Integrating Enterprise Architecture into Cybersecurity Risk Management in Higher Education

Mafika Nkambule[1], Joey Jansen van Vuuren[1] and Louise Leenen[2]
[1]Tshwane University of Technology, Pretoria, South Africa
[2]University of the Western Cape and CAIR, Cape Town, South Africa

nkambulemw@tut.ac.za
Jansenvanvuurena1@tut.ac.za
lleenen@uwc.ac.za

Abstract: Cybercriminals constantly seek new methods to infiltrate a company's defences, making cybersecurity investments essential. Enterprise architecture (EA) provides a systematic risk detection and mitigation process by emphasising the interdependencies between systems, data, processes, people, and other factors. This paper provides a comprehensive approach, also referred to as a process, based on EA to assist African universities in developing a comprehensive cybersecurity plan. The EA process comprises four pillars: business architecture, data architecture, application architecture, and technology architecture. African universities can develop a comprehensive cybersecurity strategy using an EA approach in cybersecurity to achieve institutional goals and objectives. The potential attack surface comprises isolated EA components and their interconnections. This article comprehensively examines various EA processes such as business, information, application, and technology architecture. These processes are carefully analysed to evaluate the organisational structures and uncover opportunities to enhance security protocols. Additionally, we delve deep into abstract security patterns, seeking to cultivate an environment of trustworthiness within complex systems. Our research findings underscore the significant potential within African higher education institutions. By embracing a model-based approach to risk analysis and mitigation, these institutions can fortify their cybersecurity defences and bolster their capabilities to ensure uninterrupted business operations and enhance overall resilience in the face of evolving security challenges. When we combine EA and information security (ICS), we uncover many vulnerabilities malicious actors might exploit. By embracing a holistic EA-based methodology, institutions can craft and implement robust security protocols to safeguard their components and connections. Leveraging EA, our proposed integrated approach aims to forge a comprehensive cybersecurity risk management strategy tailored to the African higher education sector. This strategy seeks to facilitate the identification of critical elements and their intricate interrelationships, thus formulating an effective defence strategy against potential cyber threats. The synergy between EA and cybersecurity within African universities promises to elevate cybersecurity practices, ensure uninterrupted business operations, and fortify the continent's resilience.

Keywords: Enterprise architecture, Cybersecurity risk management, Higher education, Integration, Framework

1. Introduction

1.1 Background

Cyber threats have evolved in complexity and frequency in today's interconnected digital landscape. With their vast resources, universities have become enticing targets for cybercriminals, who covet assets like trademarks, student data, and collaborative research ventures (Lallie et al., 2023). Within the academic realm, cybersecurity presents a multifaceted challenge, as it demands the perpetual preservation of digital resources' confidentiality, integrity, and accessibility, all while contending with limited resources and a diverse user base.

Despite notable advancements in cybersecurity, a gap persists between the prevailing security needs and the broader institutional framework of our modern world. It has become increasingly imperative for higher education institutions to align their cybersecurity initiatives with their overarching goals, systems, and procedures (Dlamini et al., 2011). By establishing this alignment, security processes can seamlessly integrate into an organisation's operational framework, taking on a proactive role.

EA, a comprehensive approach to managing a corporation Maulana, Azmi and Phon (2023), may hold the key to bridging the existing gap in cybersecurity handling. EA provides a holistic view of an organisation, encompassing its processes, procedures, data flows, and technological infrastructure. Institutions seeking to enhance their risk management capabilities and adapt to changing circumstances would be well-advised to merge their EA and cybersecurity strategies. This integration can lead to more robust and proactive security measures in an ever-evolving digital landscape.

1.2 Purpose and Relevance of the Study

The central aim of this research is to delve into the prospective advantages associated with the incorporation of EA processes into a comprehensive cybersecurity risk management framework tailored specifically for higher education institutions. Given the alarming surge in cybersecurity attacks and the emergence of formidable vulnerabilities within the realm of higher learning institutions—occasionally driven by personal interests and gains, as outlined by Lallie et al. (2023), there exists an urgent imperative to formulate a strategy. This strategy must not only effectively tackle the operational challenges posed by cybersecurity threats but also harmoniously align with the holistic academic and research objectives of these institutions, from start to finish.

