contexts which can be divided into network, application, information, operational security, business continuity, disaster recovery and end-user education**.** According to Rouse (2020), "*The goal of implementing cybersecurity is to provide a good security posture for computers, servers, networks, mobile devices and the data stored on these devices from attackers with malicious intent*". As such, it is imperative to proactively monitor the constantly evolving threats in a business environment, such as malware, phishing attacks, man-in-the-middle attack, ransomware and social engineering, among others, thus endorsing a total security need to protect businesses in the worst-case scenario (Deloitte, 2019; Kaspersky, 2020; Pawar and Palivela, 2022). Essentially, a cybersecurity solution must account for total end-to-end security by *inter alia* protecting data applications, networks and end-users by preventing unauthorized access and improving recovery time after a breach while ensuring continuity among other things.

To adequately manage cybersecurity, the National Cyber Security Alliance (NCSA) (2018) recommends a top-down method to cybersecurity where management must take a leading role in prioritizing cybersecurity management and continuity across all a business' practices. Essentially, the NCSA maintains that organizations must be prepared to respond to unavoidable cyber incidents, restore normal operations and ensure that an organization's assets and reputation are protected. Additionally, organizations should take cognizance of any regulations or standards that will influence the way data should be collected, stored and secured to protect individuals, citizens, corporate and governmental agencies among others.

In effort to ensure cybersecurity, organizations continue to subscribe to existing best practices and standards to realize the feat, but continue to fall short as the cybersecurity problems continue to exist. The problem is existing cybersecurity standards/frameworks only present a macrolevel overview on how cybersecurity risk management should be approached leaving the details of how it should be effected to the individual organizations on account of the unique risks factors they are likely to experience (Gordon *et al.*, 2020; Al Faruq *et al.*, 2020). Existing ISM standards/frameworks are generic in scope and attempt to provide ISM practices that are focused on securing organizations' perimeter centric information systems, which when adopted by organizations at best showcases their commitment to secure business practices by applying and obtaining certificates that attest to their compliance, which is not enough to guarantee the required level of security. Meeting the bare minimum of a given framework can suffice in certification that will show compliance with mandatory regulations/laws, keep customers happy as it helps the organization maintain an image of responsibility at the lowest cost possible (Culot *et al.*, 2021). Thus, this derails cybersecurity efforts that should ultimately take cognizance of a variety of variables that can compromise absolute security.

Given the nuanced and dynamic nature of cybersecurity needs, a method that takes cognizance of these generic ISM guidelines and advocates a well-tailored solution that takes cognizance of the ever evolving organizations environment and operations to enable continuous and absolute security is desirable. Essentially, what is required to aid realize requisite level of security is an analytical and management approach that is vigorous and extends its focus beyond securing an organization IS to encapsulate both an organization and its customers' environment, as with their operations which continue to evolve.

According to Williams-Banta (2019), a solution that considers technology and human participation is necessary since looking at technology alone is not enough to stop hackers, and after all, people have often been considered the weakest link in a security chain (Dalal *et al.*, 2022; Poehlmann *et al.*, 2021). Spear phishing, a type of social engineering attack that targets an individual(s) has been blamed for more than 90% of cyberattacks that begin with tailored phishing emails that target a person in a company (Kerner, 2022). Thus, it is sensible that a solution that accounts for both the people's view as well as the technology is more desirable than paying attention to just one perspective that leaves the other vulnerable. To holistically account for the continuously evolving and sophisticated cybersecurity threats and vulnerabilities, this research proffers that taking a service approach leveraged on existing industry information security best practices, cybersecurity due-care and due diligence can be better attained. The approach employed toward that end is explicated in the next section.

3. The approach

Customers, citizens and lawmakers among others need to be ensured that a viable process to deal with cybersecurity threats, meet regulatory compliance and assure total security is in place. As such, organizations need to adopt sound cybersecurity measures to continuously gain a competitive advantage while ensuring customers' trust. Through an extensive

literature review, the study explores lessons from the service systems concepts, the information security management literature and cybersecurity bests practices among others to propose a cybersecurity service system model. Logical reasoning is employed to design the model by deliberately combining the best parts of existing frameworks toward holistically addressing cybersecurity concerns. The paper argues that this approach will present a holistic view that will adequately account for the understanding and mitigation of the ever-evolving cybersecurity threats and vulnerabilities while proactively and adaptively managing the resulting incidents from an end-to-end perspective. The proposed model is primarily framed within the service system concept theory and supported by the industry-specific standard frameworks. These concepts and frameworks that underpin the solution toward ensuring cybersecurity continuity and management are discussed in the next section.

4. The underlying concepts

This section delves into the concepts that provide the underlying premise for holistic cybersecurity management and continuity highlighting their strengths, focus and limitations. The section begins by unpacking the ITIL ISM framework and the NIST cybersecurity framework, respectively. Next, the service system concept theory which frames the proposed solution is explicated. The following subsection begins with a discourse on the ITIL-ISM framework followed by the NIST CSF and finally the service system concept.

4.1 The ITIL information security management framework

Primarily, *the ITIL defines a service as "a means of enabling value co-creation by facilitating outcomes that customers want to achieve, without customers having to manage specific costs and risk.* The ITIL outlines a set of detailed practices that centers on aligning IT services with the needs of the business. The ITIL describes processes, tasks, procedures and checklists that are neither organization nor technology-specific but can be applied by an organization to strategy, value delivery and keeping a minimum level of proficiency. It allows organizations to create a reference point from which they can plan, implement and assess improvements as well as demonstrate compliance. As such, the ITIL ISM looks to align IT and business security to ensure that information security elements (availability, integrity, confidentiality authenticity and nonrepudiation) are well managed in all services and also in the service management activities (BMC, 2016).

Essentially, the ITIL ISM which is premised on the ISO 27001 standard specifies requirements to establish, implement, maintain and continually improve an ISMS within the context of an organization by assessing and treating information security risks to fit the needs of the organization (Al Faruq *et al.*, 2020). Certification to the ISO 27001 Standard is recognized worldwide to indicate that an ISM system is aligned with information security best practices (Culot *et al.*, 2021; Pawar and Palivela, 2022). It is designed to check the selection of sufficient and appropriate security controls to protect information assets while giving and ensuring trust to interested and relevant entities. Thus, security controls are specific and tailored to the needs of individual establishments or their parts (Fonseca-Herrera *et al.*, 2021). Several leading establishments such as Netflix, Apple, Amazon, Facebook and Microsoft and their partners among others advocate being ISO/IEC 27001 certified (Culot *et al.*, 2021).

However, the focus of the ISM implementation is predominantly organization perimeter-specific focused on service providers and barely on the customers' side who are only seen as just the consumers/users of the service who provide only marginal contribution to the entire service provision process (Alter, 2010). Thus, the ITIL ISM approach is service provider-centric with a focus on the internal production processes with very little or no attention to the customers' responsibility and activities to co-produce value in terms of providing more valuable insight that will improve the entire service system among others. As such, despite

the existence of the ISMS framework among others,the impact of cybersecurity breaches on organizations continues to rise (Williams-Banta, 2019; Hitchcox, 2020). Additionally, the focus for an organization has been on compliance models, which oftentimes means providing the bare minimum using some type of checklist to meet compliance as opposed to sufficiently meeting the security needs of the organization. By complying with such standards, most of the time it is easy to assume that an organization has fewer risks even if it is not the case as gaps may exist that need to be tackled to realize the requisite level of security.

