Pepperdine University

Graziadio School of Business

HUMAN FACTORS MATTER: THE INTERSECTION OF CYBERSECURITY GOVERNANCE, AND CULTURE IN RISK MANAGEMENT OF CRITICAL INFRASTRUCTURE

A dissertation submitted in partial fulfilment

of the requirements for the degree of

DOCTOR OF BUSINESS ADMINISTRATION

by

Prince Abubakari

December, 2024

Nelson Granados, Ph.D. – Dissertation Chair

This dissertation, written by

Price Abubakari

under the guidance of a Dissertation Committee and approved by its members, has been submitted to and accepted by the Pepperdine Graziadio Business School in partial fulfilment of the requirements for the degree of

DOCTOR OF BUSINESS ADMINISTRATION

Doctoral Dissertation Committee:

Nelson Granados, Ph.D., Supervisor

Ann Feyerherm, Ph.D., Secondary Advisor

Charla Griffy-Brown, Ph.D., External Reviewer

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

VITA

Clearance: Top SECRET/SCI– DCID 6/4/U.S. Citizen/10-point Disabled Veteran

Education:

Executive Doctorate in Business Administration (Cyber) – Pepperdine University	August 2024
Master of Eng. – University of Maryland College Park – Cybersecurity Engineering	January 2020
Graduate – University of Maryland College Park – Software Engineering	January 2020
Graduate – Wharton Business School - Business Analytics Executive Leadership	September 2018
Master of Business Administration – Finance, National University San Diego	September 2017
Graduate – Boston University – Project Management	January 2012
Bachelor of Science – Electrical Engineering, University of Science and Technology Gh	May 2004

Key Experience:

- 18+ years of Acquisition Category I program experience
- 18+ years of Systems Engineering/Information Security experience,
- 15+ years of Executive management
- Experience championing and leading interagency programs, projects and initiatives

Current Work Experience

Department of the Navy – Naval Facilities Engineering Command, Washington Navy Yard, DC
Command Information Operations Directorate

Deputy Director - Cybersecurity Infrastructure and Engineering/ Cyber Commissioning ISSM
March 2021 to Present (GS-14 IT Specialist (2210 - InfoSec)) 40 hours/week

Lead a 650-person organization on the vision, strategy, execution, and serve as the performance-improvement champion for Navy Ashore Enterprise Cyber, Information, and Operational Technology operations. Serve as the senior advisor to command leadership synthesizing Cybersecurity, Innovation, and Cloud Computing programs concept of operations to prepare capital investment plans and execute a $2B infrastructure budget. Oversee the acquisition, development, implementation, maintenance, security, and architecture of Ashore mission technology. Develop assessment strategies for determining risk gaps in existing technology programs; design new methods for measuring and improving information systems and cyber operational effectiveness and productivity in critical infrastructure. Develop, deliver, integrate, and advocate technology governance policies. Facilitate technology strategy, including hybrid cloud strategy and infrastructure modernization, to transform and innovate IT/OT operations that meet short and long-term Navy Ashore plans, policies, and programs as set forth by the Chief of Naval Operations. Encourage a collaborative, inclusive, and creative environment for all team members to propose innovative solution sets to meet command objectives. Empower and mentor junior civilians and military members into positions of leadership and management that provide organizational career accession.

Awards:

Navy Commendation Medal (COM)	NAVFAC Washington DC	March 2021
Navy Commendation Medal (COM)	NAVFAC EURAFSWA	June 2019
Navy Achievement Medal (NAM)	MCAS Miramar	July 2016
Navy Achievement Medal (NAM)	NMCB-4	August 2013
Navy Achievement Medal (NAM)	NWS Earle	April 2012
Navy Achievement Medal (NAM)	Al Asad, Iraq	May 2009
Navy Achievement Medal (NAM)	USS Ponce LPD-15	December 2009