This research work is guided by the following pivotal goals:

- **Deep Dive Analysis:** We aim to assess the current cybersecurity frameworks, and pinpoint both shortcomings and avenues for enhancement.
- **EA and Cybersecurity Synergy:** The study seeks to understand how integrating EA can act as a bedrock in formulating a malleable yet steadfast cybersecurity risk management framework. This encompasses assessing the convergence of institutional objectives, technological underpinnings, data pathways, and protective mechanisms.
- **Blueprint Creation:** Our ambition is to curate an actionable guideline based on EA principles, crafted for academic institutions. This blueprint is envisioned to equip institutions with a strategic trajectory to amplify their digital protection, ensure operational consistency, and match protective endeavours with the broader institutional vision.

In pursuing these objectives, the study hopes to contribute significantly to the discourse on cybersecurity in higher education, offering institutions a nuanced strategy that goes beyond traditional, siloed approaches to cyber risk management. By fostering a deeper integration of EA and cybersecurity, this research aspires to pave the way for a more secure, resilient, and adaptive digital environment within academia.

2. Literature Review

2.1 Cybersecurity in Higher Education

Institutions of higher learning are increasingly becoming main targets for cyber criminals due to their huge repositories of student data, intellectual property, and collaborative research projects (Nasir et al., 2023). There is always that huge obligation to ensure the confidentiality, integrity, and availability of digital resources, paired with budget constraints and a diverse user environment. This makes the task of cybersecurity in the academic environments an extremely difficult undertaking. According to Eltahir and Ahmed (2023), the move for institutions of higher learning to go online has made them even more vulnerable to cyber criminals.

2.2 The Role of Enterprise Architecture in Cybersecurity

There are many definitions of enterprise architecture, but this study adopted the definition by the Pereira and Sousa (2005), who defines EA as the process by which organizations standardize and organize IT infrastructure to align with business goals. EA, by design, looks at all aspects of an organisation, and these various aspects are what attackers use to strike. An EA based approach, therefore, offers a promising approach to bridging the gap between cybersecurity measures and the overall institutional architecture.

EA lays out a structured and comprehensive blueprint of an organisation's operations, encompassing its goals, processes, information flows, and technological infrastructure (Kotusev et al., 2023). By making sure EA is integrated with cybersecurity measures, there is an opportunity to create a unified, resilient, and adaptive security architecture that is responsive to threats and aligns with the institution's goals and changing landscape.

2.3 Existing Frameworks and Their Limitations

It is important to note that numerous cybersecurity risk management frameworks are used across all industries, including higher eductaion. While each of these frameworks offers its own set of guidelines and practices, they often fall short in synchronizing seamlessly with the comprehensive objectives, infrastructure, and day-to-day workings of organisations. Many of these models typically react to issues post-occurrence, rather than embedding themselves organically into the core strategies of institutions.

While there is undoubtedly a plethora of frameworks available, we first present a unique overview of the various cybersecurity frameworks that are most widely recognized and utilized across different industries as identified an documented by (Taherdoost, 2022). For a clearer comparison, we have encapsulated our observations in the table below, contrasting these mainstream frameworks against our innovative approach. Through the integration of EA with conventional cybersecurity strategies, there is a potential for a more harmonized, robust, and agile security structure, one that not only anticipates threats but also aligns perfectly with an institution's evolving objectives and landscape.

Table 1: Cybersecurity Frameworks Comparison

#	SOURCE	EXISTING FRAMEWORK	COMPARING EXISTING FRAMEWORKS WITH OUR PROPOSED EA-BASED APPROACH TO DEVELOP A CYBERSECURITY RISK MANAGEMENT FRAMEWORK
1	(White & Sjelin, 2022)	**NIST Cybersecurity Framework (CSF)**	While the NIST CSF provides a detailed set of cybersecurity practices, its primary focus is on managing and reducing cybersecurity risk. Using the EA approach, with the comprehensive overview of business, data, application, and technology, inherently ties cybersecurity to the organization's strategic objectives.
2	(Humphreys, 2016)	**ISO/IEC 27001**	ISO/IEC 27001 is largely about defining controls based on a risk assessment. EA, on the other hand, allows for a more holistic risk assessment that looks at risks from multiple dimensions - business processes, data flows, and applications.
3	(Groš, 2021)	**CIS Critical Security Controls**	CIS controls are prescriptive and are designed to provide a set of actions for cyber defence. In contrast, the EA approach is inherently customizable, designed to adapt to the unique needs and structures of individual organizations.
4	(IGNAT, 2022)	**FAIR (Factor Analysis of Information Risk)**	FAIR is primarily a quantitative risk analysis model, focusing heavily on the financial implications of cybersecurity risks. The EA approach offers a broader view that aligns cybersecurity with business goals and objectives.
5	(Ahmed et al., 2022)	**MITRE ATT&CK**	Focuses primarily on the tactics, techniques, and procedures used by adversaries against organizations. While it's a comprehensive knowledge base of adversary behaviour, it doesn't inherently provide an overall organizational strategy., which the EA approach offers.
6	(Morse & Raval, 2008)	**PCI DSS (Payment Card Industry Data Security Standard)**	PCI DSS is specific to payment card security. While it's crucial for companies dealing with card payments, it's narrow in scope. In contrast, an EA-based approach offers a more holistic view, covering all business, data, application, and technology domains.
7	(De Haes et al., 2013)	**COBIT (Control Objectives for Information and Related Technologies)**	Both COBIT and EA offer governance structures, but the EA-based approach has a core focus on aligning cybersecurity strategies with business objectives.
8	(Burkett, 2012)	**SABSA (Sherwood Applied Business Security Architecture)**	While SABSA is an enterprise security architecture framework, it heavily focuses on security. The EA-based approach ensures a balanced representation of business, data, application, and technology domains, emphasizing their co-dependency.
9	(Sharkov, 2020)	**C2M2 (Cybersecurity Capability Maturity Model)**	C2M2 is designed to measure the maturity of an organisation's cybersecurity capabilities. An EA-based approach, while valuing maturity measurements, also emphasises the holistic alignment of all cybersecurity measures with the business's overarching goals.

