Journal of Leadership and Management®
An International Journal of Strategic, Behavioral and Public Aspects of Leadership in Management
Cabell's Listed
A journal of the Institute of Leadership and Management Association, PO Box 564, Douglassville PA 19518. 484-332-3331. https://www.jleadershipmanagement.org

Strengthening Cybersecurity Resilience with Transformational IT Leadership: *PASTA-TITL Threat Modeling Framework*

U. Yeliz Eseryel, College of Business/East Carolina University, eseryelu17@ecu.edu
Brenda L. Killingsworth, College of Business/East Carolina University
April H. Reed, College of Business/East Carolina University
Christopher P. Furner, College of Business/East Carolina University

Online published: July 2024 Print published: July 2024 Editors: Adam Szpaderski & CJ Rhoads	Authorship Roles and Conflict of Interest Statement is on file at the Journal of Leadership and Management offices, available on request. Contact editors@jleadershipmanagement.org

ABSTRACT

Today's digital landscape challenges organizations with escalating cyber threats that surpass traditional security measures. The knowledge and engagement gap between leadership and cybersecurity management fosters vulnerabilities, impeding security integration into strategic decision-making. This study pioneers a solution by integrating important elements of cybersecurity resilience: It incorporates Transformational Information Technology Leadership (TITL) principles into the PASTA threat modeling framework. The transformational IT leadership principles recommended for each stage of PASTA framework help overcome key challenges of PASTA framework such as the complexity of implementation. Transformational IT leadership principles help create a strategic IT vision that incorporates cybersecurity resilience. Further, transformational IT leaders both inspire and empower not only IT staff but functional staff by fostering a culture of proactive engagement in cyber risk management, where a business makes informed decisions to mitigate risks. The PASTA-TITL framework aims to fortify cybersecurity resilience by implementing effective planning, mitigation, resilience, and recovery from threats. This integrated framework fosters improved leadership training and robust cybersecurity practices while contributing to a more secure digital ecosystem.

This study bridges theoretical tenets and practical cybersecurity strategies, advocating heightened leadership engagement for combatting evolving cybersecurity challenges. The PASTA-TITL framework promotes aligned IT leadership practices, effectively strengthening cybersecurity resilience.

KEYWORDS

Cybersecurity, Threat Modeling, Integrated Threat Methodology; PASTA Process, Transformational IT Leadership, Resilience, PASTA-TITL Framework

Introduction

Digital evolution brings increasingly connected and complex digital landscapes to corporate governance and risk management (McKinsey Global Institute, 2023). This forces organizations to rethink their security processes and how they align with the organization's strategic objectives and management processes. The digital evolution has brought with it an emergence of sophisticated and persistent cyber threats that seek to undermine an organization's mission and security protections (Ardagna et al., 2023). Recent regulations, exemplified by the U.S. Securities and Exchange Commission (2023) mandates, underscore the criticality of leadership commitment to resilient cybersecurity governance. The regulations also highlight the pivotal role of leadership commitment in effective decision-making in this critical area. Much like when financial literacy

was required of C-suite and board members after the Enron incident (Fairfax, 2018), cybersecurity literacy and its incorporation within an organization's strategic and management processes is now a top priority (Hueca, 2020).

Cybersecurity breaches pose multifaceted threats jeopardizing an organization's reputation, financial stability, and operational continuity (Anderson & Moore, 2007; Verizon, 2023). As traditional cybersecurity approaches struggle to adapt to the evolving threat landscape (Jarvis, 2023), there exists a noticeable lack of alignment between management practices and cybersecurity expertise (Palo Alto Networks, 2022).

Transformational Information Technology Leadership (TITL) can be defined as inspiring followers to go above and beyond in their Information Technology (IT) use to increase their followers' work efficiency and effectiveness. Transformational IT leadership is developed by Eseryel (2020), who adapted the transformational leadership theory to work settings that involve IT use. Transformational leadership theory stream, while being renowned for inspiring teams and adapting to dynamic environments (Bass, 1985), remains relatively underexplored in its integration within cybersecurity frameworks (Lohrke & Frownfelter-Lohrke, 2023). This research framework aims to bridge this gap by integrating transformational Information Technology (IT) leadership (TITL) principles into the Process for Attack Simulation and Threat Analysis (PASTA) framework, a comprehensive threat modeling methodology (UcedaVélez & Morana, 2015).

This research delineates symbiotic relationships between leadership strategies and cybersecurity practices within each PASTA stage. It aims to elucidate how transformational IT leadership components fortify organizational resilience against cyber threats. Aligning TITL practices with PASTA stages showcases the role of transformational IT leadership in enhancing threat identification, mitigation, and prevention to strengthen organizational cybersecurity resilience significantly. Ultimately, this study contributes to the literature by proposing a novel framework unifying leadership principles and cybersecurity strategies while emphasizing their integration within organizational governance, risk management, and strategic processes.

Theoretical Foundations

To develop an integrated framework for understanding the influence of leadership and cybersecurity effectiveness, relevant literature related to the PASTA framework and transformational IT leadership (TITL) are presented next.

Process for Attack Simulation and Threat Analysis (PASTA) Framework

Threat modeling is a process for analyzing potential attacks or threats (Uzunov & Fernandez, 2014), which provides a structured way to secure software design. This approach involves understanding an adversary's goal in attacking a system (Bedi, et al., 2013). PASTA is a structured threat modeling framework with seven stages (Figure 1) that are used to conduct comprehensive threat modeling and analysis for an organization (UcedaVélez & Morana, 2015).

To develop an integrated threat framework, we build from the PASTA framework for the following reasons: PASTA aligns cybersecurity efforts with organizational strategy and goals, which ensures that assets and processes that are critical to an organization will be protected (UcedaVélez, 2021). This framework is customizable for different industries or project types, and can be scaled up or down, based on organizational size and needs (Allen-Addy, 2023). PASTA framework allows departments to collaborate and leverage existing business processes (UcedaVélez, 2021). The PASTA model is attack-centric, by adopting the perspective of the attacker. It is also risk-centric in that it mitigates what matters and it enhances the cybersecurity know-how in the organization (Subhash, et al., 2024, p.3858). It uses evidence-based threat modeling and focuses on probability likelihood, risk, and impact of the attack (Subhash, et al., 2024; UcedaVélez, 2021). By focusing on the threats that are most likely to occur and that would cause the greatest disruption to business continuity, PASTA framework allows for the effective distribution of organization's cybersecurity efforts and resources (Allen-Addy, 2023; Subhash, et al., 2024; UcedaVélez, 2021).