ABSTRACT

In the 21st century, cybersecurity threats have evolved into pressing socio-technical issues, with significant implications for the safety and stability of global critical infrastructure. This dissertation explores the intersection of cybersecurity governance and culture in risk management of national critical infrastructures, defined as essential systems and assets, whether physical or virtual, that are vital to the security, public health, safety, economy, or any combination thereof, and the disruption of which would have a debilitating impact on a nation. The study delves into how human factors like organizational culture and governance mechanisms interplay to influence cybersecurity outcomes. The research adopts a qualitative approach, leveraging in-depth interviews with key stakeholders across various critical infrastructure sectors, including Chief Information Security Officers, Chief Information Officers, and other cybersecurity professionals involved in safeguarding critical infrastructures. The findings highlight the complexities and challenges of balancing stringent security measures with operational efficiency, the importance of fostering a cybersecurity-aware culture, and the role of governance in shaping cybersecurity strategies. This study contributes to the understanding of how human factors and organizational dynamics affect cybersecurity risk management, providing insights into the practical challenges faced by organizations. There is a need for comprehensive governance frameworks that integrate technological defenses with human-centric approaches to effectively manage cyber-risks for critical infrastructures. I propose strategies to enhance cybersecurity resilience.

Keywords: cybersecurity governance, culture, risk management, essential systems

CHAPTER 1: INTRODUCTION

In the 21st century, cybersecurity threats have evolved beyond mere technical challenges, becoming pressing socio-technical issues that have significant implications for the safety and stability of our increasingly interconnected global infrastructure. With the expansion of digitalized operations and the Internet of Things (IoT), critical infrastructure protection has gained unprecedented importance (Scholl et al., 2008; U.S. Department of Homeland Security, 2022).

A nation's critical infrastructure, including its energy, transportation, and communication sectors, relies heavily on complex cyber-physical systems. As evidenced by high-profile cyberattacks such as the Colonial Pipeline attack in 2021 and the Ukraine power grid cyberattack in 2015, these infrastructures are vulnerable targets. The Colonial Pipeline attack highlighted the real-world consequences of such vulnerabilities, resulting in significant fuel shortages and economic repercussions across the United States (Sanger et al., 2017). Similarly, the Ukraine cyberattack served as a wake-up call for nations worldwide, underscoring the potential for coordinated cyberattacks to disrupt essential services and plunge regions into darkness (Wilshusen & Barkakati, 2012).

Furthermore, with initiatives such as StarLink aiming to provide global internet coverage via satellite networks, the scale and scope of cyber threats could magnify in unforeseen ways. While these satellites intend to democratize internet access, they also present potential vulnerabilities that cybercriminals might exploit, bridging the gap between local infrastructure and global networks (Situational Awareness, Data Analytics, and Assessment, 2019).

However, beyond the technicalities of these attacks, two common threads often characterize cybersecurity challenges: governance and the human factor. Cybersecurity is not just

a technology problem but a people, process, and risk problem (Griffy-Brown et al., 2019). It is increasingly recognized that while technology plays a vital role in facilitating and thwarting cyberattacks, human behavior and organizational culture significantly influence the susceptibility and response to these threats (Severance, 2016; Winnefeld Jr et al., 2015). For instance, research by Romney (1995) on computer fraud highlights the need for robust technical measures and a pervasive culture of cybersecurity awareness to prevent fraudulent activities.

Moreover, the governance mechanisms within organizations play a pivotal role in shaping cybersecurity strategies and their effectiveness. They include identifying risk appetite, building accountability frameworks, and defining those responsible for making decisions (Miller & Griffy-Brown, 2018). As Stanciu and Tinca (2016) point out, the alignment between perceptions and reality concerning information security emphasizes the need for accurate knowledge dissemination and governance. Without effective governance, even the best technical measures may fail to protect against threats, as the organizational culture may not support or prioritize their proper implementation and maintenance (Sezer & Caliyurt, 2018).

In the ever-evolving landscape of cybersecurity threats, the confluence of culture, governance, and human behavior within organizations that manage or rely on critical infrastructure becomes paramount. The interplay between these factors can strengthen an organization's resilience against cyber threats or make it vulnerable to potentially catastrophic breaches.

This research seeks to delve into this intersection, exploring the roles that culture and governance play in influencing behaviors in critical infrastructure cyber risk management. Based on a comprehensive examination grounded in previous literature and current cybersecurity

incidents, I aim to comprehensively understand the factors contributing to or mitigating risks in our connected world.