The ITIL ISMF is recognized under the service design process group of the ITIL best practice framework to control access to organizational information. It describes the techniques and commands the degree of IT security with business security inside an organization, ensuring that information security is managed aptly in all services and the services' management activities. The security requirements based on a risk assessment are prescribed in the service level agreements (SLAs) and the operational-level agreements (OLAs) are used by the internal working groups to support SLAs along with other external requirements that are defined in supporting contracts, legislation or regulatory bodies among others. The ITIL suggests that an ISMS should address people, processes, products and technology and partners and suppliers. Typically, the ISMS framework addresses five key elements, namely control, plan, implement evaluate and maintain (Invensis, 2020). Figure A1 in Appendix presents an overview of the ITIL ISMS framework.

The control component based on the requirements stated in an SLA suggests preparing and implementing an information security policy, allocating responsibilities and controlling documentation. Thereafter, developing a plan and putting it into action (implement) taking cognizance of the budget and corporate culture, evaluating the implemented plans to ensure they meet the requirements and ensuring continuous service improvement (maintain). The activities of the information security management process can be equated to Edwards Deming's Plan, Do, Check and Act (PDCA) Quality Circle. A service provider will develop security plans (PLAN) for the organization based on a client or environmental requirement stated in an SLA. These plans consist of policies and OLAs which are then implemented (Do) and then eventually evaluated (Check) after which the plan's implementation is sustained (Act) toward meeting the client or environmental needs. Based on reports, clients can change or adjust their requirements while service providers make adjustments to their plan or implementation based on findings towards satisfying all requirements (Old + New) stated in an SLA. Looking at the evolving nature of the framework given the changing nature of requirements, this study equates the framework to the work system lifecycle model (WSLC) discussed in section 4.3, which looks at how a service system changes and evolves through iterations of both planned and unplanned changes.

To adequately meet service level requirements, the ITIL service strategy takes cognizance of organizational capacity in terms of capabilities and resources as important constructs for service realization. The resources here refer to the components which serve as direct inputs for production while the capacity to control, coordinate and deploy the resources refers to capability. The "resource" here is considered to be organizational assets inclusive of IT infrastructure, people, finances, applications and information or anything that can aid in IT service delivery while "capability" is seen as the organization's capacity to deploy resources considering the ability of an organization, person, process, knowledge, configuration item or IT service to carry out an activity. Thus, it is the workings and availably of these two components that will determine a successful service provision. While it is convenient to distinguish the asset types, it is often impractical, as in reality, they correlate and overlap, forming a mixture or composite. Although the degree of intermixing may vary, they can influence the performance or functioning of one another. The people as assets can be referred to as both resource and capability as they are instrumental in delivering a service and carrying out actions.

The ITIL ISM is broad in scope as the intent is on protecting organizational information assets from both technical and nontechnical threats from unauthorized access, use, disclosure, disruption, modification or destruction to provide confidentiality, integrity and availability.Thus, the ITIL ISM deals with data security in general which means protecting data in cyberspace is an aspect of it and beyond as online threats continue to lurk over organizations. Although the ITIL ISM advocates a holistic approach to ISM like the NIST framework discussed in the next section, they lack specificity and are ambiguous on how an implementation is carried out. The NIST framework which was created with the sole purpose of preventing attacks and protecting data in cyberspace is unpacked in the next section.

4.2 National Institute of Standards and Technology (NIST) cybersecurity framework

The NIST cybersecurity framework (NIST CSF) was published in February 2014 as a set of best practices recommended for organizations and businesses alike to protect critical IT infrastructure. This was in reaction to US Presidential Executive Order 13,636, which called for Improving Critical Infrastructure Cybersecurity in the USA. The framework has been recognized as a resource to help improve the security operations and governance of public and private organizations. Like the ISMS, it comes at cybersecurity from the point of view of risks rather than just suggesting controls to implement. Hence, it has been adopted and modified by several organizations. One such adoption can be seen in the Nigerian National CSF developed by the National Information Technology Development Agency (NITDA) (2019). The framework presents guidelines for transforming an organizational security posture and risk management approach from a reactive to a proactive one. The NIST CSF has gained wide acceptance as an approach to facilitating cybersecurity risk management. The framework has got wide adoption by businesses and government agencies in the USA and around the world (Gordon *et al.*, 2020). Ibrahim *et al.* (2018) use the NIST CSF to assess cybersecurity posture of a local government in Western Australia.

The NIST framework makes compliance suggestions along 98 subcategories, which can become challenging without adequate guidance on prioritization. The framework core reflects five functions of cybersecurity risk management which are Identity, Protect, Detect, Respond and Recover were under each category and subcategories as shown in Figure A2 appendix overviews the NIST CSF categories and functions. Each function is crucial to a working security posture and successful management of cybersecurity risk. Each of the subcategories can be matched to a list of standards such as NIST, Control Objectives for Information and Related Technologies (COBIT), International Organization for Standardization (ISO) among others that can be followed to take advantage of their specific controls; it is expected that organizations will make their own choices on measurement scales. The framework core function "Identify" reflects developing organizational understanding to manage cybersecurity risk to assets systems, data and capabilities; "Protect" by developing and implementing appropriate safeguards to ensure service delivery; "Detect" to identify occurrences of a security event; "Respond" to developing and implementing appropriate security event mitigation or resolve activities; and finally "Recover", putting together appropriate activities for resilience and restoration of capabilities and services that were compromised or weakened due to a security event.

The NIST CSF also presents the control or implementation tiers, to help organizations benchmark their operation in terms of how well they view cybersecurity risk and the processes in place to mitigate risks. Essentially, the tiers indicate the implementation level of the determined organization's controls. The NIST CSF does not provide detailed prescriptions instead organizations are required to profile themselves based on their business requirement, available resources, capability and risk tolerance to guide the cybersecurity options to be selected. The framework is adaptable and engages cybersecurity from a risks point of view as opposed to just suggesting controls to implement. Although the

NIST CSF provides a very comprehensive guide to perform cybersecurity risk assessments of information systems, it is limited given the continuous surge in cybersecurity breaches and incidents (Hitchcox, 2020; Williams-Banta, 2019). The failure to adequately meet the cybersecurity needs can be attributed to the frameworks being too high level, and in addition to its difficulty to navigate, it is a compliance checklist that can present a false sense of security and fewer risks (Jones, 2018; Hitchcox, 2020). Thus, while the industry standard compliance checklist is useful, it does not mean there are no gaps left in the system when they are utilized, making them limited when it comes to realizing complete security.

The NIST CSF as mentioned is a very high-level, broad and flexible framework where the details and depth of security assessment are open to organizational interpretation and preference. More so, the CSF implementation tiers (partial, risk-informed, repeatable and adaptive) do not represent a maturity model but rather just show an indication of an implementation level. As such, it is left to the organization to subscribe to other complementary standards and best practices to realize certain aspects of their security needs to attain an adequate level of compliance and service (Ibrahim *et al.*, 2018). The Nigerian cybersecurity framework, for instance, draws from the NIST CSF core functions and added the procure dimension to account for the role procurement plays in compromising other efforts in situations where "not up to code" information assets exist. More so, to build the maturity model to assist with assessment and calibration concerns the NITDA framework looked to assessment models such as the OCTAVE from the Carnegie Mellon Software Engineering Institute and the CCTA Risk Analysis and Management Methodology (CRAMM) among others. The NITDA maturity model consists of the basic, intermediate and advanced calibration levels to assist with status quo finding of where an organization is and where the organization needs to be.