The Seven Stages of the PASTA Framework

The first stage of PASTA, "Define Objectives," aims to clarify the goals and scope of the threat modeling exercise. At a more detailed level, three main activities occur in this stage requiring effective leadership. First, assets and information systems must be identified to ensure vital assets are prioritized for business resiliency.

Identifying critical assets cannot be left to any one department because they might focus only on their own issues. Instead, it is important to poll all departments and then collaborate to prioritize the assets. The second activity defines success metrics for risk mitigation, supporting efforts to reduce attack likelihood and long-term impacts. The third activity considers business objectives and regulatory requirements when aligning threat modeling with overall business goals and ensuring compliance with required security regulations (e.g., HIPAA, PCI DSS).

The second PASTA stage, "Define Technical Scope," establishes the boundaries of the system under analysis. The three main activities in this stage that are impacted by leadership effectiveness are: (a) identifying key system architectural components needing fortification to ensure business resilience, (b) charting data movement within the organization and mapping user interactions with different system components, and (c) defining trusted internal networks and public-facing untrusted zones to fortify potential attack entry points. Completing the activities at this stage will likely fall to the technical staff, who will work better if empowered by leadership.

The goal of the third PASTA stage, "Application Decomposition," is to break down the system into smaller, manageable units. The main activities in this stage that are impacted by leadership effectiveness are: (a) dividing the system into functionalities and dependencies; (b) mapping data assets and defining user roles with respective access privileges; and (c) identifying how potential interactions and dependencies can create vulnerabilities and establishing potential control points to mitigate those vulnerabilities. Leaders should encourage creativity and critical thinking to identify and address potential vulnerabilities beyond traditional avenues. The decomposition in this stage must be thorough since every missed vulnerability is an opportunity for a breach.

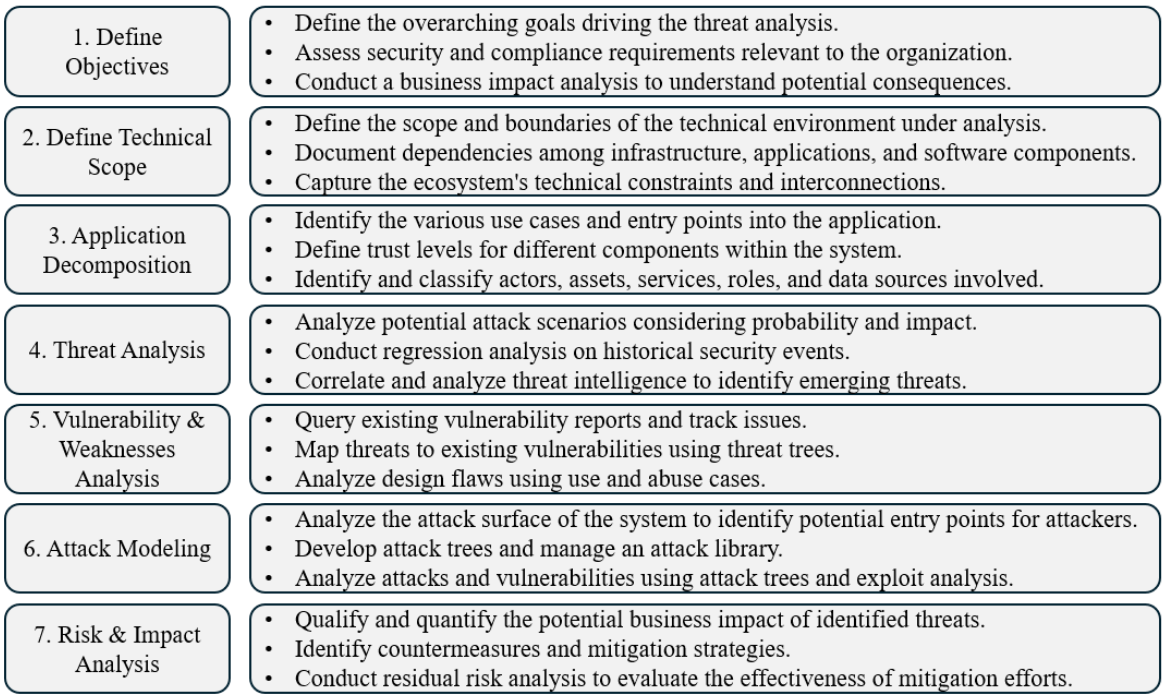

Figure 1. The PASTA Stages (Adapted from UcedaVélez & Morana, 2015)

The purpose of the fourth PASTA stage, "Threat Analysis," is to identify and categorize potential threats targeting the system. Three main activities occur in this stage which are impacted by leadership effectiveness: (a) ideating possible attack scenarios, systematically considering possible attack methods for each identified asset; (b) identifying potential threat actors and their motives (for financial gain, data theft, sabotage, or gaining a competitive advantage); and (c) prioritizing threats based on the likelihood of occurrence and the potential impact on the organization if the threat is successful.

The intent behind the fifth PASTA stage, "Vulnerability Analysis," is to identify system weaknesses and vulnerabilities exploitable by identified threats. The main activities in this stage that are impacted by

leadership effectiveness are: (a) evaluating the effectiveness of existing security controls and analyzing system configurations and code for vulnerabilities; (b) actively attempting to exploit vulnerabilities and weaknesses; and (c) assessing the feasibility, technical difficulty, and staff abilities to counter each identified vulnerability. Across all stages, leaders delegate autonomy to team members, empowering them to make decisions that are aligned with business and cybersecurity objectives. This is important since team members are usually the experts on vulnerabilities in their areas (see Avolio Zhu, Kho, & Bhatia, 2004 on *empowerment*).