While each of the listed frameworks provides important guidelines, tools, and metrics in specific areas of cybersecurity and governance, the proposed EA-based approach stands out due to its holistic perspective, adaptability, and emphasis on aligning cybersecurity with overarching organizational goals. It provides a comprehensive process that bridges the multifaceted dimensions of an organization, making it a potentially valuable addition to the cybersecurity landscape.

3. The Importance of Cybersecurity Risk Management in African Higher Education Institutions

3.1 Current Cyber Threat Landscape

While it is acknowledged that cybersecurity challenges are a global phenomenon affecting institutions worldwide, this study specifically narrows its focus to the African context. In particular, African higher education institutions face a growing threat from cyber adversaries due to their increasing reliance on digital technologies (Eltahir & Ahmed, 2023). The threat landscape constantly evolves, with cybercriminals using sophisticated techniques to gain unauthorised access to sensitive data. The most common types of cyber threats include phishing attacks, malware, ransomware, and denial-of-service attacks (Rana & Sharma, 2023). These threats can result in data breaches, financial losses, and reputational damage to institutions.

3.2 Unique Challenges Faced by African Institutions

As indicated in section 3.1 above, this is a challenge for institutions across the globe. To ensure the effectiveness of the proposed framework, we narrowed our scope to focus only on challenges prevalent to African universities. According to Rana and Sharma (2023), African higher education institutions face unique challenges in implementing effective cybersecurity measures. These challenges include limited financial resources, inadequate cybersecurity expertise, and a lack of awareness among users. The diverse user environment, including students, faculty, and staff, makes implementing a unified cybersecurity strategy difficult (Kayode-Ajala, 2023). The lack of a comprehensive legal framework for cybersecurity in many African countries also poses a challenge (Bouke et al., 2023).

To address these challenges, it is essential for African higher education institutions to prioritise cybersecurity and invest in robust cybersecurity measures (Kayode-Ajala, 2023). It is for this reason that the implementation of an EA-based approach is proposed, to align cybersecurity measures with academic institutions' holistic objectives, infrastructure, and operations. By integrating EA with cybersecurity measures, institutions can create a unified, resilient, and adaptive security architecture that is responsive to threats and aligns with the institution's goals and changing landscape.

4. Understanding Enterprise Architecture

4.1 Definition and Components of EA

EA, in its essence, represents a meticulously detailed and all-encompassing roadmap of an organization's operations, entailing not just its objectives and processes but also the intricate flow of information and the underpinning technological infrastructure (Rozas et al., 2020). The beauty of EA lies in its ability to paint a panoramic portrait of an organization, granting stakeholders the insight to decipher the intricate symphony of components working in tandem to fulfil its ambitions. In concurrence with The Open Architecture Group's (TOGAF) insights, the facets of EA encompass a wide spectrum of elements (Maulana, Azmi, & Arshah, 2023) as elegantly illustrated in the visual representation provided in Figure 1 below:

- Business Architecture: Describes the organisation's business strategy, goals, processes, and organisational structure.
- Information Architecture: Describes the organisation's information assets, data flows, and information systems (Taherdoost, 2022).
- Application Architecture: Describes the organisation's software applications, interdependencies, and alignment with business objectives.
- Technology Architecture: Describes the organisation's hardware, network, and infrastructure components.