As shown in the discussion so far, there is no one framework, model or best practice that proffers a total solution for cybersecurity management, rather several aspects of security are considered from different perspectives as such it is a combination of the different frameworks' strength and more that will adequately address cybersecurity concerns. Given the continuous rise in cybersecurity breaches, Jones (2018) maintains that the way cybersecurity risk management is carried out should be reexamined because a successful security risk management program revolves around the ability to correctly assess an information system risk environment (Hitchcox, 2020; Wilkinson, 2020). Thus, the development of an analytical model to enable individual entities to evaluate their unique threats and adequately leverage the large menu of standards and practices dished in the CSF in a sustainable manner is recommended. This study argues that combing the service system concepts discussed in the next section in cognizance with the NIST CSF and ITIL ISMF discussed previously a basis to better understand and mitigate the ever-increasing cybersecurity breaches and incidents can be realized. The next section unpacks the service system concepts which this paper employs as the primary theoretical frame for the proposed cybersecurity service system model.

4.3 The service systems concept

Almost all purposeful systems within governmental entities or a business can be seen as service systems since competencies and skills are manifested and applied to yield something of value for someone. A service system view employs the notion that value from a service system is coproduced by service providers and service consumers. Thus, the view takes cognizance of the activities and responsibilities of both service providers and customers. Essentially, the customers' value to the system involves more than just receiving and using whatever the service system produces. In line with Alter (2008a), this paper adopts Vargo and Lusch's (2004) definition of a service they say represents "the application of specialized competencies (knowledge and skills) through some actions or processes, and performances

for the benefit of another entity or the entity itself (Self-service)." This definition reflects a "service" as a value-producing process between a service provider and a customer, be it a business, software engineering or an IT service standpoint.

According to Alter (2013), viewing systems as services improves business/IT communication and provides an umbrella that enhances systems analysis and design methods by making known concepts that would have otherwise been ignored or labeled outside the valid scope of analysis. Alter (2010) maintains that by acknowledging service concepts and constructs, issues associated with inadequate user/business engagement and IT solution alignment can be addressed. By placing a customer of the work system in view throughout an analysis, a deeper insight beyond just inquiring about IT requirements, building capabilities that fit the elicited requirements and assuming that the users will be happy. This trend which has been the cornerstone of most information systems can present capabilities that may satisfy the IT user but may adequately support the work system entirety geared to meet the customer's wants and needs. For example, a banks' information system can be built to support their internal processes without taking cognizance of how that can impact the customer of the tool user as long as it simplifies their effort. According to Alter (2008b, 2010, 2013), most of the IS field hinges around a tool-centric approach that is focused on building tools, providing detailed specifications, adopting and using such tools by users. He maintains that, while the tool-centric approach is essential to building well-engineered tools and interfaces, the service system view should complement the approach to accommodate contexts that might be ignored or downplayed.

Viewing cybersecurity as a service system will help cybersecurity analysts focus on the processes by which a customer (internal or external) attains value from what the system produces and how it will shape the requirements that the supporting technical artifact should satisfy and vice versa. Thus, customers are treated as coproducers, recognized as a vital part of the system being studied, as opposed to being seen as just users of what the system produces. The service system approach appreciates the performance of work to realize the customer needs and recognizes the tool as what is needed to do the work. As such, the service system and the tool-centric approach will shape each other where the latter has little usefulness without the former which in turn cannot achieve effectiveness without the latter. Essentially, rather than just emphasizing service providers' processes and information as usually witnessed in a typical system analysis and design approaches, a service system customer perspective is accounted for whose activities and responsibilities would have otherwise been considered irrelevant or marginal at best unless they hinged on the providers information system.

Spohrer *et al.* (2007) and Thomas *et al.* (2015) described service systems as compound systems comprised of dynamic arrangements of resources and capabilities inclusive of people, organizations, shared information/knowledge and technology, with at minimum, one active partaker capable of interconnecting and judging outcomes. Thus, they emphasize a holistic understanding of such organizational assets and their contribution capacity to the entire service system to create value. Alter (2008a, 2010) introduced three frameworks that provide the footing for understanding, analyzing and building service systems. This group of frameworks is said to be apt for identifying difficulties and opportunities in service systems. The frameworks include the work system framework which is ideal for situation analysis that provides an organized way to reflect on systems as service systems with the customers in perspective, the service value chain framework that considers value co-creation in terms of opportunities and expectations and the work system life-cycle model that focuses on a systems' malleability to change. Thus, the frameworks work together toward establishing a successful service system. Figure 1 overviews that the suite of the service system frameworks must work together to realize a holistic service system management. A service system is a work system that can be understood and probed in terms of the elements of a work system

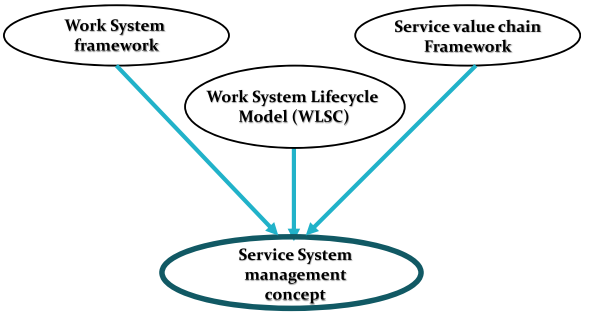

Figure 1.
Suite of the service system frameworks for service management

Source(s): Alter, 2008a; 2010

element which provides a catalog of components to appraise, how they are organized and what they intend to accomplish.

The work system framework utilizes nine basic elements to provide system-oriented visibility of any structure that carries out work within or across organizations. This makes it useful in identifying problems and opportunities (Alter, 2008a; Petkov and Petkova, 2008). The four elements responsible for production include work practices (processes and activities), participants, information and technologies. The other five elements existing to facilitate an understanding of the situation include products/services produce, customers, environment, infrastructure and strategies. This provides a basic understanding of the operation, context and significance of the service work system. The environmental context where the service will operate determines how the service system, and the corresponding services, should be designed. Customer satisfaction underpins a service system as such they must be designed to deliver services that most satisfy the needs and expectations of the customers. Therefore, the technology configuration and the design of organizational networks to deliver a cybersecurity service must satisfy the security requirement of both the external and internal customers. Essentially, a cybersecurity service system will see human participants and/or machines perform work (processes and activities) using information, technology and other resources to produce security products and services for internal or external customers who are also participants in the value-producing service system. The elements and behavior of the work system elements can be equated to the ITIL resource and capability components highlighted in section 4.1 as they can influence the performance or functioning of one another at different levels of granularity given a need context.

The service value chain framework emphasizes the importance of recognizing both the service customer and service provider's responsibilities at every step in the processes and the corresponding activities. The concepts such as awareness, negotiation, preparation, request, fulfillment and follow up among others in the service value chain framework can facilitate the analysis design and evaluation of an IT-dependent work system by highlighting notions or discrepancies that an analysis from only a provider perspective might miss, thus emphasizing that value from services is co-produced by both the service provider and consumer alike.