The objective of the sixth PASTA stage, "Attack Modeling," is to develop detailed attack simulations based on identified vulnerabilities and threats. The activities in this stage that are impacted by leadership effectiveness are: (a) identifying key vulnerabilities, paths, and control points and mapping the sequence of actions that are required for a successful attack so that plans can be developed to provide a layered defense; (b) analyzing existing security controls and proposing mitigation strategies to defend against the identified attack scenarios; and (c) assessing the overall likelihood and impact of successful attack scenarios on the business resiliency.

The aim of the seventh PASTA stage, "Risk and Impact Analysis," is to evaluate the overall risk posed by identified threats and vulnerabilities. Four main activities occur in this stage which are impacted by leadership effectiveness: (a) assessing the likelihood and impact scores of each threat scenario using a scoring system that highlights the potential impact on business operations, financial losses, reputational damage, and legal consequences, among others; (b) prioritizing risks based on the risk scoring system and organization priorities, focusing on high-risk, high-impact scenarios first; (c) developing actionable recommendations for risk mitigation and remediation through the development of a playbook to guide organizational actions; and (d) prioritizing resource allocation by evaluating the cost of implementing mitigation strategies to the probability of losses from a successful attack.

Transformational IT Leadership (TITL)

Two key challenges of the PASTA framework are: (1) the complexity of execution especially due to the PASTA methodology requiring higher level of cybersecurity expertise, and (2) the difficulty of conducting a thorough analysis required by the PASTA methodology for very large or distributed systems (Allen-Addy, 2023).

The integration of transformational IT leadership principles within the PASTA framework provides a new approach to manage and overcome these two key challenges, specifically by providing the right kind of vision, inspiration, motivation, support, and involvement across the whole organization. This integration offers a novel perspective on the synergy between leadership strategies and cybersecurity resilience. TITL adds a leadership perspective that increases the effectiveness of PASTA. Together, the PASTA-TITL framework provides both a strategic approach that considers the human aspect of cybersecurity and a detailed and focused tactical plan for threat management. PASTA-TITL framework further allows the involvement and commitment of businesspeople to heightened cybersecurity resilience norms to achieve strategic organizational goals. TITL component of the integrated framework emphasizes the role IT leadership and IT vision in fostering a proactive cybersecurity culture. TITL component helps align strategic organizational goals with robust cybersecurity practices and enhance organizational readiness to combat evolving cyberthreats.

While the leadership paradigm is wide-reaching and continues to evolve, the dynamic nature of cybersecurity threats requires cybersecurity research to evolve at an even faster pace (Ganapati et al., 2023). Compared to other organizational contexts, IT is characterized by several idiosyncratic characteristics, including a focus on innovation (Melville & Ramirez, 2008), dynamic and shifting objectives (Prahalad & Krishnan, 2002), and projects with tight timelines. Some researchers suggested that traditional models of leadership may not be robust to the idiosyncrasies of the IT industry (e.g. Hickman & Akdere, 2018), resulting in an emerging domain of IT specific leadership research.

Conceptualizations of leadership that are specific to the IT industry include action-based transformational leadership (Eseryel, 2009; Eseryel & Eseryel, 2013), e-leadership (Avolio et al., 2000), IT (self) leadership (Eseryel et al., 2014; Eseryel, 2020; Eseryel & Biernath, 2024), and functional & visionary leadership theory (Eseryel et al., 2021). The most relevant among these to cybersecurity initiatives is transformational IT

leadership (Eseryel, 2009; Eseryel & Biernath, 2024). Transformational IT leadership (TITL) should not be confused with transformational leadership. Transformational leadership is contrasted with transactional leadership to refer to a leader's ability to motivate and inspire subordinates to contribute beyond their contractual requirements and take ownership of organizational outcomes (Rafferty & Griffin, 2004). Transformational leadership "does not really require the use of technology, or affect IT-related values, beliefs or attitudes" (Eseryel, 2020, p.128). Transformational IT leadership, on the other hand, refers to the ability of a leader to foster a culture of innovative thinking where the followers use IT to improve their work processes and outcomes. The goal of transformational IT leadership is to help followers increase the efficiency and effectiveness of their work by using IT effectively, efficiently, and even by innovating with IT.

Eseryel (2020) investigated instructors' transformational IT leadership in educational settings. She adapted the short form of the transformational leadership scale (Carless et al., 2000) to focus specifically to measure how the transformational IT leadership enables an instructor to: (1) encourage the use of IT, (2) inspire the students by being a highly competent role model in IT use, (3) instill positive IT-related values, and (4) encourage thinking about IT problems in new ways. She found that transformational IT leadership of an instructor increases their students' IT self-leadership (Eseryel, 2000). In another study, Eseryel and Biernath (2024) investigated a similar relationship in large European companies across different industries. This time they adapted the transformational leadership instrument of Podsakoff et al. (1996) to capture transformational IT leadership. According to their study, transformational IT leaders: (1) expect high IT-use performance, (2) articulate an innovative IT vision, (3) foster collaboration through IT, (4) role model IT use, and (5) stimulate others to innovate with IT. They found a positive relationship between team leaders' transformational IT leadership and the team members' IT leadership (Eseryel & Biernath, 2024).

As such, transformational IT leaders do not only articulate an innovative IT-vision and expect an IT-intensive performance. They also model their vision with their behaviors, and support individuals' and teams' use of IT. While still emerging, a few studies have adopted this conceptualization of leadership. For example, Pittenger et al. (2022) found that when IT governance practices are highly formal, the ability of transformational IT leaders to innovate is reduced, both in traditional IT contexts and the digital domain.

In summary, leadership theories developed for military, manufacturing, or service industries may not be effective at predicting behavior related to IT-use, or behavior in the IT industry, which is characterized by continuous innovation. A few IT industry-specific leadership theories are emerging, primary among these, transformational IT leadership, which is adopted for the current paper. Transformational IT leadership is relevant to understanding leadership effectiveness in a cybersecurity context, not only because cybersecurity is a domain of the IT industry, but also because cybersecurity is characterized by a constant need for innovation, an ability to react and adapt quickly and by a need for cybersecurity professionals who are willing to work beyond their contractual obligations and take ownership of the safety of organizational systems and data.