Background on Critical Infrastructure and Cybersecurity

Critical infrastructure refers to the physical and virtual systems and assets vital to society so that their incapacitation would have a debilitating effect on national security, the economy, public health, or safety (U.S. Department of Homeland Security, 2022). Examples include transportation networks, energy grids, healthcare systems, and communication networks.

Historically, concerns about critical infrastructure have been mainly about physical threats. However, with the increasing digitization of processes and the adoption of interconnected systems, there is a growing recognition of cybersecurity threats targeting these vital assets. Sanger et al. (2017) showcased the global impact of cyber capabilities when they discussed how North Korea transitioned from being a laughingstock in cyber operations to a formidable player after launching multiple high-profile cyber-attacks, notably the Sony Pictures hack. Such incidents underscore the vulnerabilities inherent in an interconnected world and emphasize the need to protect critical infrastructures from various digital threats.

Modern critical infrastructure systems heavily rely on Information and Communication Technologies (ICT). With advancements like the IoT and Industry 4.0, these systems' cyber and physical elements are now closely integrated (Süzen, 2020). This convergence of digital and physical systems means that the implications of a cyberattack can extend far beyond data breaches to physical damage and service disruption. Furthermore, the cascading effects of attacks on interconnected infrastructures can compound the overall impact. For instance, a cyberattack on an electricity grid could disrupt power supply, which, in turn, could affect transportation systems, hospitals, and other dependent services.

The rise in high-profile cyberattacks targeting critical infrastructure has heightened the awareness and necessity for robust cybersecurity practices. For instance, the Health Insurance Portability and Accountability Act (HIPAA) Security Rule was created to protect electronic personal health information, which indicates the importance placed on safeguarding critical health infrastructure (Scholl et al., 2008). The U.S. Navy's Cybersecurity Readiness Review further emphasized the importance of cybersecurity in protecting national defense assets (Secretary of the Navy, 2019).

Several organizations have recognized the importance of cultivating a robust cybersecurity culture. This goes beyond just implementing security measures; it means fostering an environment where every stakeholder, from top management to the operational level, understands, values, and consistently practices sound cybersecurity behaviors. This understanding aligns with the National Initiative for Cybersecurity Education (NICE) framework, emphasizing the importance of educating a diverse workforce to address cyber threats (Shoemaker et al. 2016).

The challenge with cybersecurity, particularly in the context of critical infrastructure, is the constantly evolving nature of threats. Adversaries continually adapt and refine their techniques, seeking vulnerabilities in systems. Straub and Welke (1998) pointed out that coping with systems risk requires an ongoing commitment to security planning and risk management.

The Rising Importance of Human Factors

The intersection of cybersecurity culture and governance, especially within critical infrastructure, is paramount. Therefore, protecting critical infrastructure in the age of digital threats demands a multi-faceted approach. While technological safeguards are vital, the

organizational culture and governance mechanisms that prioritize, support, and adapt to the dynamic landscape of cybersecurity are equally important.

Understanding cybersecurity requires a shift in perspective. It is not merely about the technology, but also the human element involved. As Severance (2016) aptly highlighted, the security mindset entails anticipating unforeseen uses of systems and planning for them. This becomes crucial when considering the human operators of critical infrastructure, who can either be a system's greatest vulnerability or its most stalwart line of defense, depending on their cybersecurity awareness and training (Wilson & Hash, 2003).

The interplay between technology and human behavior is at the core of cybersecurity challenges, particularly critical infrastructure protection. While technology advancements have streamlined processes and bolstered defenses, the human factor remains a persistent vulnerability and, at times, the linchpin of robust cybersecurity posture. In recent years, there has been a burgeoning recognition of the importance of human factors in determining the efficacy of cybersecurity strategies (Shoemaker et al., 2016). Cybersecurity's human element is a complex interplay of behaviors, beliefs, motivations, and skills. Severance (2016) highlighted that a security mindset involves anticipating unforeseen system uses and preparing accordingly. Yet, such a mindset is not inborn - it must be nurtured. This underscores the vital role of ongoing training and awareness programs in fostering a security-aware workforce.