The WSLC describes how a service system or a work system evolves, which is said to be through iterations of changes that are planned or unplanned. The planned changes occur similar to the traditional project management phases which are initiation, development, implementation operation and maintenance phases whereas the unplanned changes represent unending adaptations that change aspects of the service system which can be due to changes in the environment, uncertainties or opportunities that might occur. The WSLC reflects aspects of both the ITIL ISMF and NIST framework. The ITIL ISMF in

addition to the streamlined formal project approach recognizes an evolving security framework that takes cognizance of unplanned changes, and the NIST, on the other hand, is more aligned with the planned changes approach. Notwithstanding, given the ever-evolving threat and vulnerability landscape in cyberspace, a cybersecurity service system must take cognizance of both the planned and unplanned changes that are reflected in the WSLC model. Thus, the proposed cybersecurity service system model leverages on the lessons from the service system concepts, the ITL ISMF and NIST CSFs. Figure 2 overviews the conceptual fitting to building the cybersecurity service system as it looks to address the cybersecurity problem space from both the service provider and customer perspectives.

The proposed cybersecurity service system in section 5 subscribes to the principles of the service system concepts which recognize that value from service systems is co-produced by both the service provider and customers. In addition, the interaction between a service provider and consumer which is viewed as the essence of service is important for garnering more insight. Also, it should be noted that a service system changes and evolves. The capacity of service providers to recognize, identify and respond to consumers' needs (stated or unstated), interests, fears and concerns are vital especially to ensure continued service quality among other things. By applying a customer-centricity idea to the cybersecurity service system, hidden insight/concerns surrounding the workings of the IT-reliant system can be exposed. This study argues that by taking a service system approach to cybersecurity, the nuanced cybersecurity challenges associated with the continuous increase in cyberattacks, breaches, online fraud in cyberspace and the ever-evolving threats (internal/external) and vulnerabilities landscape can be better mitigated. The next section presents the proposed cybersecurity model which hinges on the service system concept.

5. The conceptual cybersecurity service system model (CSSM)

What is clear from the review in the previous sections is that no one framework or standard provides an all-encompassing cybersecurity solution, what is recommended is a combination of different aspects driven by contextualized service provider/customer-centric requirements. Also, there is a need to ensure adaptive continuous management of cybersecurity service

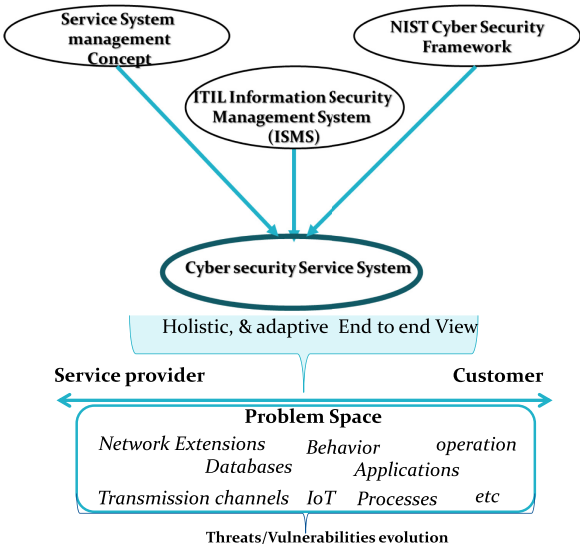

Figure 2.
The underlying cybersecurity service system concepts

systems to account for the ever-evolving threat and vulnerabilities landscape. To avoid a one-sided assessment focusing totally on the internal operation of the work system that may leave weaknesses undetected, giving an organization a false sense of security state and risk exposure, a holistic and continuous approach to cybersecurity and cyber resilience needs to be employed. As the cybersecurity threat and vulnerability landscape continues to evolve, a flexible and adaptive approach that can account for such changes and uncertainties alike becomes desirable. This section proposes a cybersecurity service system archetype.

This paper argues that to account holistically for the cybersecurity problem, there is a need to view cybersecurity as a service system. The service system view promises an approach that looks beyond a service provider perimeter to capturing and evaluating how a service consumer is faring and is satisfied. The proposed cybersecurity service system is premised on the combined lessons from the industry-specific standard frameworks and the service system concepts discussed in section 4. For instance, the proposed model leverages the customer/service provider relationship supported by the work system elements from the service system concept and the PDCA lifecycle model implemented in the ITIL ISMS, as well as the linearly streamlined actions elaborated in the NIST CSF framework which resonates and complements the planned and unplanned changes as prescribed in the service system WSLC. Figure 3 presents an overview of the cybersecurity service system model (CSSM) composite of various components as identified in the previous section working together.

Figure 3 shows that the cybersecurity services will be co-produced by both the service providers and the customers as inspired by the service value chain framework in section 4.3.

Thus, understanding and explicitly laying out the actions and responsibilities of both the service provider and customer is critical. Every instance of the service delivered suggests an explicit or implied service request from the customer component. The customer component represents both an external customer that will consume what work system produces (e.g bank customer) and the internal customers who are bank workers/units that are part of the work processes (internal operation) that depend on each other to ensure value is delivered to the external customer. Essentially, the service providers' responsibility includes creating awareness of the service, handling and fulfilling service requests while ensuring customer follow-up based on negotiated commitments. The customer in turn becomes aware of a need, consumes and contributes to the service by making service requests, participating in fulfillment, providing feedback performing follow-ups as per negotiated commitments.

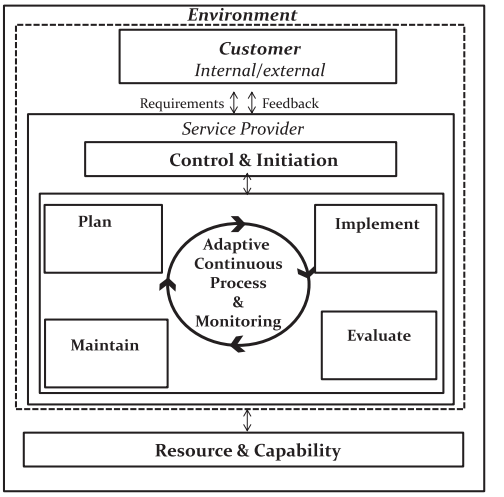

Figure 3.
The cybersecurity service system model (CSSM)

The interaction between the service provider and customers opens a way for both parties to be situationally aware in terms of the needs, ongoings, interests, fears and concerns of each other. Projecting the successful cybersecurity effort will depend on what the provider understands based on quality analysis, which is fed by quality input from customers and their surrounding environment who in turn are expected to comply with what is prescribed, evaluate its impact (positive or negative) and feedback into the system.

The **customer component** represents the direct beneficiaries of the cybersecurity service representing the service customer and other environmental entities. The **customer** component of the customer section includes individuals, groups, organizations or functional units within that will receive the benefits created by the activities of the cybersecurity service system. The service benefits should apply regardless of whether services are directed at external customers, internal customers or both. The environmental entities include *inter alia* the relevant regulations, policies, standards or legislation that require compliance. As such, the customer component with the environment is responsible for making up the service requirement that will guide the action of the service provider, which will influence the SLA prescribed in the control and initiation component. Thus, the SLA should be malleable to change. Changes in customers' needs often driven by environmental uncertainties, opportunities or challenges in their resource/capability can lead to changes in the work system elements supporting the service system. Also, from the service provider's direction, changes in one of the work system elements like information and technology can be appraised on their effect on the internal operational efficiency of the service system and customer satisfaction. Thus, the need for consistent interactions between the two parties cannot be overemphasized.