PASTA-TITL Threat Modeling Framework

Moving an organization from ad-hoc cybersecurity initiatives to adopting and implementing the PASTA-TITL framework is an example of a major organizational transformation. Transforming organizational vision with IT requires strong IT-enabled transformational leadership (Eseryel & Eseryel, 2013; Eseryel, 2019, p.47).

This section details how transformational IT leadership principles can be strategically used for the success of each stage of the PASTA framework. By overlaying transformational IT leadership components onto specific stages of the PASTA framework, this study aims to unveil how transformational IT leadership can augment the efficacy of cybersecurity measures. Figure 2 presents the PASTA-TITL framework. PASTA stages presented in the first column of the Figure 2 and the TITL behaviors are presented in the first row. The TITL behaviors include the five constructs provided by the study of Eseryel and Biernath (2024). We call the sixth construct "navigating individuals' IT psychology". Eseryel and Biernath (2024) had included in their study another variable called 'individualized support' referring to the degree of attention that the TITL pays to the followers on a more personal basis. Yet, during the adaptation and pilot-testing of their survey, this variable had lost its face value and was removed from the analysis. They recommended researchers to include

individualized support construct in their study but adapt the construct "to specifically address individuals' feelings, fears, and anxieties about information technologies" (p.21). Lastly, we include a seventh construct called "modeling ethical leadership", that we deemed absolutely necessary at least for the cybersecurity context.

	COMPONENTS	Expecting High IT-Use **P**erformance	Articulating an Innovative IT **V**ision	Fostering **C**ollaboration through IT	**R**ole Modeling IT Use	Navigating **I**ndividuals' IT Psychology	**S**timulating others to Innovate with IT	Modeling **E**thical Leadership
	Acronyms	P	V	C	R	I	S	E
PASTA STAGES		**TRANSFORMATIONAL IT LEADERSHIP**						
1	**Define Objectives**		V	C				E
2	**Define Technical Scope**	P					S	
3	**Application Decomposition**			C		I		
4	**Threat Analysis**				R	I		E
5	**Vulnerability Analysis**			C				
6	**Attack Modeling**		V					
7	**Risk & Impact Analysis**	P		C				E

Figure 2. PASTA-TITL Framework for Cybersecurity Resilience

PASTA-TITL Stage 1: Define Objectives

Figure 3 shows the PASTA-TITL stage 1. This stage combines PASTA stage 1, "Define Objectives" stage, with relevant Transformational IT Leadership principles. This stage outlines the goals and scope of threat modeling.

To set the direction during this stage, transformational IT leaders can motivate their teams by outlining a compelling and innovative IT vision for business and cybersecurity resilience. The transformational IT leadership behavior ***of articulating an innovative IT vision*** refers to envisioning an IT-intensive work, where individuals always seek new ways to use IT for accomplishment of the work. When this TITL behavior is adapted into the PASTA framework, the innovative IT vision should also have aspects of cybersecurity resilience embedded into it. Finally, this TITL principle suggests that transformational IT leaders can get others in the organization committed to their innovative IT vision about cybersecurity resilience.

Secondly it is important to develop an innovative IT vision statement that consistently aligns with strategic organizational goals and simultaneously fosters a proactive cybersecurity culture at all levels of the

organization. This could be achieved with the Transformational IT Leadership principle of ***fostering collaboration through IT***. When applied to the cybersecurity setting, this principle refers to the transformational IT leader being able to get individuals, groups, and departments to work together the same goal, specifically the goal of achieving cybersecurity resilience, in their collaboration through IT. Transformational IT leaders further develop a positive attitude towards cybersecurity resilience using this principle. Finally, this principle would allow all staff to uphold stringent cybersecurity measures. As a result, this principle plays an important role in instilling a sense of responsibility among teams to uphold stringent authentication practices.

While not a principle in the current TITL framework, we recommend adding a new TITL principle of ***modeling ethical leadership*** to the first PASTA stage, advocating for the integration of an emphasis to ethical leadership into the Transformational IT Leadership model. This addition would recognize the important role that IT leaders have in providing ethical leadership as a guiding principle across all stages of the PASTA framework, ensuring alignment with ethical standards and principles. By prioritizing ethical leadership within an organization, leaders can create a culture where individuals feel empowered and motivated to uphold high ethical standards, even beyond what is strictly required by regulations or guidelines. Ethical leaders set a positive example and create an environment where ethical behavior is valued and rewarded, inspiring others to act ethically in all aspects of their work, including the use of IT.

Transformational IT Leadership Principles			PASTA Stage
Articulating an Innovative IT Vision	Fostering Collaboration through IT	Modeling Ethical Leadership	PASTA Stage 1: Define Objectives

Figure 3. PASTA-TITL Stage 1

At the C-suite level, the emphasis remains on ensuring alignment between cybersecurity objectives and overall organizational goals and ethical standards. Leaders within this tier contribute to ***articulating an innovative IT vision*** on cybersecurity resilience. CIO's and C-level executives are key to the development of a strong non-IT business leadership team and getting their buy-in (Eseryel, 2019) for an innovative IT vision prioritizing cybersecurity resilience. They can further support this process by integrating a strong and centralized change management function, which covers role development and access security within the system, training, communication, and documentation (Eseryel, 2019).

C-suite leaders articulate the overarching vision for the organization's security posture, emphasizing the criticality of authentication methods, and fostering a culture that promotes vigilance and consistently high standards of security practices across all departments.

PASTA-TITL Stage 2: Define Technical Scope

Figure 4 presents the PASTA-TITL stage 2. This stage combines PASTA stage 2, "Define Technical Scope," with relevant Transformational IT Leadership principles.