Organizational Culture and Cybersecurity

A key dimension of human factors is the broader organizational culture. According to Wilson and Hash (2003), fostering a strong cybersecurity culture means going beyond merely implementing security measures. It involves creating an environment wherein everyone, from top-tier management to frontline employees, understands, values, and practices consistent

cybersecurity behaviors. When an organization's culture embodies security principles, it transforms each employee into a proactive participant in the defense mechanism, making the system less susceptible to breaches.

Human Error and Cybersecurity Breaches

Despite advances in security protocols and defense mechanisms, human error remains one of the primary causes of security breaches. In their report, Sanger et al. (2017) described how state-sponsored attacks, like the Sony Pictures hack, exploited human vulnerabilities through tactics like spear-phishing. Such instances underline that even the most advanced defense systems can be rendered ineffective when a single individual acts carelessly or falls for a deceptive tactic.

It is worth noting that human errors do not always result from negligence. In many cases, system users may be overwhelmed by the complexity of security protocols, leading to shortcuts or mistakes (Straub & Welke, 1998). This accentuates the importance of designing security processes that are robust and user-friendly, reducing the cognitive load on the end-users.

One of the predominant attack vectors capitalizing on human vulnerabilities is social engineering. Cyber adversaries often find it easier to manipulate human behavior than directly attacking fortified technical defenses. Techniques such as phishing, baiting, and tailgating showcase how attackers prey on human psychology to gain unauthorized access (Süzen, 2020). This underscores the rising significance of cultivating a vigilant organizational culture that can recognize and resist such manipulative tactics.

Given humans' central role in cybersecurity, there is a growing emphasis on developing solutions centered around human behaviors and needs. The U.S. Navy's Cybersecurity Readiness Review (2019) stressed the importance of such human-centric solutions. By understanding and

addressing the cognitive, behavioral, and cultural aspects of security, organizations can more effectively prevent breaches and respond to incidents. This involves approaches like user behavior analytics, which monitors and analyzes user activities to detect anomalies indicative of potential threats.

The dynamic nature of cyber threats necessitates continuous training and awareness. The NICE framework emphasizes educating a diverse workforce to address emerging cyber threats (Shoemaker et al., 2016). Such initiatives equip employees with the necessary skills and foster a security-aware mindset, making them less susceptible to threats and manipulative tactics.

The intersection of human factors and cybersecurity has significant implications for the future. As we move towards an increasingly interconnected world with the proliferation of the IoT and Industry 4.0, the number of potential attack vectors will multiply. With this growth, the human role will become even more pivotal. Whether it is a factory worker interacting with a smart manufacturing system or a healthcare professional using a connected medical device, their security decisions will cascade effects on the broader ecosystem. Thus, addressing human factors in cybersecurity is not just a current need; it is an ongoing requirement that will shape the future of cyber defense strategies. Organizations must prioritize human-centric solutions, invest in continuous training, and, most importantly, cultivate a robust cybersecurity culture that integrates security into every facet of operations.

Research Questions

To address the problem of cybersecurity governance and behaviors that currently fail to manage cybersecurity risk on critical infrastructure, I examine the relationship between governance and behaviors in critical infrastructure cyber risk, exploring the following research questions:

- How do governance mechanisms influence the management of cybersecurity risks within critical infrastructure systems?
- How can governing bodies incorporate behavioral considerations to enhance cybersecurity of critical infrastructure systems?
- How can governance strategies enable effective cyber risk critical infrastructure management?

Purpose Statement

The intertwining relationship between technological architecture, organizational culture, and human behavior is becoming more evident in cybersecurity. The security of critical infrastructure does not merely rest on the sophistication of technology but is significantly influenced by the human elements that interact with it. With cyber threats persistently evolving, understanding these human factors and how they align with organizational culture and governance is vital. This study aims to delve into the intersection of cybersecurity governance, placing special emphasis on the exploration of human factors in the risk management of critical infrastructure.