The **service provider** component hosts the control and initiation activity as well as the security management process supported with the necessary resource and capabilities to ensure complete and satisfactory cybersecurity service provision to customers. The service provides represents the internal operation of an organization's cybersecurity service system which takes cognizance of customers' evaluation of what the system offers towards improving the entire service system. The control and initiation activity of the service provider perspective is responsible for organizing, directing and managing the security management process. It defines the processes, allocates the responsibility and defines the policy statements, rules and management framework. It initiates the security process setting the tone that is supported in the other subsequent process activities stages introduced. The control component sets up and modifies the SLA or contracts between the service provider and the customer. Contracts are agreements set for accessing, processing, communicating, or managing information, software or services between an organization and external parties or employees. For example, an agreement can be set to ensure that external parties and employees abide by the policies set out by an organization. The security requirements are defined under SLA alongside the responsibility of the service provider and customer as well as the service level targets. The control components also handle the Service Level Report to be issued by service providers to their customers.

The **Plan** activity in cooperation with service level management devises and recommends appropriate cybersecurity measures based on an understanding of the requirements as defined in an SLA. The Plan activity specifies the goals as expressed in the SLA in the form of OLA security plan that will be undertaken by an internal unit within the service provider's standpoint toward the general cybersecurity service provision. Other input into the "Plan" activity includes among others; the policy statement and rules established in the control activity process. Furthermore, The Plan activity incorporates the "identify, analyze and evaluate the risks" as can be seen in the NIST in section 4.2 CSF and part of the "Do" as in the ISMS cycle in section 4.1 which involves controls selection and implementation of policies. The output of the "Plan" activity is the implementation plan.

The **Implement** plan activity ensures that all the control measures as specified in the plans are properly carried out. The section handles the implementation of protection technology and services to help mitigate cybersecurity threats and vulnerabilities taking cognizance of both the customer/provider perspectives. This also involves Security Education, Awareness, and Training (SETA,) which should be specified in the plan base on planned or unplanned changes. This activity reflects the "Do" section of the ISMS model, requiring the implementation of controls to reduce or ease the risks discovered during the analysis activity. The content will determine what level of control will be required. For instance, the health sector will find unique controls as specified in the Health Insurance Portability and Accountability Act (HIPAA) security rule. However, whether the controls implemented are effective or successful, an evaluation needs to be carried out to confirm which the customer must be engaged in.

The **Evaluation** activity is vital to appraise the success of the security plan implementations. It checks the sturdiness and compliance of the security implementation with the security policy and requirements spelled out and specified in SLAs and OLAs, respectively. An Evaluation result is used to uphold the agreed measures or lead to new requirements where a "Request for Change" process can be engaged. The evaluation activity represents the Check process of the ISMS, which is responsible for reviewing whether requirements as specified have been satisfied. Both technical and nontechnical measures employed to realize compliance or total security are evaluated periodically to ensure that requirements are being met. A service desk incident report in terms of the number of breaches, resolutions and escalations can indicate the efficiency and proficiency level of existing measures while exposing vulnerabilities if any. Organizations can do well to evaluate their level of security maturity at this stage to determine where they are and where they need to be and are adequately meeting and satisfying customer needs.

The **Maintenance** activity process suggests that for cybersecurity management to be effective, it needs to be improved and enhanced continuously. This involves reviewing the SLAs, the security policies as well as the control and monitoring techniques. As organizational and IT infrastructure and work patterns continue to change, the security risks change as well over time. Thus, the need for consistent revisions of the security segment of an SLA and security plans. The results from evaluations and the insight into the changing risk landscape serves as input to the maintenance activity. The output of the maintenance activity is the change proposal to be acted upon at the control stage and translated into an action plan. Essentially, the evaluation outputs propose improvements or changes to the security implementation and agreements as laid out in the SLAs and OLAs.

The plan, implement, review and maintain activities are not one-time activities; they are adaptive cyclic and continuous activities, as shown in Figure 2. These actions are in line with the WSLC model described in section 4.3, which states that a service system evolves through a combination of planned and unplanned changes. An initiation stage will follow a formal project development approach in terms of the planned changes while uncertainties that may occur from the environmental changes will result in unplanned changes such as ongoing adaptations and experimentation that will change aspects of the service system. The success of such engagement is certainly determined by the availability of the resource and corresponding capabilities. The iterative nature of the model speaks to the Identify, Protect, Detect, Respond and Recover functions of the NIST CSF. Thought must be given towards the abilities of an entity (Service provider/customer) to perform their activities as required or specified by a plan, matching the supporting resource and capability at their disposal.

The **resource and capability** components are composite of both the work system elements described in section 4.3 and ITIL organizational capacity elements described in section 4.1 in the context that knowing the proficiency and availability levels of these components is critical to successful cybersecurity service provisioning. By focusing on

probing questions around the resource and capability components, insight into their proficiency level to provide the expected service return from both provider and customer can be uncovered. For instance, if an issue revolved around competency, experience, knowledge of execution or know-how of doing something, roles and responsibilities among others, tt can be deemed a capability problem, and if it dealt with something *that* could be acquired, such as an IT infrastructure, people and money among others it is a resource problem. Table A1 in Appendix presents a template made up of composed dimensions premised on the service work system and the organizational capacity elements as well as the service value system interaction constructs. The template dimensions which are presented in no particular order will aid analysis that considers the customer/provider perspectives, noting where a problem is indicated along a dimension, its risk level and impact, what is proposed as a solution requirement, the state of implementation and what was realized in the form of results (successful or not) and other likely comments. By probing the dimensions, failure points that will need to be addressed whether for example through changes in an IT system or behavioral changes in participants among other things can be realized. Of course, the dimensions are by no means exhaustive, they can be extended given a need context or opportunity context and they can be further broken down to lower levels of detail items. For instance, the infrastructure dimension can include detailed concepts like interoperability and integration concerns, the knowledge dimension could include constructs like acquisition and utilization codification concerns, and the participant dimension could reflect a lack of awareness, knowledge or skill concerns, and application can reflect a configuration issue among others. As changes in one component can affect other components at different levels of granularity, the ripple must be traced and logged. Thus, the study argues that questions structured around these components from both the service provider and customer angles will help determine risks that will affect the cybersecurity service systems' successful functioning. Of course, further dimensions can be incorporated into the template at different levels of details to account for nuanced cybersecurity landscape.

6. Discussion

The proposed cybersecurity service archetype promises a total end-to-end view of the cybersecurity service delivery system that takes cognizance of technology and human participation among others, moving beyond the often technical or compliance focused views of existing approaches. Given the IT-reliant nature of the cybersecurity service system, the protection required is considered from the backend support systems, processing, transmission and front-end customer interfacing and service consumption. Thus, remedies for all possible aspects of cybersecurity, including network, information, application operational security, disaster recovery, business continuity planning, end-user education and continuous interaction with the service providers, are considered. An effective cybersecurity approach must encompass the entire IT infrastructure involved in service provision and must be premised on consistent risk assessments that may come from both a customer and service provider environment.

The customer and service provider interaction provides an avenue to better understand a situation status-quo so as to better prescribe the solution or approach a customer can contribute to the system without too many difficulties and vice versa. Both service providers and customers whether internal or external should be aware of the ongoings and the reaction required in a given situation. Thus, a culture of being situationally aware can be nurtured. Whether it is human-to-human or IT-reliant interaction (service desk) and follow-up, knowledge can be acquired that can result in quality data that can be leveraged by cybersecurity security professionals or artificial intelligent (AI) and machine learning systems for instance to better fortify an intrusion detection system that can predict, mitigate

possible threats and manage vulnerabilities to prevent cybersecurity breaches. Also, the interaction between the stakeholders can require changes in behavior of actors to achieve better levels of security. Thus, efforts to realize better security form the service lens can result in changes that impact both the technological and the people or participants dimensions among others for example.