The PASTA stage of "Define Technical Scope" requires the technical staff to delineate the boundaries and parameters of the system's technical scope. This involves ensuring that the technical environment is resilient against cybersecurity threats. The technical environment refers to infrastructure, network, applications, and

software components. These threats directly relate to defining technical boundaries, software integration points and data handling practices.

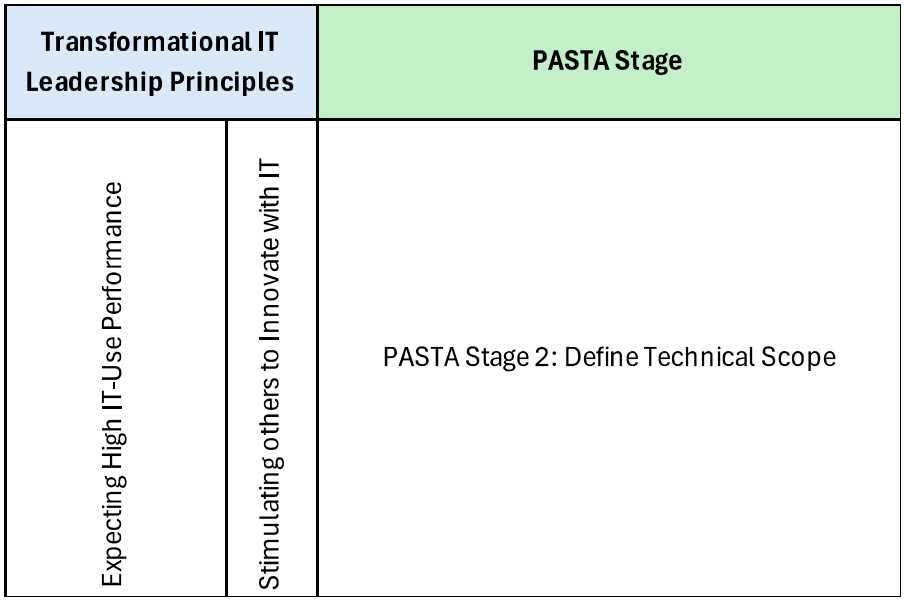

Figure 4. PASTA-TITL Stage 2.

Two transformational IT leadership principles related to PASTA stage 2. Transformational IT leaders' ***high IT use performance expectations*** would create an IT culture where best cybersecurity practices are applied in the integration system and transfer of data. Another transformational IT leadership principle that is relevant is ***stimulating others to innovate with IT***. This TITL behavior motivates the leaders to provide as much access to different levels of users to be innovative with IT, while ensuring strict cybersecurity measures. This approach is supported by the board and C-suite level, who provide strategic direction for defining technical boundaries and help set policies ensuring resilient technical boundaries against such threats. Leadership at the executive level emphasizes the importance of aligning technical scopes with broader organizational objectives, fostering a culture of adherence to technical guidelines set forth by the leadership team.

PASTA-TITL Stage 3: Application Decomposition

Figure 5 illustrates the PASTA-TITL stage 3. This stage combines PASTA stage "Application Decomposition," with relevant Transformational IT Leadership principles.

Application decomposition helps conduct a more detailed threat analysis by partitioning systems into smaller, manageable units. This may include dividing end-to-end transactions into functionalities, and dependencies between these functionalities. Then users' interaction with these functionalities can be managed by defining and controlling user roles. User roles establish the match between organizational roles and the type of access that is appropriate within the system.

The primary focus of the application decomposition is on analyzing the application's structure and functionality, and the interaction between the functionalities. Transformational IT leaders may help this process especially by involving key non-IT functional middle managers in this stage. An example of this is provided by the Med-Global case (Eseryel, 2019), where non-IT functional managers were involved with role-development within the system. These roles were then used to create levels of access security, and for training the employees for the transactions for which their security levels allow access (Eseryel, 2019). Such involvement by middle managers across different departments helps define the correct access security to avoid elevation of privilege, i.e., allowing an individual to do something above their authorization level. By managing authentication requirements that allows each transaction to be attributed to a user with appropriate security level, risk of repudiation is reduced. In other words, it would be undeniably clear who executed which transaction in a system.

Transformational IT Leadership Principles		PASTA Stage
Fostering Collaboration through IT	Navigating individuals' IT Psychology	PASTA Stage 3: Application Decomposition

Figure 5. PASTA-TITL Stage 3.

A transformational IT leader may achieve this level of involvement by ***navigating individuals' IT psychology*** to the functional or departmental managers. This leadership behavior involves understanding the anxieties, fears, and other negative feelings of functional managers towards IT. With this understanding the transformational IT leaders can present the cybersecurity-related initiatives not as an IT-initiative, but as a business and strategy-driven initiative, where the involvement of functional managers is imperative. Another transformational IT leadership principle that supports the involvement of non-IT functional managers is ***fostering collaboration through IT***. By creating work environments were collaboration between teams and departments are made simple and easy with IT, transformational IT leaders make the necessary knowledge exchange among functional managers from different departments and IT staff smooth and effortless. These two TITL principles increase the involvement of key middle managers in the cybersecurity resilience initiatives, thereby further increasing the buy-in and resulting compliance to cybersecurity measures by the businesspeople. By involving functional managers in establishing protocol, transformational IT leaders develop a proactive risk management culture.

CIO's and C-level executives should continue emphasizing the importance of involvement of the non-IT middle managers in contributing to and promoting the cybersecurity initiatives' alignment with organizational goals. C-level executives emphasize the importance of proactive risk management, aligning it with the organization's strategic objectives.

PASTA-TITL Stage 4: Threat Analysis

Figure 6 depicts the PASTA-TITL stage 4. This stage combines PASTA stage 4, "Threat Analysis" stage, with relevant Transformational IT Leadership principles.

