Human Factors in Cybersecurity, Vol. 127, 2024, 9–18
https://doi.org/10.54941/ahfe1004761

Proposing a DESM-Based Analytical Framework for the Enterprise Cyber Defender

Rahmira Rufus[1], Ulku Clark[1], Geoffrey Stoker[1], Jeff Greer[1], and Thomas Johnston[2]

[1]University of North Carolina, Wilmington, NC 28403, USA
[2]University of Maryland, Adelphi, MD 20783, USA

ABSTRACT

This paper proposes an analytical framework for the next generation of cybersecurity architecture and strategy to assist the enterprise cyber defender. We built an enterprise system model for practitioner use by leveraging representative enterprises as critical infrastructure operators to achieve a learning objective. The learning objective is to assist the cyber defender with developing the enterprise cybersecurity architecture and strategy via the framework. The focus is to investigate an awareness, education, and training (AET) approach aimed at human factors concerning the role of the enterprise cybersecurity architect, where one architectural perspective is concerned with the successful operation of the enterprise. In contrast, the other is focused on the operation not failing. The goal is to identify the cybersecurity practitioner's progress outcomes via a process prescribed by the Descriptive Enterprise System Model (DESM) as an adapted analytical framework for cybersecurity architect utilization (Clark et al., 2023). The objective is to 1st utilize the framework's three-tiered structure and 2nd that the process targets resolving Crume's three key factors for cybersecurity architecture roles and tools: (1) understanding how the system operates, (2) what is the potential for failure, and (3) what is the threshold to circumvent failure (Crume, 2023)?

Keywords: Enterprise cybersecurity, Human factors, Cyber defender, Analytical framework, Awareness, education, and training (AET), Descriptive enterprise system model (DESM), Cybersecurity architect

INTRODUCTION

Human factors affecting and influencing aspects of cybersecurity are vastly skewed, but a significant contributor to increases in human error with cybersecurity can be associated with the lack of awareness, education, and training (AET). This might be due to limited research exposing the gaps and correlations among the human entity within the general cybersecurity discussion. Other considerations could be that the human element at the core of cybersecurity plays a fundamental role in the complexity of cyberspace. Nevertheless, one can generalize that existing factors benefit cybersecurity while others are detrimental to it.

Now the cybersecurity architect's practice for developing security by design is beneficial to cybersecurity education. For the next generation of computing, this cybersecurity architecture training provides an applicable component to complement the theoretical aspects of teaching, thus drastically reducing the learning curve for the cybersecurity practitioner focused on protecting cyberspace. It begins by mapping the goals of the cybersecurity architect to that of the information technology (IT) architect, where the IT architect designs a practical and optimizable solution that works, and the cybersecurity architect designs a stable, safe, and resilient solution that is fault tolerant (Crume, 2023). The work conducted in this paper focuses on improving the practitioner use while concurrently studying enterprise cybersecurity by leveraging representative enterprises as critical infrastructure operators via models. The next section demonstrates how such modeling can be derived from analytical frameworks designed with a cyber security focus that is tailored to specific usability factors and operating environment usage scenarios.

LEVERAGING FRAMEWORK DEVELOPMENT FOR CYBER DESIGN AND MODELING

Developing an analytical framework for enterprise cyber defense involves structuring a systematic approach to understanding, analyzing, and responding to cyber threats tailored to the enterprise threat landscape. A structured framework to consider entails but is not limited to the following concepts (see Table 1). Enterprise cyber defenders adhering to the analytical components of a framework structure like the example below can systematically assess, prioritize, and mitigate cyber risks to protect organizational assets and maintain operational resilience.

Table 1. Enterprise cybersecurity-based analytical framework components.