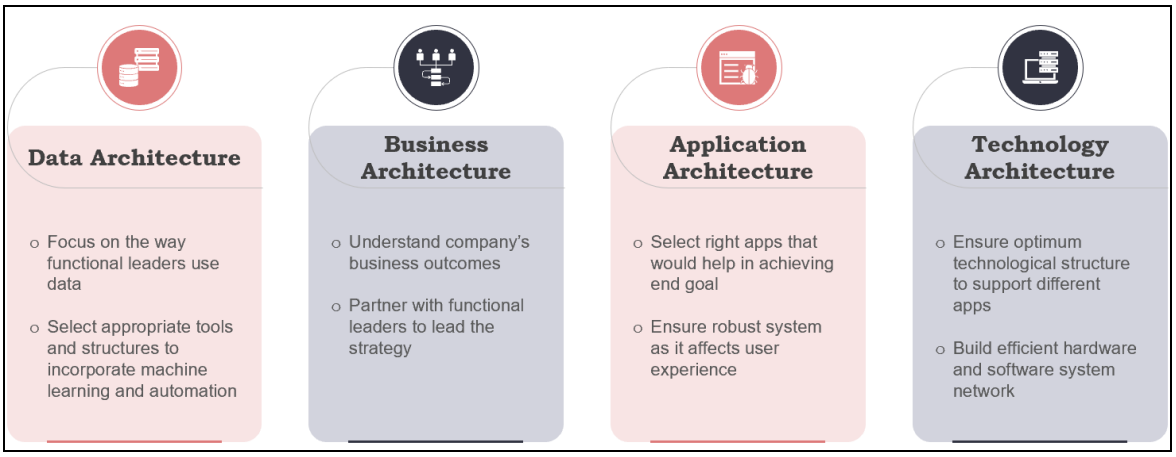

Figure 1: Enterprise Architecture Domains

5. Proposed EA-Based Cybersecurity Approach for Higher Education

For the distinctive challenges African academic institutions face in implementing robust cybersecurity controls, we propose a cybersecurity blueprint based on EA processes. This blueprint is specially proposed for the academic institutions, aspiring to synchronize cybersecurity initiatives with the encompassing goals, foundation, and functioning of these educational bodies in Africa and beyond. Figure 2 below depicts the elements to be covered within each domain of EA in relation to cybersecurity. The suggested blueprint encompasses these core elements:

5.1 EA Approach: Adopting an Organisational Architecture within Security Governance

Within the dynamic landscape of academic institutions in Africa, the fusion of organizational architecture with the realm of security governance takes on paramount significance. At its core, this fusion entails the meticulous crafting of a precisely tailored governance framework, purpose-built for the astute management of cybersecurity risks within the unique confines of higher education environments, as eloquently articulated by (Gloria Appiah, 2020).

- **Role Definition and Allocation:** A crucial initial step is to demarcate clear roles within the institution's cybersecurity landscape. By understanding who is responsible for what, institutions can foster both accountability and clarity. From frontline IT staff to top-tier management, each stakeholder's role in the cybersecurity matrix needs clear delineation.
- **Policy and Procedural Process:** Once roles are defined, the next step is to develop a comprehensive set of policies and procedures. These aren't just rulebooks but are dynamic guides that evolve with the changing cyber threat landscape. They act as the institution's first line of defence, guiding actions and setting the standards for cybersecurity measures.
- **Regulatory Adherence and Compliance:** Higher education institutions often deal with a plethora of sensitive data, making regulatory compliance non-negotiable. This facet ensures that the institution isn't just following internal guidelines but is also in line with regional, national, or international cybersecurity regulations, as applicable.
- **Risk Management Aligned with Institutional Vision:** The beauty of a tailored risk management strategy lies in its alignment with the broader goals of the institution. It's not just about countering threats but doing so in a way that seamlessly blends with the institution's educational, research, and administrative objectives. This ensures that while risks are mitigated, the institution's primary functions and aspirations aren't hampered.

Fundamentally, this element revolves around the conception of a resilient and adaptable framework, one in which cybersecurity seamlessly weaves itself into the very fabric of the institution, transcending the status of an afterthought.

5.2 EA Approach: Using Business Architecture for Security Strategy

At the heart of each forward-thinking educational establishment lies the essential quest to harmonize its business ambitions with the domain of cybersecurity pursuits. In this paper, we embark on a deep and

enlightening odyssey through this intricate interweaving, as thoughtfully illuminated by the discerning perspectives (Choudhuri et al., 2023).