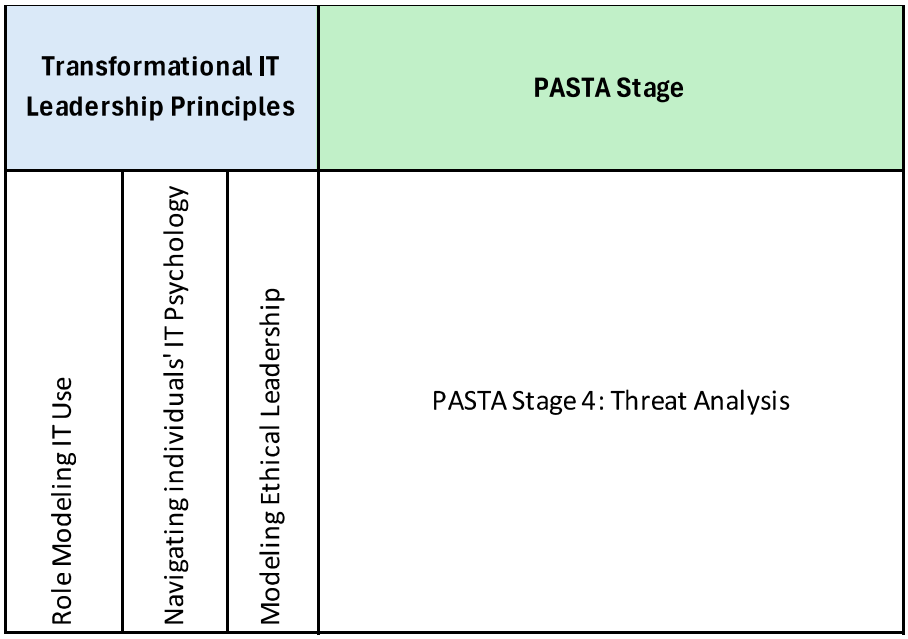

Figure 6. PASTA-TITL Stage 4.

In the previous stage (stage 3) the application environments and details were captured. Stage 4 focuses on identifying and understanding potential threats, and how they relate to the organization's technical environment.

This is a stage where attack scenarios are identified, and list of threat agents and attack vectors are made, and threat intelligence is obtained related to the identified attack scenarios.

Transformational IT leaders' key contribution to this stage is ***role-modeling IT use*** and ***modeling ethical leadership***, which play crucial roles in ensuring cybersecurity decisions align with ethical standards. This stage emphasizes ethical decision making ***influenced by ethical leadership***. Transformational IT leaders should include middle management by ***navigating their IT psychology.*** Further TITL should influence the actions of functional managers through ***role modeling IT-use*** when aligning threat analysis strategies with ethical guidelines set forth by corporate boards. ***Navigating individuals' IT psychology*** includes empathizing with the anxieties and fears of individuals (in this case non-IT business managers) with regards to information technologies. Further, it includes supporting and empowering them to contribute to the threats analysis based on their knowledge of their business processes and their departments' functional use of enterprise-wide systems. Alignment ensures that decision-making processes concerning cybersecurity threats uphold ethical standards and organizational values, fostering trust and integrity within the team and across stakeholders.

The board and C-suite provide guidance on aligning threat analysis strategies with the organization's ethical standards and organizational values. Leaders at all levels should foster a culture of understanding by considering diverse perspectives throughout the PASTA stages. In fact, many organizations now seek cybersecurity expertise from individuals with a wide range of experiences and from an array of disciplines (Holt et al., 2009). Thus, ***navigating individuals' IT psychology*** is an important transformational IT leadership behavior when directing the development of cybersecurity guides and training, especially for those risks that are only understood well by a small number of team members who can use their expertise to perform a good analysis. This approach not only strengthens the organization's cybersecurity posture but also fosters a sense of inclusivity and collaboration among team members.

PASTA-TITL Stage 5: Vulnerability Analysis

Figure 7 illustrates the PASTA-TITL stage 5. This stage combines PASTA stage 5, "Vulnerability Analysis" stage, with relevant Transformational IT Leadership principles.

Transformational IT Leadership Principle	PASTA Stage
Fostering Collaboration through IT	PASTA Stage 5: Vulnerability Analysis

Figure 7. PASTA-TITL Stage 5.

The "Vulnerability Analysis" stage involves a detailed examination of system susceptibilities and potential weaknesses. This stage connects vulnerabilities with organization's assets. In this stage all relevant cybersecurity threats are addressed. Analyzing system parameters and configurations helps detect vulnerabilities that could be exploited. Transformational IT Leadership principles of ***fostering collaboration through IT*** empower teams to collaboratively identify and mitigate vulnerabilities within organization's assets proactively and in collaboration with the functional employees who are working at relevant levels of the organization.

At the C-suite level, ensuring that resources are appropriately allocated to strengthen an organization's security posture and that vulnerability assessments align with the organization's risk appetite and strategic goals is paramount.

PASTA-TITL Stage 6: Attack Modeling

Figure 8 shows PASTA-TITL stage 6. This stage combines PASTA stage 6, "Attack Modeling" stage, with relevant Transformational IT Leadership principles.

During the "Attack Modeling" stage, threats are evaluated and scrutinized more deeply to understand potential attack scenarios. To counter identified attacks, the focus is on modeling possible attack vectors and scenarios based on identified vulnerabilities. Understanding potential attack methods helps an organization devise effective mitigation strategies to counter potential attacks and reduce their impact. Strategic leadership should guide this process by ensuring these strategies align with long-term organizational objectives and sustainability goals. Countering attacks involves simulating or analyzing scenarios and pathways for unauthorized privilege escalation. Transformational IT Leadership should ***articulate an innovative IT vision*** that connects strongly to cybersecurity resilience to guide proactive measures here and are essential for effective risk mitigation. At the C-suite level, ensuring the strategic direction aligns with attack analysis, and allocating time and resources to the analysis of assets that are core to organization's strategic advantage is essential.

Transformational IT Leadership Principle	PASTA Stage
Articulating an Innovative IT Vision	PASTA Stage 6: Attack Modeling

Figure 8. PASTA-TITL Stage 6.

PASTA-TITL Stage 7: Risk and Impact Analysis

Figure 9 presents the PASTA-TITL stage 7. This stage combines PASTA stage 7, "Risk, and Impact Analysis" stage, with relevant Transformational IT Leadership principles.