Framework Components	Descriptions
Asset Inventory: Identification & Prioritization **NIST SP 800-53: CSF (NIST, 2023)**	Identify all assets within the enterprise, including hardware, software, data, and personnel. Prioritize assets based on their criticality to the business operations.
Threat Intelligence Gathering: Threat Hunting & Modeling **NIST SP 800-150 (NIST, 2014)**	Gather intelligence on potential threats, including known vulnerabilities, attack vectors and emerging risks Utilize both internal sources (logs, incident reports) and external sources (threat feeds, industry reports).
Patch & Vulnerability Mgt: Assessment **NIST IR 8011 vol.4 (NIST, 2020)**	Conduct regular vulnerability scans and assessments to identify weaknesses in systems, applications, and networks. Prioritize vulnerabilities based on severity and exploitability.
Risk Assessment **NIST SP 800-30 (NIST, 2023)**	Evaluate the potential impact and likelihood of exploitation for identified vulnerabilities. Assess the risk tolerance of the organization and align mitigation efforts accordingly.

(Continued)

Table 1. Continued

Framework Components	Descriptions
Defense Strategy Development **(DoD, 2011)**	Develop a comprehensive defense strategy that incorporates preventive, detective, and responsive measures. Consider a defense-in-depth approach, leveraging multiple layers of security controls.
Incident Detection & Response **NIST SP 800-86 (NIST, 2006)**	Implement robust monitoring and detection capabilities to identify suspicious activities and security incidents in real-time. Establish clear incident response procedures to contain, mitigate, and recover from security breaches.
Security Awareness & Training **NIST SP 800-50 (NIST, 2022)**	Educate employees and stakeholders about cybersecurity best practices, including phishing awareness, password hygiene, and data protection. Conduct regular training sessions and simulations to reinforce security awareness.
Continuous Improvement & Adaptation **(NICE, 2020)**	Regularly review and update the analytical framework based on lessons learned, evolving threats, and changes in the business environment. Foster a culture of continuous improvement and adaptability within the cybersecurity team.
Compliance & Governance **NIST IR 8286C (NIST, 2022)**	Ensure compliance with relevant regulatory requirements and industry standards (GDPR, HIPAA, ISO 27001). Establish clear governance structures and accountability mechanisms for cybersecurity within the organization
Collaboration & Information Sharing **NIST SP 800–150 (NIST, 2016)**	Foster collaboration with external partners, industry peers, and government agencies to share threat intelligence and best practices. Participate in industry forums and working groups to stay informed about emerging threats and trends.

Each framework component in the left column is above the security standard (in bold) that the component briefly describes in the column to the right. Theoretically, all the cyber defense practitioner would need to do is develop an enterprise security architecture and/or strategy that uses these components and the organization would have a sound security declaration, policy and protection procedures to ensure an effective secure operating environment, protocols and posture for the enterprise. However, the problem evident in the DESM proposal by Clark et al. demonstrates how applying cybersecurity concepts are not that simple, specifically for enterprise platform use cases. The reason is that the modern enterprise presents challenges for the cyber defense practitioner studying enterprise cybersecurity because of multilevel enterprise-wide risk management (see Figure 1) problems when developing effective modeling techniques (Clark et al., 2023).

ENTERPRISE ARCHITECURE MAPPING

In this work, the focus is to investigate an AET approach. The approach is aimed at human factors concerning the roles of the enterprise to condition and better equip the cybersecurity defender executing enterprise cybersecurity architecture operations. Crume illustrates how the cybersecurity architect can protect the enterprise by understanding the role of the IT architect, where the architectural perspective of the IT role is concerned with the successful operation of the enterprise. In contrast, the cybersecurity architect is focused

on the operation not failing based upon the IT understanding (Crume, 2023). The analytical framework developed in this paper includes the addition of the enterprise architecture (EA) perspective. This EA viewpoint can provide the cybersecurity practitioner (now as the learner/student) with an additional layer of comprehension that extends out to the priorities of the enterprise represented in the NIST tiered risk management approach (see Figure 1).