- **Asset and Data Prioritization:** Recognizing and ranking the institution's pivotal assets and data repositories is a foundational step. It's about discerning what's at the core of the institution's operations and what would have the most profound impact if compromised.
- **Strategising with Vision:** Rather than adopting a one-size-fits-all approach, crafting a security plan that mirrors the institution's broader aspirations is crucial. Such alignment ensures that security measures don't just shield but also bolster the institution's growth trajectory.
- **Integration into Business Processes:** Cybersecurity is not an isolated domain but rather a pervasive one. It's essential to weave these protective measures seamlessly into the institution's everyday business activities, ensuring continuity and safety without hampering functionality.

In summary, this segment underscores the necessity of a holistic approach where cybersecurity is not an appendage but is integrally rooted in the institution's business architecture, promoting both growth and safety.

5.3 EA Approach: Using Information Architecture for Data Security

Within the expansive realm of academic institutions, safeguarding information assets and data stands paramount. This section delves into the nuances of this integration, ensuring a seamless blend of structure and protection.

- **Policy Formulation and Classification:** Before diving into protective measures, it's essential to have a structured approach to data. Creating clear policies and procedures aids in classifying data based on its sensitivity and relevance, ensuring each data subset gets its due attention.
- **Access Regulation and Retention:** Not all data should be accessible to everyone. Establishing rigorous access controls ensures that only authorized personnel can access specific data sets. Moreover, data retention policies help in determining the lifespan of data, ensuring obsolete or non-essential information doesn't clog the system or pose unnecessary risks.
- **Technical Fortifications:** While policies create a protective process, technical tools are the actual shields. By deploying state-of-the-art encryption protocols, robust firewalls, and proactive intrusion detection systems, institutions can defend against the ever-evolving threats of data breaches.

In essence, this segment emphasizes a layered approach to data protection. By intertwining robust information architecture with cutting-edge security protocols, institutions can ensure their data remains both organized and impenetrable.

5.4 EA Approach: Using Application Architecture for Software Security

In the digital fabric of modern educational institutions, the security of software applications holds a prominent position. This section illuminates the intricate balance between application structure and its subsequent protective layers.

- **Guided Software Lifecycle:** Every software application in the institution's arsenal undergoes a lifecycle from inception to decommission. Crafting meticulous policies and procedures ensures that each phase, be it development, testing, or deployment, is executed under a lens of security. This proactive approach ensures potential pitfalls are addressed long before they become threats.
- **Upholding Software Integrity:** It's not just about creating software; it's about creating software that's robust and resistant. Adopting secure coding practices right from the get-go ensures that the software's foundation is resilient. Regular vulnerability scans then ensure that this foundation remains uncompromised, catching potential weaknesses before they're exploited.
- **Proactive Defence Mechanisms:** Beyond just looking for weaknesses, penetration testing takes a more aggressive approach, simulating cyberattacks to test the software's defences. This "offensive defence" strategy gives institutions a clearer picture of potential real-world threats.

In summary, this segment champions a multi-faceted approach to software security. By harmonizing well-defined application architecture with advanced security methodologies, institutions can rest assured that their software arsenal is both functional and fortress-like.

5.5 EA Approach: Using Technology Architecture for Infrastructure Security

As academic institutions increasingly intertwine with the digital realm, ensuring the safety of their technological backbone becomes paramount. This section shines a spotlight on the delicate orchestration between technological design and its protective armoury.

- **Blueprinting Security Infrastructure:** The essence of any secure technological infrastructure starts with its blueprint. Drafting comprehensive policies and procedures for aspects like network security, device management, and system administration lays the groundwork for a fortified infrastructure. It's akin to building a structure with security ingrained in its very architecture.
- **Fortifying Network Structures:** With the ever-increasing complexity of networks, a strategic approach to their security becomes crucial. Network segmentation, for instance, helps in isolating different parts of the institution's network, thereby minimizing potential breach impact. Such an approach ensures that if one segment faces issues, the entire network doesn't come crashing down.
- **Strengthening Access and Oversight:** While the institution's technological assets are vital, it's equally essential to regulate who has access to them. Rigorous access control mechanisms act as gatekeepers, ensuring only authorized personnel can interact with critical systems. Coupled with real-time monitoring, institutions can maintain a vigilant eye, ensuring anomalies are detected and dealt with swiftly.

To encapsulate, this segment emphasizes the harmony between technological structuring and its protective layers. By fusing meticulous technology architecture with state-of-the-art security mechanisms, academic institutions can cultivate a digital environment that's as robust as it is secure.