Aims and Objectives

Aim 1: Cybersecurity Culture within Organizations

To understand the underlying culture of cybersecurity within organizations, fostering a balance between technological defenses and human dynamics.

- Objective 1.1: Examine organizations' existing cultures and individual behaviors related to cybersecurity and how they impact the overall security state.

- Objective 1.2: Assess the alignment of organizational goals with cybersecurity initiatives and how they correlate with actual security outcomes, emphasizing the challenges and opportunities that the human element presents.

Aim 2: Governance Mechanisms and Impact

To evaluate the role of governance in shaping cybersecurity outcomes and its implications for risk management, especially in organizations responsible for critical infrastructure protection.

- Objective 2.1: Explore the existing governance frameworks and their ability to support a holistic cybersecurity approach that integrates technology, people, and processes.
- Objective 2.2: Analyze how governance mechanisms facilitate or hinder the development of a cybersecurity culture within organizations, drawing attention to policies, procedures, and guidelines related to human interaction with systems.

Aim 3: Human Behaviors in Critical Infrastructure Cyber Risk Management

To explain the influence of human behavior, cognition, and decision-making on risk management, particularly in critical infrastructure security.

- Objective 3.1: Examine the strategies employed to reduce the impact of human error, including user training, intuitive interface design, and feedback mechanisms, highlighting their effectiveness in actual settings.
- Objective 3.2: Understand how risk perceptions among individuals vary and how they influence cybersecurity behaviors, thereby impacting the overall risk profile of an organization's critical infrastructure.

How Aims will be Accomplished

A qualitative research methodology will be employed to authentically explore the intersections of cybersecurity culture, governance, and human factors within critical infrastructures. Interviews to experts, with their in-depth, exploratory nature, are best suited to unearth the intricate nuances of human behavior, organizational dynamics, and the underlying intricacies of cybersecurity culture.

The qualitative approach allows for an in-depth understanding of the human experiences, perceptions, and motivations within cybersecurity. It provides the flexibility to probe deeper into responses, clarifying ambiguities and exploring underlying motivations that may not be immediately evident (Bryman, 2016).

CHAPTER 2: LITERATURE REVIEW AND FRAMEWORK

Method for Conducting the Literature Review

In today's digital age, the significance of cybersecurity in safeguarding critical infrastructure cannot be overstated. As the mesh of technology, commerce, and society tightens, understanding the multiple facets of cybersecurity becomes pivotal. Several scholars have delved deep into these multifaceted concerns to provide us with a comprehensive understanding.

The literature review was conducted using peer-reviewed journal articles, practitioner white papers, research studies, books, and governmental agency reports. Scholarly business databases were used to identify relevant research; searches were conducted using Scopus, Business Source Premier, and Google Scholar. Additionally, searches were conducted using several combinations of the search terms listed in Table 1, spanning three major domain categories: “Cybersecurity and Critical Infrastructure,” “Human Factors in Cybersecurity,” and “Cybersecurity Culture and Governance.” The main categories were the sub-categorized and grouped by: “Concept/Teams,” “Primary Search Terms,” and “Related Terms/Phrases”. Articles were limited to those in peer-reviewed scholarly journal articles receiving top ranks (A* and A) in the Australian Business Deans Council Journal Quality List. The searches produced 1,236 articles using several combinations of the abovementioned keywords to run queries. To be more precise, Scopus retrieved 276 results and Business Source Premier returned 1,043 results.