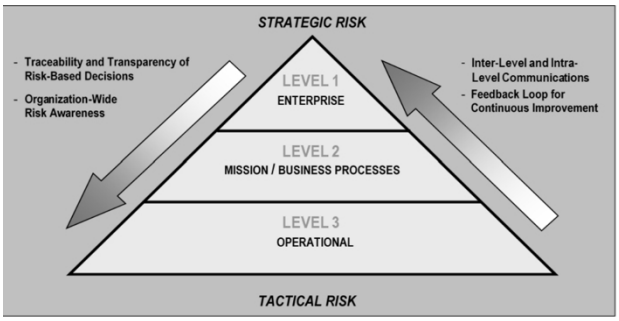

Figure 1: Multilevel enterprise-wide risk management (Boyens & Smith, 2022).

DESM's goal is to produce models reflecting perspectives for studying enterprise cybersecurity. To effectively learn how to manage strategic risk, the student's viewpoint is required to be proficient at Level 1 to adequately defend the enterprise. In addition, the DESM should cultivate utilization of relevant information required for strategic risk management decision making, which addresses the scope and complexity of a system of digital systems at Level 1. The EA stakeholder correlation (see Table 2) can be captured in a framework structure where the framework components are employed (see Table 1).

Table 2. Enterprise architecture (EA) stakeholder mapping.

Each stakeholder role has a focused mindset, tools of their trade and domains where they operate…			
Role	**Enterprise Architect**	**IT Architect**	**Cybersecurity Architect**
Focus	Organization's holistic business processes, information systems & technology infrastructure.	Organization's information systems & technology infrastructure design.	Security infrastructure for entire organization (processes, information systems, technology, data, etc.)
Mindset	Enterprise strategic goals, technical capabilities & infrastructure alignment	Focused successful enterprise operation & optimization	Focused on enterprise not failing & understands how enterprise functions
Tools	Business context diagrams, organizational flows & high-level architectures	Systems & networks diagrams; solutions, implement & deployment architectures, etc.	Security & risk architectures, assessments, threat & maturity models, etc. (aligning to enterprise & IT architects' materials in columns to left

(Continued)

Table 2. Continued

Each stakeholder role has a focused mindset, tools of their trade and domains where they operate…			
Domains	• Business Architecture • Application/Service • Information/Data • Tech/Infrastructure	Architecture Types: • Specific Domains • Technical • Solution • Implementation • Deployment	In the Appendix, there are 25 cybersecurity domains. (See Table 3)
All Roles Perform	• Collectively perform planning, designing, testing, implementing & maintaining organization's systems, devices, data, network, processes, infrastructure, priorities, vision, etc. • Leverage frameworks, reference architectures, models, etc.		

METHOD

This research focuses on the cybersecurity practitioner's progress outcomes by proposing an analytical framework for next-generation cybersecurity architecture and strategy for the enterprise. The process begins by building an enterprise system model for practitioner use to develop next-generation enterprise cybersecurity strategy centered around resolving three key factors: (1) understanding how the system operates, (2) what is the potential for failure, and (3) what is the threshold to circumvent failure (Crume, 2023)? Next, the opportunity to position a Descriptive Enterprise System Model (DESM) developed by Clark et al. as an adapted analytical framework for cybersecurity architect utilization is instituted. The framework uses a three-tiered axis decomposing the enterprise function, its attack surface structure/condition, and the abstraction of the attack surface. All three of these components are essential to enterprise cybersecurity proficiency development because cybersecurity architects require decision-making support to secure a large-scale complex system of systems like a modern enterprise. The learning objectives accomplished in this work via the framework are for cyber defenders who need to understand how enterprise function shapes attack surface structure and condition and how to manage enterprise risk in the presence of incomplete information.