The "Risk & Impact Analysis" stage is the final stage of the framework. This stage assesses the potential risks posed by identified vulnerabilities and their potential impact. The goal is not just to identify risks but identifying countermeasures for mitigation, and risk reduction.

Transformational IT leadership reinforces compliance with risk mitigation measures while fostering a culture of ethics and accountability regarding potential threats. While integral underpinning to every stage, the proposed transformational IT leadership principle of ***modeling ethical leadership*** is especially important in the risk and impact analysis stage, as it ensures that risk analysis decisions align with ethical standards. Still, leaders should emphasize ethical principles by incorporating ethics review checkpoints throughout the PASTA framework. It should not be assumed that team members understand the ethics that should be applied, meaning ***modeling ethical leadership*** is needed to set the stage across the organization (see Dark, 2011 on information assurance and security ethics).

Transformational IT Leadership Principles			PASTA Stage
Expecting High IT-Use Performance	Fostering Collaboration through IT	Modeling Ethical Leadership	PASTA Stage 7: Risk & Impact Analysis

Figure 9. PASTA-TITL Stage 7.

At the C-suite level, ensuring ethical considerations and alignment with organizational values during risk and impact analysis is crucial. Further, feedback loops and learning sessions should be incorporated after each stage to ***foster collaboration through IT. High IT-use performance expectations*** are especially critical during the risk and impact analysis stage. This facet encourages ongoing learning and adaptation to enhance cybersecurity measures continuously.

To summarize, we presented the PASTA-TITL framework (Figure 2) and how different components of the integrated framework support each other. Specifically, we shared the PASTA stages with their corresponding implications for both the C-suite and transformational IT leaders to show how organizations can holistically manage cybersecurity risks. An integrated approach ensures that leadership strategies and management decisions align with the organizational goals. Ultimately, this fosters a culture of cybersecurity resilience and proactive risk mitigation.

Conclusion

PASTA-TITL framework expands on the human element so critical to threat modeling. PASTA-TITL framework increases cybersecurity resilience by overcoming two major challenges of an otherwise strong PASTA framework: the complexity of execution, and the challenge of thorough analysis in very large or distributed systems (Allen-Addy, 2023). Therefore, this model is directly applicable to practitioners, who would like to use PASTA-TITL for cybersecurity resilience.

Our contribution to leadership theory is two-fold: (1) we presented the application of specific transformational IT behaviors to the cybersecurity field. (2) We extended the transformational IT leadership theory (Eseryel & Biernath, 2024) to include two additional behaviors: navigating individuals' IT psychology and modeling ethical leadership. Role modeling is an important part of transformational leadership. Since TITL is focused on IT leadership of transformational leaders, the 'role modeling' component specifically focuses on the transformational IT leader modeling the kind of effective and innovative IT use behaviors that they aspire the followers to follow. In our efforts to combine TITL with PASTA, we determined the need for the transformational leader to become a role model in ethical leadership. Thus, we recommend both 'navigating individuals' IT psychology' and 'modeling ethical leadership' to be empirically tested in future studies on TITL.

This study emphasizes that cybersecurity resilience cannot be accomplished solely by IT staff. Moreover, it cannot be solely attained with IT and technical solutions. PASTA-TITL model expands on the human element that is imperative to cybersecurity. Involving users, middle management, and the C-Suite is imperative in dealing with cyber-threats. Thus, development of internal transformational IT leaders is essential to planning to avoid, mitigate, and control cyberthreats. Transformational IT leaders in turn will help all participants to be fully involved in cybersecurity initiatives. Further they will help create a culture that upholds stringent cybersecurity measures. Such understanding is fundamental for enhancing organizational cybersecurity resilience and fostering more ethical decision-making practices in the face of evolving threats.

References

Allen-Addy, C. (2023, September 29). *Threat modeling methodology: PASTA*. IriusRisk. Retrieved June 6, 2024 from https://www.iriusrisk.com/resources-blog/pasta-threat-modeling-methodologies

Anderson, R., & Moore, T. (2007). Information Security Economics and Beyond. In: Menezes, A. (eds) Advances in Cryptology - CRYPTO 2007. *Lecture Notes in Computer Science*, vol 4622. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74143-5_5

Ardagna, C., Corbiaux, S., van Impe, K., & Ostadal, R. (2023, October 19) *ENISA threat landscape 2023* Retrieved May 1, 2024 from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 .

Avolio, B. J., Kahai, S., & Dodge, G. E. (2000). E-leadership: Implications for theory, research, and practice. *The Leadership Quarterly*, *11*(4), 615-668. https://doi.org/10.1016/S1048-9843(00)00062-X

Avolio, B. J., Zhu, W., Koh, W., & Bhatia, P. (2004). Transformational leadership and organizational commitment: Mediating role of psychological empowerment and moderating role of structural distance. *Journal of Organizational Behavior* 25 (8), 951–968. https://doi.org/10.1002/job.283 .

Avolio, B. J., & Yammarino, F. J. (2013). *Transformational and charismatic leadership: The road ahead (*10th ed.). Emerald Group Publishing. https://doi.org/10.1108/S1479-357120135 .

Bass, B. M. (1985). *Leadership and performance beyond expectations.* New York: Free Press.