Business Architecture		**Data Architecture**	
Business Strategy Alignment	**Plan**	Data Classification	**Plan**
Business Process Analysis	**Monitor**	Data Access Control	**Identify**
Cybersecurity Governance	**Review**	Encryption	**Detect**
User Awareness Training		Data Retention & Disposal	**Protect**
Compliance & Regulations		Backup & Recovery	**Recover**
Incident Response Plan		Data Leak Prevention	**Review**
Vendor & Third-party Management		Database Security	
Business Continuity & Disaster Recovery		Data Integrity Checks	
Resource Allocation		Audit Trails	
Stakeholder Communication Plan		Data Privacy Regulations	
Information Architecture		**Technology Architecture**	
Secure Development Lifecycle	**Plan**	Network Segmentation	**Plan**
Application Vulnerability Assessment	**Identify**	Firewall Implementation	**Identify**
Patch Management	**Detect**	Intrusion Detection &Prevention(IDPS)	**Detect**
Access Controls	**Protect**	Endpoint Protection	**Protect**
Application Performance Monitoring	**Recover**	Physical Security	**Recover**
API Security	**Review**	Network Monitoring & Logging	**Review**
Code Review		Access Controls	
End-point Security		Cloud Security	
Malware & Antivirus Scanning		Virtualization Security	
Application Training		Wireless Network Security	
INTEGRATE WITH PROPRIETORY FRAMEWORKS			

Figure 2: Proposed EA-based Cybersecurity Process

The process being proposed involves using all EA domains, as depicted in figure 2 above, to guide the design and implementation of strategies and security controls within higher education institutions in South Africa. Incorporating these diverse components within an EA-based cybersecurity blueprint empowers academic institutions to craft a holistic, robust, and agile security process. Such an architecture not only stands firm against evolving cyber threats but also seamlessly dovetails with the institution's overarching objectives and the ever-shifting educational environment. By fostering this symbiotic relationship between cybersecurity and

institutional aspirations, establishments can fortify their digital frontiers while staying in tune with their evolving operational paradigms. The proposed process can also be used with any other framework of choice.

6. The Role of Relationships Across all EA Components

EA provides a structured and comprehensive approach to aligning cybersecurity measures with an organisation's holistic objectives, infrastructure, and operations (Trad, 2023). Relationships between different components of EA are critical in identifying interconnections and vulnerabilities that cyber attackers can exploit. The following are the roles of relationships in EA components:

6.1 Identifying Interconnections and Vulnerabilities

EA serves as a keen eye for uncovering the intricate interplay among diverse facets of an organization's operational machinery, affording stakeholders a profound understanding of the collaborative efforts that steer the organization toward its goals, as elucidated by (Trad, 2023). This revelation of interconnections not only unveils the inner workings but also unveils potential points of vulnerability that cunning cyber criminals might seek to exploit.

To illustrate, should a vulnerability rear its head within one facet of an organization's operations, its repercussions can reverberate through the entire ecosystem, giving rise to a cascade effect that could culminate in a far-reaching security breach. Such is the power of comprehending these interconnections, as revealed through the lens of EA.

6.2 Analysis of Potential Attack Surfaces

EA lends its capability in delving into the realm of prospective attack surfaces, adeptly identifying the pivotal assets, integration between assets, and data that demand a vigilant shield of protection, as elucidated by (Masi et al., 2023). Through the intricate cartography of an organization's intricate processes and the graceful meandering of information, EA unfolds its capabilities in uncovering potential junctures of vulnerability and gracefully choreographing contingency plans. This comprehensive analysis emerges as a strategic compass, empowering organizations to judiciously prioritize their cybersecurity endeavours and efficiently allocate precious resources.

6.3 The Importance of Relationship Analysis in Cybersecurity

Relationship analysis is critical in cybersecurity risk management as it helps identify potential vulnerabilities and attack surfaces (Walter et al., 2023). Understanding the relationships between different components of an organisation's operations makes it possible to develop a comprehensive and integrated cybersecurity strategy that aligns with the organisation's goals and objectives. This approach ensures that cybersecurity measures are not just reactive but integrated into institutional operations' foundational structure. The diagram in Figure 3 below gives a view of the comprehensive nature of elements covered by EA.

When we decode the symbiotic ties between diverse operational components, it empowers organizations to draft a cybersecurity blueprint that is not merely reactionary. Instead, it becomes an integral part of the organization's foundational matrix, harmonizing with its overarching aspirations. The accompanying figure 3 (Archimate, 2000), drawing inspiration from the comprehensive tenets laid out by EA further explains this intertwined nature.