DESM AS A FRAMEWORK MODELING COMPONENT

The analytical framework is constructed from DESM via all the elements needed to represent the enterprise as a conceptual model. This is performed to develop risk treatments plans, make risk-informed decisions, etc. for the cyber defender to leverage (see Figure 2). The analytical framework is structured as a series of cyber analysis that confirms each enterprise state or condition as prescribed via the DESM model. The analytical framework process begins by resolving the key factors (see Figure 3) in the initial landscape analysis. Following the landscape is the stakeholder analysis and the process continues until the risk considerations are conducted in the risk analysis phase.

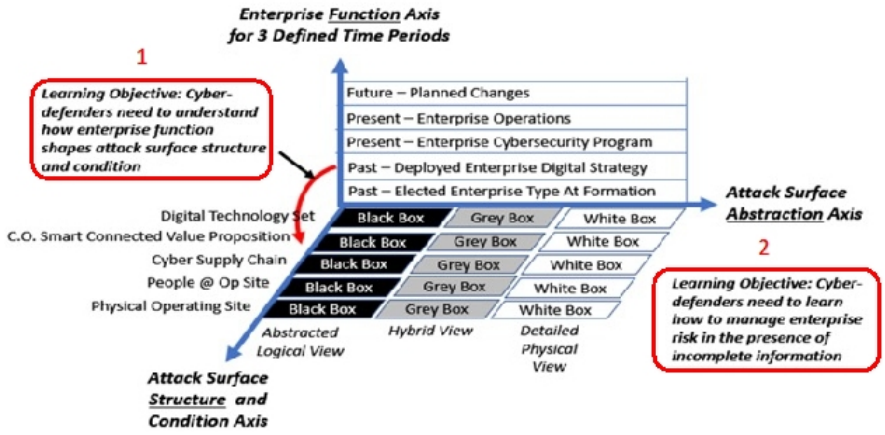

Figure 2: Adapted DESM framework (Clark et al., 2023).

The Enterprise Cyber Defender Analytical Framework provides the learner the opportunity to systemically approach the nuances and complexity of the enterprise function from the viewpoint that analyses, and educational progression or growth is happening concurrently in a lateral and vertical direction while not limiting, losing or lacking the ability to administer the enterprise situation, scenario or event.

Analyses	Extraction Description	Derivatives	Framework Processes
Landscape	Operating environment (OE), data & process workflows	Enterprise OE Assets Inventory	1. understand how the system operates, 2. what is the potential for failure, 3. what is the threshold to circumvent failure?
Stakeholder	Owners & authorizers of landscape	Charts: RACI, MOCHA, etc.	EA Stakeholder Mapping (Table 2)
Gap	Comparing the actual level of performance to the desired level of performance	As-Is → To-Be	DESM Adapted Framework (Figure 2)
Threshold	• What are the cybersecurity concerns resulting from the gap analysis? • What is the plan to address the gaps?	Progress Outcomes A	Learning Objective 1 (Figure 2)
Impact	• Within the threshold, what are the major security factors to focus on? • What are the vulnerabilities & weaknesses to assets discovered?	Progress Outcomes B	Learning Objective 2 (Figure 2)
Threat	Identify the realization of vulnerabilities & weaknesses → assets = threats (via attack vector)	Progress Outcomes C	• Framework Components (Table 1) • Cybersecurity Domains (Table 3)
Risk	What is the condition or state that the proposed threat compromise puts enterprise in?	• Risk Treatment Plan • Risk-informed decisions	Multilevel Enterprise-Wide Risk Management (Figure 1)

Figure 3: Enterprise cyber defender analytical framework.

This framework has been designed to utilize its execution in the virtual learning environment developed for real-world, sensory input simulation to heighten the cyber defense experience for the enterprise function. The next

iteration of this research will focus on the outcomes, experimentation, etc. resulting from the implementation.

CONCLUSION

This paper developed an analytical framework structure that focused on the cybersecurity practitioner's progress outcomes to study enterprise cybersecurity via simulated cyber enterprises. The process began with the creation of a model for enterprise systems tailored for practitioners, aimed at crafting a next-generation cybersecurity strategy addressing three critical elements: understanding system operations, anticipating potential failures, and determining the threshold to prevent these failures (Crume, 2023).