The proposed service system approach ensures value is co-produced by both the service provider and customer as prescribed in section 4.3. In essence, the service expectations are defined by both the delivery organization and those that will be using the service. For instance, a debit card fraud incident may occur online after a customer's card has been compromised resulting in the card termination when reported to the bank to prevent further damage. To get a workaround that ensures customers' funds are protected, the bank creates awareness on a virtual card service where only funds that are required for the immediate transaction are deposited. The virtual card will perform the service of the debit card with a limited risk of loss. Of course, to ensure the success of such a venture, the service provider bank must ensure customers are aware that such a service exists to subscribe to and make sure they are equipped with the requisite knowledge to make it work. Thus, two-way feedback traffic exists to ensure success. In addition, the circumstance that caused the fraud incident to occur should be noted and made sure other customers are educated regarding the situation and how to prevent such occurrences. Surely, an agreement on the service level quality that is required and expected is explicated to put targets and measures in place, to keep track and measure success or otherwise.

The proposed service system approach allows the move beyond the often once-off IT requirement and specification that has been central to the existing system analysis and design approaches that are fixated on building a technical artifact as a tool for users, which may not necessarily benefit the customer of the work system. The service system presents an opportunity to make the customers be more involved in contributing to the overall functioning of the service systems as opposed to their often-marginal roles in the requirement elicitation process as potential users of an IT tool witnessed in existing system analysis and design approach as highlighted in section 4.3. Thus, by employing a service system lens, the customer is seen to have more responsibilities that involve more than just consuming or using what the service system produces but providing feedback that will in turn improve the service system. For example, iterative feedback from a consumer can be used to improve an IT component feature or participants' behavior, knowledge or competence from a service provider perspective to provide an overall positive service provisioning experience. Employing a service stem approach promotes co-value production that emphasizes quality interactions between a service provider and a consumer to adequately understand the state and concerns of each other from the obvious to the nonobvious ones. Given the cybersecurity landscape, this is an important feature to help cybersecurity professionals get ahead of the consistently evolving nature of the threats and vulnerability landscape discussed in section 2 that will result in consistently changing requirements from planned or unplanned changes.

The service system process as shown in Figure 3 ensures that activities required to realize adequate security provision are in play as well as those necessary to ensure its maintenance and continuity. Essentially, the model understands that starting with customer requirements or environmental needs explicated in a contract, law, regulation standards or organizational policies, among others, actions should be carried out to ensure that requirements are serviced while taking cognizance of the fact the requirement will evolve due to changes in the environment that continuously introduces new threats/vulnerabilities. Essentially, the proposed CSSM promises due care and diligence which although limited is mostly the goal of the industry-standard compliance frameworks highlighted in section 4. Due care and due diligence are realized as the model ensures that what is required to ensure that organization and customers are protected is in play, and appropriate measures are taken to ensure

continuity and improvement towards meeting the set security goals. Thus, the model explores ways to ensure potential security gaps are closed while ensuring that the business is prepared when faced with unknown but present malicious threats and vulnerabilities. The proposed CSSM approach promises to proactively combat and manage threats and vulnerabilities across a business process to improve cybersecurity and ensure cyber resilience.

The analytical dimensions presented in Table A1 as instances of the resource and capability components will enable organizations to evaluate and measure the cybersecurity gaps and the sufficiency and limitation of the controls in play from both the service provider and customers' perspectives so that informed choices can be made about what is needed and where to apply the often-limited resources. This action will take cognizance of the service provider and customer problem spaces. The CSSM promises a broad-spectrum view of what is required from start to finish of service from the service management, its supporting structure, resources and capabilities. The model is designed to ensure that any context-specific security is based on risk assessments, defined policies, procedures and controls while ensuring that cybersecurity is integrated as much as possible into the daily work and operations of the service provider and customer alike to ensure utility and warranty through adequate interactions, feedbacks and follow-ups. Utility defines the usefulness of the service ensuring it fits *for purpose*, and warranty defines the guarantee of the service that it meets the set requirements. By following a holistic approach to cybersecurity, it is ensured that everything organizations will choose to do to co-create value for themselves and their customers is protected at each point in the value chain. Creating a cybersecurity service unit that will take ownership of the CSSM model overseen by the cybersecurity professionals to ensure its implementation and fulfillment is desirable.

The implication for cybersecurity management researchers and practitioners alike is that traditional organizational IS-centric thinking needs to extend beyond the organization and take cognizance of the customers' environment and operations that equally contribute to the overall service provisioning experience. Thus, the proposed model presents a novel analytical perspective identifying relevant elements that should be considered to truly satisfy an end-to-end security and better streamline existing standards controls. Essentially, solutions should encapsulate technologies, people, structures, processes and practices among others. The paper urges practitioners to consider cybersecurity needs and practices in a broader business environment where data/information are exchanged to satisfy service provisioning. Using the proposed approach will prompt for early knowledge of possible risks as such allow for a proactive action than reactive.

Given the multi-disciplinary and complex nature of cybersecurity and its varying application domains, it is important that researchers and practitioners collaborate and share knowledge as cybersecurity risks continue to evolve, in terms of identified threats, vulnerabilities and mitigation strategies. By having a common knowledge repository that logs such action (cause and effect), organizations can learn about prominent threats and vulnerabilities among others to proactively evolve their security programs based on their unique assessment, projections and resource courtesy of a shared knowledge base. It has been established that the unavailability of data on cyberrisk poses a huge problem for stakeholders looking to tackle cybersecurity issues (Cremer *et al.*, 2022). Proactively modeling or simulating actions in relation to the risk impact will certainly be useful for projections, especially when AI is leveraged.

Another area of interest to the cybersecurity domain is to try and minimize end-users' cyber misbehavior (employee or customers) by identifying and understanding factors that can aid predict such behaviors as well as design interventions (technical, processes or rules, etc) that can alter such behaviors while incorporating new ones that will better serve the cybersecurity agenda. An investigation into how behavioral characteristics can be incorporated into service design to help mitigate job role over extension and behavioral cues overload for both employees and customers will be valuable. Cybersecurity-centric

additional work should be identified and not assumed as part of a primary employee job role so that it is better infused into their work patterns. Also, knowing the managerial implications of integrating multiple standards towards addressing cybersecurity concerns will be valuable, especially for capacity planning, resource allocation and distribution among other things.

7. Conclusion and future work

It has been established that given the ever-changing threat and vulnerability landscape associated with cyberspace adoption, organizations and individuals are exposed to different types of risk daily. As such, employing a clear approach premised on a service system concept and lessons from industry-standard compliance frameworks will enable an organization to identify risks, know how to address them, monitor and repeat the process. However, the success of the service system is premised on the fully engaged interactions between the service provider and consumer of the service system who will contribute immensely to the functioning of the service system as co-producers of value. By supporting the consistent interactions with customers (internal or external), the model promises to help cybersecurity professionals who are tasked with the responsibilities of looking out for holes and misconfigurations that can cause or create vulnerabilities across the service spectrum. In essence, having an end-to-end view of the service will ensure that security incidents can be detected, mitigated and corrected without compromising service delivery. To possess, an effective cybersecurity solution for any given context careful planning is required to secure and manage the business processes and corresponding devices from the source to the destination. The activities described in the proposed CSSM need to be taken cognizance of to achieve a total and effective end-to-end cybersecurity solution as well as ensure up-to-date compliance. The proposed service system sees a technical artifact as a tool needed to help perform work effectively to fulfill customer needs who in turn contribute the service system functioning. By employing the ISMS cycle as part of the cybersecurity model functioning, a proactive and continuous security assessment, management and appropriate scaling given situational changes is ensured. The implementation of controls should be context-driven and dependent on the risk assessment which must be continuous to ensure new threats, and vulnerabilities are identified, documented, and appropriate actions are taken. The analytical dimensions in Table A1 provide a broader scope of inquiry that goes beyond the limited focus on technical or compliance issues. The proposed CSSM approach promises to provide the confidence needed for organizations, employees and individuals to focus on value production by extending their business to cyberspace with the assurance that they will be adequately protected.