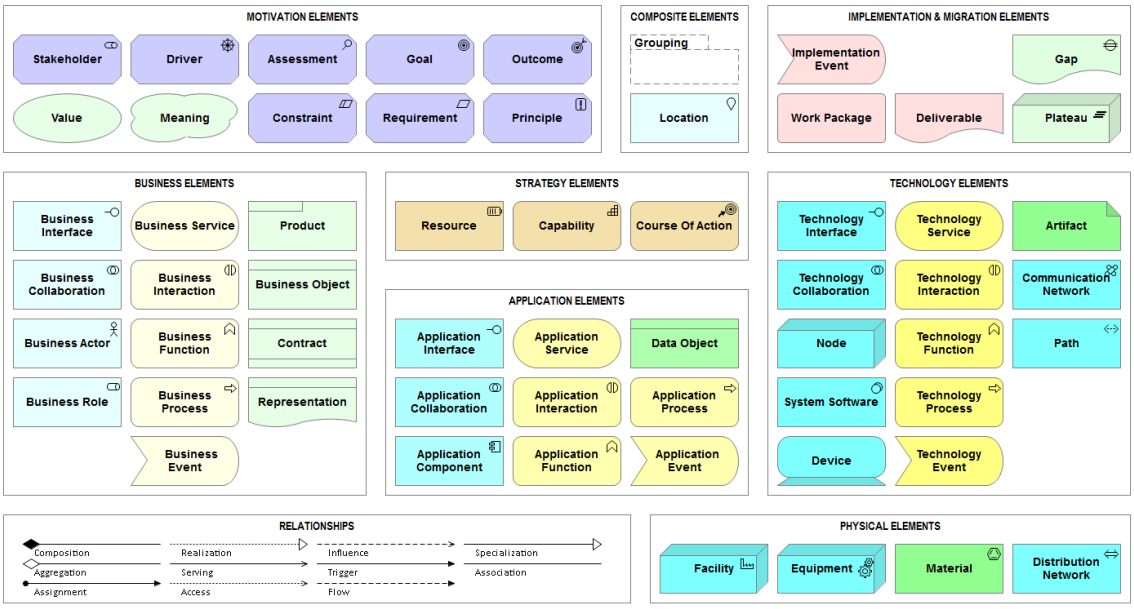

Figure 3: EA components – (Archimate, 2000),

The relationship within all EA elements can help us spot weak points that cunning attackers might want to exploit. By closely looking at these relationship and possible threats, organizations can better plan their online safety measures. This means they will not just respond to dangers, but they will also strengthen their online spaces in a way that fits their main goals.

6.4 Implications for Higher Education Institutions in Africa

We believe the EA-driven cybersecurity approach brings profound implications for universities, especially African higher education institutions, sparking a transformative shift. By aligning cybersecurity strategies with the intricate tapestry of academic goals, infrastructure, and operations, this approach promises heightened resilience against looming cyber threats. Moreover, it serves as the linchpin for seamless business continuity while harmonizing cybersecurity efforts with the overarching institutional vision.

Yet, the EA approach extends its reach further, offering a potent response to unique challenges facing African institutions—constraints in finances, a shortage of cybersecurity expertise, and pervasive user awareness gaps. Furthermore, it aids in navigating the complex legal landscape surrounding cybersecurity in many African nations, ensuring compliance with comprehensive legal frameworks in this domain.

7. Conclusion

The presented EA-driven cybersecurity approach offers a holistic and integrated methodology for harmonizing cybersecurity strategies with the comprehensive objectives, infrastructure, and operational facets specific to African higher education institutions. This approach carries notable implications for these institutions as they grapple with distinctive challenges in the implementation of effective cybersecurity measures. Prospective avenues for future research within this academic domain may encompass the development of a comprehensive legal framework, the augmentation of cybersecurity expertise, the pursuit of additional case studies, and the exploration of emerging technological paradigms.

References

Ahmed, M., Panda, S., Xenakis, C., & Panaousis, E. (2022). MITRE ATT&CK-driven cyber risk assessment. Proceedings of the 17th International Conference on Availability, Reliability and Security,

Archimate. (2000). Archimate EA Digram [Web]. https://www.archimatetool.com/resources/. https://www.archimatetool.com/resources/

Bouke, M. A., Abdullah, A., ALshatebi, S., Atigh, H. E., & Cengiz, K. (2023). African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions. *arXiv preprint arXiv:2307.01966*.