Following this, we used the the Descriptive Enterprise System Model (DESM) proposed by Clark et al. as a modified analytical framework for cybersecurity architects. This framework employs a three-tiered approach, breaking down enterprise function, attack surface structure/condition, and the abstraction of the attack surface. Each of these elements are necessary for enhancing proficiency in enterprise cybersecurity because cybersecurity architects need support in making decisions to safeguard intricate systems such as modern enterprises. The learning objectives achieved through this framework are twofold: firstly, for cyber defenders who must comprehend how enterprise function influences attack surface structure and condition, and secondly, for managing enterprise risk when confronted with incomplete information.

APPENDIX

In Table 3 there are 25 cybersecurity domains with definitions gathered from NIST, ISC2, Infosec, etc. for the cyber architect role domains field (see Table 2). These domain selections are to be used in conjunction with the framework components and other elements required to utilize the Enterprise Cyber Defender Analytical Framework developed in the paper.

Table 3. Cybersecurity domains for DESM to guide framework construction.

	Cybersecurity Domain	Description
1.	Security Operations	Detecting and protecting sensitive and business critical information within any organization.
2.	Identity & access management	Managing user identities, access controls, and authentication mechanisms to ensure that only authorized individuals access certain data or systems.

(Continued)

Table 3. Continued

	Cybersecurity Domain	Description
3.	Network security	Combines multiple layers of defenses at the edge and in the network. Implementing advanced measures such as intrusion detection and prevention systems, firewalls, and secure network architecture to protect against unauthorized access and threats to network infrastructure.
4.	Governance	Process of making and enforcing decisions within an organization or society. It encompasses decision-making, rule-setting, and enforcement mechanisms to guide the functioning of an organization or society.
5.	Security assessment & testing	Determines the performance and design of an organization's security.
6.	Asset security	Covers the concepts, structures, principles, and standards that monitor and secure assets.
7.	Application security	Focuses on the techniques used to protect applications from threats and vulnerabilities from design to development and into the deployment and maintenance stages.
8.	Physical security	Protecting people, property and tangible assets from situations and occurrences that could cause harm or loss.
9.	Software development security	Helps professionals understand how to apply and enforce software security. Additionally, deals with issues regarding the internally developed applications and/or systems.
10.	Risk assessment	Process of carefully analyzing the workplace for identifying scenarios, processes, et cetera that might cause harm to assets.
11.	Risk management	Monitors, assesses, and manages the risks that organizations and their users are exposed to.
12.	Risk strategy	Encompasses actions and activities that reduce the impact of risk by helping organizations reduce or control the likelihood of risk turning into an issue and mitigating the severity to minimize any negative consequences.
13.	Threat Intelligence	Involves data collection, processing, and analysis; organized, analyzed and refined information about potential or current attacks that threaten an organization.
14.	Frameworks and standards	(1) Guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk; (2) Guidelines, best practices, and compliance benchmarks organizations must achieve to control their environments effectively.
15.	Security & risk management	Deals with the people and processes; Security and risk management ensures the security threats and risks are at an acceptable level.
16.	Security architecture	Unified security design to address the potential risks and requirements of a specific condition or environment.

(Continued)

Table 3. Continued

	Cybersecurity Domain	Description
17.	Security architecture & engineering	Covers several important information security concepts: engineering processes using secure design principles; fundamental concepts of security models; security capabilities of information systems; assessing and mitigating vulnerabilities in systems; cryptography; designing and implementing physical security.
18.	Education	Strategy used by IT and security professionals to prevent and mitigate user risk, designed to help users and employees understand the role they play in helping to combat information security breaches.
19.	Career development	Certifications, conferences, peer groups, self-study, training and other activities associated with the rise in demand for knowledgeable and certified cybersecurity personnel.
20.	Regulatory compliance	Process of complying with applicable laws, regulations, policies and procedures, standards, and the other rules issued by governments and regulatory bodies
21.	Cryptography	Practice and study of techniques for secure communication in the presence of adversarial behavior.
22.	Enterprise risk management	Includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives
23.	IT policies & procedures	Maximize IT value and promote the most productive usage of IT products and services.
24.	Security engineering	Includes network security and computer operations security and emphasizes technical expertise to prevent attacks on both the network and the host.
25	Vulnerability Management	Systematically identifying, assessing, and remediating software vulnerabilities, using tools like vulnerability scanners and implementing patch management strategies.