However, future work should see to the instantiation of the proposed model and corresponding analytical template across different industries to validate its utility towards generalization. Findings from such instantiation will contribute to research and practice in the security management sphere for instance, further breaking down the analytical dimensions into sub-dimension inquiry or specifics and more. Also, the approach can augment IS research as the dimensions' inquiry can provide insight for better requirement fulfillment that might be missed or ignored by an analyst. While the CSSM is premised on the service system principles and lessons from the industry standards, it is still conceptual. Thus, what is required is testing the model to show its usefulness and possible limitations in analyzing and curbing cybersecurity challenges from both the service provider and customer perspectives.

References

Al Faruq, B., Herlianto, H.R., Simbolon, S.H., Utama, D.N. and Wibowo, A. (2020), "Integration of ITIL V3, ISO 20000 and ISO 27001: 2013 for IT services and security management system", *International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 9 No. 3, pp. 3514-3531.

Alter, S. (2008a), "Service system fundamentals: work system, value chain, and life cycle", *IBM Systems Journal*, Vol. 47 No. 1, pp. 71-85.

Alter, S. (2008b), "Defining information systems as work systems: implications for the IS field. European", *Journal of Information Systems*, Vol. 17 No. 5, pp. 448-469.

Alter, S. (2010), "Viewing systems as services: a fresh approach in the IS field", *Communications of the Association for Information Systems*, Vol. 26 No. 1, p. 11.

Alter, S. (2013), "Work system theory: overview of core concepts, extensions, and challenges for the future", *Journal of the Association for Information Systems*, Vol. 14 No. 2, pp. 72-121, doi: 10.17705/1jais.00323.

BMC (2016), "ITIL information security management", available at: https://www.bmc.com/blogs/itil-information-security-management// (accessed 10 September 2020).

Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. and Materne, S. (2022), "Cyber risk and cybersecurity: a systematic review of data availability", *The Geneva Papers on Risk and Insurance - Issues and Practice*, Vol. 47, pp. 698-736, doi: 10.1057/s41288-022-00266-6.

Culot, G., Nassimbeni, G., Podrecca, M. and Sartor, M. (2021), "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda", *The TQM Journal*, Vol. 33 No. 70, pp. 76-105.

Dalal, R.S., Howard, D.J., Bennett, R.J., Posey, C., Zaccaro, S.J. and Brummel, B.J. (2022), "Organizational science and cybersecurity: abundant opportunities for research at the interface", *Journal of Business Psychology*, Vol. 37, pp. 1-29, doi: 10.1007/s10869-021-09732-9.

De Smet, A. and and Mysore, M. (2020), "Reimagining the postpandemic workforce", available at: https://www.mckinsey.com/business-functions/organization/our-insights/reimagining-the-postpandemic-workforce (accessed 20 October 2020).

Deloitte (2019), "Through the risk lens, the future belongs to the prepared", available at: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/Through%20the%20risk%20lens.pdf (accessed 15 October 2020).

Deloitte (2020), "COVID-19's impact on cybersecurity", available at: https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact cybersecurity.html#:~:text=From%20our%20Cyber%20Intelligence%20Centre,infected%20personal%20computers%20and%20phones (accessed 18 October 2020).

Dixon, W. and Singh, M. (2020), "COVID-19 has disrupted cybersecurity, too – here's how businesses can decrease their risk", available at: https://www.weforum.org/agenda/2020/07/covid-19-cybersecurity-disruption-cyber-risk-cyberattack- business-digital-transformation/ (accessed 28 September 2020).

Dwivedi, Y.K., Ismagilova, E.D., Hughes, L.D., Carlson, J., Filierie, R., Jacobson, J., Jain, V., Karjaluoto, H., Kefi, H., Krishen, A.S., Kumar, V., Rahman, M.M., Raman, R., Rauschnabel, P.A., Rowley, J., Salo, J., Tran, G.A. and Wang, Y. (2021), "Setting the future of digital and social media marketing research: perspectives and research propositions", *International Journal of Information Management*, Vol. 59, doi: 10.1016/j.ijinfomgt.2020.102168.

Fonseca-Herrera, O.A., Rojas, A.E. and Florez, H. (2021), "A model of an information security management system based on NTC-ISO/IEC 27001 standard", *IAENG International Journal of Computer Science*, Vol. 48 No. 2, pp. 213-222.

Forum, W.E. (2020), "Wild wide web-consequences of digital fragmentation", available at: https://reports.weforum.org/global-risks-report-2020/wild-wide-web/ (accessed 19 October 2020).

Gordon, L.A., Loeb, M.P. and Zhou, L. (2020), "Integrating cost–benefit analysis into the NIST cybersecurity framework via the Gordon–Loeb model", *Journal of Cybersecurity*, Vol. 6 No. 1, doi: 10.1093/cybsec/tyaa005.

Hitchcox, Z. (2020), "Limitations of cybersecurity frameworks that cybersecurity specialists must understand to reduce cybersecurity breaches", *Colorado Technical University ProQuest Dissertations Publishing*, ProQuest LLC, Ann Arbor, Michigan.

Ibrahim, A., Valli, C., McAteer, I. and Junaid, C. (2018), "A security review of local government using NIST CSF: a case study", *The Journal of Supercomputing*, Vol. 74, pp. 5171-5186, doi: 10.1007/s11227-018-2479-2.

Invensis (2020), "An overview of information security management in ITIL", available at: https://www.invensislearning.com/articles/itil/overview-of-information-security-management (accessed 24 October 2020).

Ismail, N. (2018), "Global cybercrime economy generates over $1.5TN, according to new study", available at: https://www.information-age.com/global-cybercrime-economy- generates-over-1-5tn-according-to-new-study-123471631/ (accessed 10 October 2020).

Jang-Jaccard, J. and Nepal, S. (2014), "A survey of emerging threats in cybersecurity", *Journal of Computer and System Sciences*, Vol. 18 No. 5, pp. 973-993.

Jones, J. (2018), "An executive's guide to cyber risk economics", *Spokane WA: RiskLens*, available at: https://www.risklens.com/hubfs/uploads/2019/04/RiskLens-eBook_An-Executives-Guide-to-Cyber-Risk-Economics.pdf.

Jones, R., Suoranta, M. and Rowley, J. (2013), "Strategic network marketing in technology SMEs", *Journal of Marketing Management*, Vol. 29 Nos 5, pp. 671-697.

Kaspersky (2020), "What is cyber security?", available at: https://www.kaspersky.com/resource-center/definitions/cyber-security (accessed 28 September 2020).

Kerner, S.M. (2022), "34 cybersecurity statistics to Lose sleep over in 2022", *TechTarget*, available at: https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020/ (accessed 17 July 2022).