Burkett, J. S. (2012). Business security architecture: weaving information security into your organization's enterprise architecture through SABSA®. *Information Security Journal: A Global Perspective, 21*(1), 47-54.

Choudhuri, B., Srivastava, P. R., Mangla, S. K., & Kazancoglu, Y. (2023). Enterprise architecture as a responsible data driven urban digitization framework: enabling circular cities in India. *Annals of Operations Research*, 1-29.

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems, 27*(1), 307-324.

Dlamini, I., Taute, B., & Radebe, J. (2011). *Framework for an African policy towards creating cyber security awareness*.

Eltahir, M., & Ahmed, O. (2023). Cybersecurity Awareness in African Higher Education Institutions: A Case Study of Sudan. *Inf. Sci. Lett, 12*.

Gloria Appiah, J. A.-A., Yu-Lun Liu. (2020). Organizational Architecture, Resilience, and Cyberattacks. *IEEE Transactions on Engineering Management, 69*(5, October 2022), 2218 - 2233.

Groš, S. (2021). A critical view on CIS controls. 2021 16th International Conference on Telecommunications (ConTEL),

Humphreys, E. (2016). *Implementing the ISO/IEC 27001: 2013 ISMS Standard*. Artech house.

IGNAT, I. (2022). *Factor Analysis of Information Risk (FAIR™) when assessing the Information Security* Universitatea Tehnică a Moldovei].

Kayode-Ajala, O. (2023). Establishing Cyber Resilience in Developing Countries: An Exploratory Investigation into Institutional, Legal, Financial, and Social Challenges. *International Journal of Sustainable Infrastructure for Cities and Societies, 8*(9), 1-10.

Kotusev, S., Kurnia, S., & Dilnutt, R. (2023). Enterprise architecture artifacts as boundary objects: An empirical analysis. *Information and Software Technology, 155*, 107108.

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2023). Understanding Cyber Threats Against the Universities, Colleges, and Schools. *arXiv preprint arXiv:2307.07755*.

Masi, M., Sellitto, G. P., Aranha, H., & Pavleska, T. (2023). Securing critical infrastructures with a cybersecurity digital twin. *Software and Systems Modeling, 22*(2), 689-707.

Maulana, Y. M., Azmi, Z. R. M., & Arshah, R. A. (2023). Modeling of Strategic Alignment to Modify TOGAF Architecture Development Method Based on Business Strategy Model. *International Journal on Advanced Science, Engineering & Information Technology, 13*(1).

Maulana, Y. M., Azmi, Z. R. M., & Phon, D. N. E. (2023). Business-IT Alignment through Enterprise Architecture in a Strategic Alignment Dimension: A Review. *Register: Jurnal Ilmiah Teknologi Sistem Informasi, 9*(1), 55-67.

Morse, E. A., & Raval, V. (2008). PCI DSS: Payment card industry data security standards in context. *Computer Law & Security Review, 24*(6), 540-554.

Nasir, N. N. I., Radzuan, S. N., Azhami, B. A., & Hamidon, H. (2023). Cyber Security in Higher Education: Problem and Solution. Proceedings of 1st Glocal Symposium on Information and Social Sciences (GSISS) 2023,

Pereira, C. M., & Sousa, P. (2005). Enterprise architecture: business and IT alignment. Proceedings of the 2005 ACM symposium on Applied computing,

Rana, M., & Sharma, D. (2023). Understanding Cyber-Attacks and their Impact on Global Financial Landscape. 2023 International Conference on Circuit Power and Computing Technologies (ICCPCT),

Rozas, I. S., Khalid, K., Yalina, N., Wahyudi, N., & Rolliawati, D. (2020). Digital Enterprise Architecture for Green SPBE in Indonesia. *CCIT (Creative Communication and Innovative Technology) Journal, 15*(1), 26-24.

Sharkov, G. (2020). Assessing the maturity of national cybersecurity and resilience. *Connections: The Quarterly Journal, 19*(4), 5-24.

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. *Electronics, 11*(14), 2181.

Trad, A. (2023). Integrating a Holistic Enterprise Architecture Pattern: A Proof of Concept. In *Handbook of Research on Digitalization Solutions for Social and Economic Needs* (pp. 1-39). IGI Global.

Walter, M., Heinrich, R., & Reussner, R. (2023). Architecture-based attack path analysis for identifying potential security incidents. European Conference on Software Architecture,

White, G. B., & Sjelin, N. (2022). The NIST cybersecurity framework. In *Research Anthology on Business Aspects of Cybersecurity* (pp. 39-55). IGI Global.