REFERENCES

Boyens, J., Smith, A. (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations SP 800–161 Rev. 1. Retrieved from NIST, (Department of Commerce, Washington, D. C.), May 05, 2022. https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final.

Clark, Ulku, Jeff Greer, Rahmira Rufus, and Geoff Stoker. (2023). "A Descriptive Enterprise System Model (DESM) Optimized for Cybersecurity Student and Practitioner Use", Cham: Springer Nature Switzerland. In: International Conference on Human-Computer Interaction, pp. 610–621.

Crume, J. (June 13, 2023) "Cybersecurity Architecture: Roles and Tools," YouTube Website: https://www.youtube.com/watch?v=E9pHJRRfAhw&list=PLOspHqNVtKADkWLFt9OcziQF7EatuANSY&index=6

Department of Defense Strategy for Operating in Cyberspace (2011) July 01, 2011. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

National Institute for Cybersecurity Education (2020) Workforce Framework for Cybersecurity (NICE Framework), July 07, 2020. https://niccs.cisa.gov/workforce-development/nice-framework

National Institute of Standards and Technology (2006) NIST issues SP 800-86, Guide to Integrating Forensic Techniques into Incident Response (Department of Commerce, Washington, D. C.), September 01, 2006. https://csrc.nist.gov/pubs/sp/800/86/final

National Institute of Standards and Technology (2020) NIST Released Draft Internal Report 8011-vol. 4, Automation Support for Security Control Assessments: Software Vulnerability Management (Department of Commerce, Washington, D. C.), April 28, 2020. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST. IR.8011–4.pdf

National Institute of Standards and Technology (2014) NIST Released Draft Special Publication 800-150, Guide to Cyber Threat Information Sharing (Department of Commerce, Washington, D. C.), October 28, 2014. https://csrc.nist.gov/news/2014/nist-released-draft-special-publication-800-150

National Institute of Standards and Technology (2023) NIST issues SP 800–53 Release 5.1.1 in Cybersecurity and Privacy Reference Tool. (Department of Commerce, Washington, D. C.), Change Notice November 07, 2023. https://csrc.nist.gov/news/2023/cybersecurity-and-privacy-reference-tool-update

National Institute of Standards and Technology (2023) Guide to Conducting Risk Assessments, Overview of NIST SP 800-30, Revision 1. (Department of Commerce, Washington, D. C.), September 14, 2023. https://csrc.nist.gov/presentations/2023/guide-to-conducting-risk-assessment-sp-800-30-rev

National Institute of Standards and Technology (2022) Updates to NIST SP 800-50: Building a Cybersecurity and Privacy Awareness and Training Program, and SP 800-16: Information Technology Security Training Requirements: A Role and Performance-Based Model (Department of Commerce, Washington, D. C.), September 01, 2022. https://csrc.nist.gov/presentations/2022/update-to-nist-sp-800-50800-16

National Institute of Standards and Technology (2022) Released Draft Internal Report 8286C, Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight (Department of Commerce, Washington, D. C.), September 14, 2022. https://doi.org/10.6028/NIST. IR.8286C

National Institute of Standards and Technology (2016) Updates to NIST SP 800–150, Guide to Cyber Threat Information Sharing (Department of Commerce, Washington, D. C.), October 04, 2016. https://www.nist.gov/publications/guide-cyber-threat-information-sharing