Bedi, P., Gandotra, V., Singhal, A., Narang, H., & Sharma, S. (2013). Threat-oriented security framework in risk management using multiagent system. *Software: Practice and Experience*, *43*(9), 1013-1038, https://doi.org/10.1002/spe.2133

Brown, M. E., Treviño, L. K., & Harrison, D. A. (2005). Ethical leadership: A social learning perspective for construct development and testing. *Organizational Behavior and Human Decision Processes*, 97(2) 117-134. https://doi.org/10.1016/j.obhdp.2005.03.002

Carless, S. A., Wearing, A. J., & Mann, L. (2000). A short form measure of transformational leadership. *Journal of Business and Psychology*, *14*(3), 389-405. https://doi.org/10.1023/A:1022991115523

Dark, M.J. (2010). *Information assurance and security ethics in complex systems: Interdisciplinary perspectives*. https://doi.org/10.4018/978-1-61692-245-0

Eseryel, U. Y. (2009). *Leadership in a non-traditional setting: Self-managing virtual IS development teams* International Conference in Information Systems, http://aisel.aisnet.org/icis2009/65

Eseryel, U. Y. (2019). The case of "Med-Global": IT-enables innovation and implementation by non-IT business unit leaders. *Strategy & Leadership,* 47(2), 43-48. https://doi.org/https://doi.org/10.1108/SL-01-2019-0013

Eseryel, U. Y. (2020). Enabling IT self-leadership in online education. *Interdisciplinary Journal of e-Skills and Lifelong Learning*, *16*, 123-142. https://doi.org/10.28945/4684

Eseryel, U. Y., Bakker, D., & Eseryel, D. (2014). Information technology self-leadership and its influence on team level product and process innovation. *Journal of Leadership and Management*, 1(2), 95-109. https://jleadershipmanagement.org/doc/2014_V2_95-109_JLM.pdf

Eseryel, U. Y., & Biernath, P. (2024). The influence of transformational IT leadership on the IT leadership of followers. *Journal of Leadership and Management,* 10(1) 11-29. https://jleadershipmanagement.org/doc/JLM_Vol10_Iss1_Jan2024.pdf

Eseryel, U. Y., & Eseryel, D. (2013). Action-embedded transformational leadership in self-managing global information systems development teams. *The Journal of Strategic Information Systems*, *22*(2), 103-120. https://doi.org/10.1016/j.jsis.2013.02.001

Eseryel, U. Y., Crowston, K., & Heckman, R. (2021). Functional and visionary leadership in self-managing virtual teams. *Group & Organization Management*, 46(2), 424-460. https://doi.org/10.1177/1059601120955034

Fairfax, L. M. (2018). The securities law implications of financial illiteracy. *Virginia Law Review*, *104*(6), 1065-1122.

Ganapati, S., Ahn, M., & Reddick, C. (2023). Evolution of Cybersecurity Concerns: A Systematic Literature Review. *Proceedings of the 24th Annual International Conference on Digital Government Research,* 90-97.

Hickman, L., & Akdere, M. (2018). Effective leadership development in information technology: Building transformational and emergent leaders. *Industrial and Commercial Training*, *50*(1), 1-9. https://doi.org/10.1108/ICT-06-2017-0039

Holt, S., Bjorklund, R., & Green, V. (2009). Leadership and culture: Examining the relationship between cultural background and leadership perceptions. *Journal of Global Business Issues*, *3*(2).

Hueca, A., Manley, B., & Rogers, L. (2020). Building a cybersecurity awareness program. https://apps.dtic.mil/sti/pdfs/AD1112780.pdf

Jarvis, David (2023, August 14). *Tech talent is still hard to find, despite layoffs in the sector*, Deloitte Insights, Retrieved Jan 1, 2024 from https://www2.deloitte.com/us/en/insights/industry/technology/tech-talent-gap-and-skills-shortage-make-recruitment-difficult.html

Lohrke, F. T., & Frownfelter-Lohrke, C. (2023). Cybersecurity research from a management perspective: A systematic literature review and future research agenda. *Journal of General Management*. https://doi.org/10.1177/03063070231200512

McKinsey Global Institute (2023, June 14), What is digital transformation. Retrieved Feb 1, 2024 from https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-digital-transformation

Melville, N., & Ramirez, R. (2008). Information technology innovation diffusion: An information requirements paradigm. *Information Systems Journal*, *18*(3), 247-273. . https://doi.org/10.1111/j.1365-2575.2007.00260.x

Palo Alto Networks (2022). *What's next in cyber: A global executive pulse check, 2022 global survey*, Palo Alto Networks, Retrieved Feb 10, 2024 from https://start.paloaltonetworks.com/rs/531-OCS-018/images/PANW%20WNIC%20Report_FINAL.pdf?utm_source=marketo&utm_medium=email&utm_campaign=Global-DA-EN-22-11-04-7014u000001VQAEAA4-P3-%5BGTM%5D-whats-next-in-cyber-report

Pittenger, L. M., Berente, N., and Gaskin, J. (2022) Transformational IT leaders and digital innovation: the moderating effect of formal IT governance. *The Data Base for Advances in Information Systems* 53(1), 106-133. https://doi.org/10.1145/3514097.351410 4

Podsakoff, P. M., MacKenzie, S. B., & Bommer, W. H. (1996). Transformational leader behaviors and substitutes for leadership as determinants of employee satisfaction, commitment, trust, and organizational citizenship behaviors. *Journal of Management, 22*(2), 259-298. https://doi.org/10.1016/S0149-2063(96)90049-5

Prahalad, C. K., & Krishnan, M. S. (2002). The dynamic synchronization of strategy and information technology. *MIT Sloan Management Review*.

Rafferty, A. E., & Griffin, M. A. (2004). Dimensions of transformational leadership: Conceptual and empirical extensions. *The Leadership Quarterly*, *15*(3), 329-354. https://doi.org/10.1016/j.leaqua.2004.02.009

U.S. Securities and Exchange Commission (2023). *Press Release SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*, U.S. Securities and Exchange Commission. Retrieved 26 July 2023 from http://www.sec.gov/news/press-release/2023-139

UcedaVélez, T. & Morana, M. M. (2015). Risk centric threat modeling: Process for attack simulation and threat analysis. Wiley. 2015. ISBN 978-0-470-50096-5. DOI:10.1002/9781118988374

UcedaVélez, T. (2021, November 23). *Why PASTA threat modeling?* Vesprite. Retrieved June 6, 2024 from https://versprite.com/blog/what-is-pasta-threat-modeling/

Uzunov, A.V., & Fernandez, E.B. (2014). An extensible pattern-based library and taxonomy of security threats for distributed systems. *Computer Standards & Interfaces*, 36(4), 734–47. https://doi.org/10.1016/j.csi.2013.12.008

Verizon (2023), *Verizon Data Breach Investigations Report 2023,* https://www.verizon.com/about/news/2023-data-breach-investigations-report