Kitsing, M. (2017), "Internet banking as a platform for E-government", *paper Presented at the Annual International Conference on Innovation and Entrepreneurship (IE 2017)*, Singapore: Estonia Business School available at: https://www.researchgate.net/profile/Meelis-Kitsing/publication/321673381_Internet_Banking_as_a_Platform_for_EGovernment/links/5e09d251a6fdcc283748b1d7/Internet-Banking-as-a-Platform-for-E-Government.pdf (accessed 15 October 2020).

Kobielus, J. (2020), "Social engineering hacks weaken cybersecurity during the pandemic", available at: https://www.infoworld.com/article/3565197/social-engineering-hacks-weaken-cybersecurity-during-the-pandemic.html (accessed 12 October 2020).

Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C. and 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 and Security*, Vol. 105, pp. 0167-4048.

Morrow, S. and Crabtree, T. (2019), "The future of cybercrime and security: threat analysis, impact assessment and mitigation strategies 2019-2024", available at: https://www.juniperresearch.com/researchstore/key-vertical-markets/cybercrime-cybersecurity-research-report (accessed 18 October 2020).

National Institute of Standards and Technology (NIST) (2014), "Framework for improving critical infrastructure cybersecurity", available at: https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf (accessed 20 October 2020).

National Cyber Security Alliance (NCSA) (2018), "It's everyone's job to ensure online safety at work", available at: https://staysafeonline.org/press-release/everyones-job-ensure-online-safety-work/ (accessed 20 October 2020).

National Information Technology Development Agency (NITDA) (2019), "Nigeria national cybersecurity framework", available at: https://nitda.gov.ng/wp-content/uploads/2020/03/NIGERIA-NATIONAL-CS-FRAMEWORK-.pdf (accessed 17 October 2020).

Pawar, S. and Palivela, H. (2022), "LCCI: a framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs)", *International Journal of Information Management Data Insights*, Vol. 2 No. 1, doi: 10.1016/j.jjimei.2022.100080.

Perwej, Y., Abbas, S.Q., Dixit, J.P., Akhtar, N. and Jaiswal, A.K. (2021), "A systematic literature review on the cyber security", *International Journal of Scientific Research and Management (IJSRM)*, Vol. 9 No. 12, pp. 669-710.

Petkov, D. and Petkova, O. (2008), "The work system model as a tool for understanding the problem in an introductory IS project", *Information Systems Education Journal*, Vol. 6 No. 21, pp. 1-12.

Pitchkites, M. (2022), "Top cyber security statistics, facts and trends in 2022", *Cloudwards*, available at: https://www.cloudwards.net/cyber-security-statistics/ (accessed 17 July 2022).

Poehlmann, N., Caramancion, K.M., Tatar, I., Li, Y., Barati, M. and Merz, T. (2021), "The organizational cybersecurity success factors: an exhaustive literature review", in Daimi, K., Arabnia, H.R., Deligiannidis, L., Hwang, M.S. and Tinetti, F.G. (Eds), *Advances in Security, Networks, and Internet of Things. Transactions on Computational Science and Computational Intelligence. Springer, Cham*. doi: 10.1007/978-3-030-71017.

Risk Based Security (RBS) (2019), "Number of records exposed up 112% in Q3", available at: https://www.riskbasedsecurity.com/2019/11/12/number-of-records-exposed-up-112/ (accessed 16 October 2020).

Rouse, M. (2020), "What is cybersecurity? Everything you need to know", available at: https://searchsecurity.techtarget.com/definition/cybersecurity (accessed 18 October 2020).

Sheehan, B., Murphy, F., Kia, A.N. and Kiely, A. (2021), "A quantitative bow-tie cyber risk classification and assessment framework", *Journal of Risk Research*, Vol. 24 No. 12, pp. 1619-1638.

Spohrer, J., Maglio, P.P., Bailey, J. and Gruhl, D. (2007), "Steps toward a science of service systems", *IEEE Computer*, Vol. 40 No. 1, pp. 71-77.

Taylor, H. (2021), "What are cyber threats and what to do about them", available at: https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/ (accessed 19 October 2021).

Thomas, G., Botha, R.A. and vanGreunen, D. (2015), "Understanding the problem of coordination in a large-scale distributed environment from a service lens perspective- A case of the South African public sector e-administration criteria for coordination support", *Government Information Quarterly*, Vol. 32 No. 4, pp. 526-538, doi: 10.1016/j.giq.2015.08.002.

Vargo, S.L. and Lusch, R.F. (2004), "The four service marketing myths", *Journal of Service Research*, Vol. 6 No. 4, pp. 324-335.

Weil, T. and Murugesan, S. (2020), "IT risk and resilience—cybersecurity response to covid-19", *IT Professional*, Vol. 22 No. 3, pp. 4-10, doi: 10.1109/MITP.2020.2988330.

Wilkinson, I.C. (2020), "Cybersecurity using risk management strategies of U.S. Government health organizations", Walden Dissertations and Doctoral Studies, Walden University, Minneapolis.

Williams-Banta, P.E. (2019), "Security technology and awareness training; do they affect behaviors and thus reduce breaches?", ProQuest LLC, Ph.D. Dissertation, Northcentral University, ProQuest LLC, San Diego.

Further reading

Cazemier, J.A., Overbeek, P. and Peters, L. (2010), *Information Security Management with ITIL V3*, Van Haren Publishing, Netherlands, NL.

Gnat, R. (2020), "ITIL 4 Information security and risk management practices: embedding safety culture and behavior", available at: https://www.axelos.com/news/blogs/march-2020/itil-4-information-security-and-risk-management (accessed 12 October 2020).

Spohrer, J., Anderson, L.C., Pass, N.J., Ager, T. and Gruhl, D. (2008), "Service science", *Journal of Grid Computing*, Vol. 6, pp. 313-324.

(The Appendix follows overleaf)

Appendix

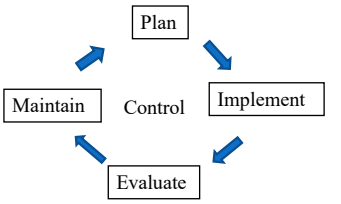

Figure A1.
ITIL Information Security management framework activities

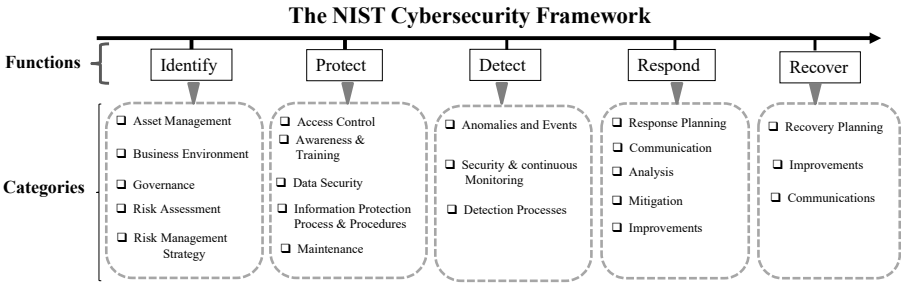

Figure A2.
The NIST cybersecurity framework

Dimension	Customer Context?	Provider Context?	Problem indication	Risk level/ Impact	Proposed Solution/ requirement	Solution Status	Result indication	comment
strategy								
Organizational Structure/configuration								
processes and activities								
Participants								
Technologies								
Services								
Product								
Environment								
Interaction								
Information								
Knowledge								
Infrastructure								
Applications								
Funds								

Table A1.
Resource/capacity template for probing into the cybersecurity service system

Corresponding author
Godwin Thomas can be contacted at: godwinthomas@gmail.com