Table 1

Seminal References

Concept/Theme	Primary Search Term	Related Terms/Phrases	References
Cybersecurity and Critical Infrastructure			
Infrastructure Security	Critical Infrastructure	National Security, Infrastructure Protection, Utility Security	Scholl et al. (2008), Sanger et al., (2017), Tagarev et al. (2020
Threat Landscape	Cyber Threats	Vulnerabilities, Exploits, Cyber-attacks	Woodruff, S. M., Sr. (2020
Legal Framework	Cybersecurity Laws	Regulation, Compliance, Critical Infrastructure Protection Laws	Babtain et.al (2019), Clark, C. Y. (2013), Corruption Review, J.O. (2022)
Human Factors in Cybersecurity			
Human Behavior	Cybersecurity Behavior	User Behavior, Insider Threats, Employee Compliance	Kleij & Leukfeldt (2019)
Training & Awareness	Security Training	Information Security Awareness, Cybersecurity Training Programs	Kusumawati (2018), Clark (2013)
Psychological Factors	Cybersecurity Psychology	Behavioral Psychology, Cyber Fatigue, User Attitudes	Bernstein, D. J., & Lange, T. (2019), Chalhoub, M. S. (2010)
Cybersecurity Culture and Governance			
Governance Mechanisms	Cybersecurity Governance	IT Governance, Governance Frameworks, Strategic Governance	Sartawi (2020), Albalas et al. (2022), ISACA (2019a), ISACA (2019b)
Organizational Culture	Security Culture	Organizational Behavior, Security Awareness, Organizational DNA	Chen et al. (2015), D'Arcy & Greene (2014), Pullin (2018)
Interplay of Culture & Governance	Governance and Culture	Corporate Governance, Cultural Impact on Governance, Organizational Dynamics	Calcara & Marchetti (2021), Hartmann & Carmenate (2021)

Cybersecurity Culture and Human Behavior

The evolving digital landscape and its intricacies have brought forward the undeniable significance of cybersecurity culture and the human element's pivotal role. Ashenden (2018) stated that understanding employee attitudes toward information security is crucial for an organization to truly safeguard its assets. This sentiment is further corroborated by Adams and Makramalla (2015) who suggested a gamified approach to cybersecurity training. They emphasized that the more interactive and engaging the training is, the better-equipped individuals are to understand the nuances of security threats. Meanwhile, Aldawood and Skinner (2018) noted the importance of raising awareness about social engineering, a rapidly growing cybersecurity threat, suggesting that understanding human behavior can be as critical as understanding the technology when dealing with cybersecurity threats.

Furthermore, the work of Chen et al. (2015) sheds light on the transformative impact of comprehensive information security programs on a culture of organizational security. They emphasize that an informed and aware workforce acts as the first defense against cyber threats, underscoring the importance of creating a security-centric organizational culture. The intricacies of human behavior concerning cybersecurity are diverse, ranging from individual actions to organizational culture and the broader societal implications.

Individual Behavior and Cybersecurity

The role of the individual in the cybersecurity landscape cannot be overstated. D'Arcy and Hovav (2007) focused on deterring internal information system misuse, highlighting that the actions of a single user can often pose significant threats to an entire organization. They reiterated the importance of user awareness and adherence to security countermeasures, emphasizing the direct impact on information systems misuse (D'Arcy et al., 2009). Moreover,

Dodge and Ferguson (2006) explored the significance of awareness through the lens of phishing attacks, emphasizing that targeted email-based attacks exploit human vulnerabilities, further stressing the need for robust user education and training.

Organizational Culture and Cybersecurity

An organizations cybersecurity posture reflects its internal culture, values, and priorities. D'Arcy and Greene (2014) argue that security culture and the employment relationship are crucial drivers for security compliance. This highlights the importance of fostering an environment where security is viewed as everyone's responsibility and the employees feel intrinsically motivated to follow best practices. Granneman (2018) further emphasizes the role of businesses in guiding and improving information security. He underscores that organizational leadership should take the helm in establishing a culture where cybersecurity is an integral aspect, not just an afterthought.

Broader Societal Implications

Cybersecurity challenges are not limited to individual users or organizations but have profound implications for the broader society. The Cybersecurity & Infrastructure Security Agency (2022) showcases efforts to safeguard national cyber and critical infrastructure, highlighting the collective responsibility to address threats and vulnerabilities. Furthermore, legislation such as the Federal Information Security Management Act (FISMA) of 2014 and HIPAA demonstrate society's commitment to securing data and information on a broader scale, enforcing regulations and penalties for non-compliance.

Human behavior, from individual actions to organizational dynamics and broader societal efforts, plays a pivotal role in cybersecurity. As Creswell and Guetterman (2019) aptly note in their research methodologies, understanding the human element requires both qualitative and