Human Factors in Cybersecurity, Vol. 127, 2024, 1–8
https://doi.org/10.54941/ahfe1004760

Using DESM to Demonstrate How Behavior Can Impact an Enterprise's Physical Attack Surface Structure

Rahmira Rufus, Ulku Clark, Geoffrey Stoker, and Jeff Greer

University of North Carolina, Wilmington, NC 28403, USA

ABSTRACT

This paper addresses behaviors affecting the attack surface structure of a simulated enterprise model. The work conducted identifies human factors that contribute to the enterprise's physical attack surface. Such factors can be social engineering, phishing, insider threats, inadequate employee awareness and training (AET), etc. By leveraging a Descriptive Enterprise System Model (DESM), we demonstrate how behavior impacts the enterprise's physical attack surface structure. The focus in this phase of the research is associating human factors that contribute to this condition. The model is leveraged to make two observations: (1) isolate behavior functionally as a factor impacting the enterprise's physical attack surface and (2) isolate human factors as an indicator of an enterprise's behavior.

Keywords: Physical attack surface, Human attack surface, Human risk management, Attack surface structure, Human systems integration, Systems engineering

INTRODUCTION

A Descriptive Enterprise System Model (DESM) was developed by (Clark et al., 2023) to support the diverse learning aptitudes necessary for the next generation of cybersecurity leaders. Specifically, the model focuses on designing a descriptive enterprise system for student and practitioner use that builds proficiency in business theory, risk management principles, and methodologies essential for effective cybersecurity strategy, implementation, and operations. The model proposes how the structure of the enterprise's physical attack surface is impacted by the enterprise type, the digital strategy and its behavior. This paper addresses behaviors affecting that attack surface structure. This work identifies human factors contributing to context for making decisions, assumptions supporting risk recommendations, mitigations, treatment plans, etc. Other aspects of developing an effective cybersecurity program are addressed, such as policies, procedures, protocols, tactics, techniques, etc.

Web interfaces such as the MITRE Common Attack Pattern Enumerations and Classifications (CAPEC) and repositories like the NIST National Vulnerability Database (NVD) are platforms that provide understanding and enhance defenses for adversary activities with known attack patterns, vulnerabilities, etc., to equip the cybersecurity practitioner better (MITRE, 2023), (NIST, 2005). However, the learning curve associated with synthesizing information and dealing with the ambiguity required to anticipate how

the adversary operates is not readily available for how enterprise function/behavior impacts its attack surface structure and condition (MITRE, 2023). Such an interface would be helpful in training enterprise cyber-defenders. It would also require a more detailed mapping of behaviors to an attack surface. The behavior-to-attack surface correlation must be established for such a novel approach. The work conducted here acts as a preamble for this future research area.

In this work, we use DESM to demonstrate how behavior impacts an enterprise's physical attack surface structure. The model is leveraged to make two observations: (1) isolate behavior functionally as a factor impacting the enterprise's physical attack surface and (2) isolate human factors as an indicator of an enterprise's behavior. The emphasis for performing the activities to establish the first observation is distinguishing behavior from the other two factors that DESM illustrates: type and digital strategy. After behavior has been isolated as a condition impacting the physical attack surface, criteria for the second observation are established, where factors relating to the 'human-in-the-loop' play a significant role in the behavioral aspects of the enterprise's security posture.

HUMAN ATTACK SURFACE

Fly suggests that with all the security tools and technology invested in over the decades, most cyber incidents are still a result of human error (Fly, 2021). Factor in that over a decade ago the same exploits were the highest factors with percentages to overall breaches, incidents and exploits. There are emerging vulnerabilities and weaknesses that threaten cyberspace, but what is significant about the compromises provided in Table 1 is that in 2022 a survey of companies from 2021 reported that out of 80% of breaches discovered, 40% of that total were never seen prior (Aiyer et al., 2022). The remaining half of that total were human factors that were common as with prior years. Based upon these metrics, it seems that the human continues to play a major role in the exploits discovered year after year. However, the data from these reports were not focused on the impact that the human entity had on cybersecurity breach data in comparison to the progression of the cybersecurity industry. In this work, we look at this finding closer to isolate human behaviors to the physical attack surface.

Table 1. Cybersecurity industry progression & human influenced exploits (Fly, 2021), (Verizon, 2022–2023).

	2011…	2021	2022	2023
Industry Global Spend	55 billion	230 billion	Increase by 12.4% each year	
Security Companies	300+	3000+	4000+ sample (both years)	
Verizon Data Breach Investigations Report (DBIR)	• Phishing • Malware	• Phishing • Malware • Passwords	80% of breaches total had 40% as novel exploits, but not with human factors	• Phishing • Stolen Creds • Exploited Vulnerabilities • Insider Threat
Breaches Confirmed	667	5250	366.7 million	299.8 million (18% decrease)

The human attack surface refers to the vulnerabilities within an organization stemming from human behavior, interactions and actions that can be exploited by attackers (IBM, 2022). This includes employees, contractors and other individuals associated with the organizational structure. The exploits commonly associated with leveraging the human entity, within the given operating environment, are social engineering, phishing, insider threats, inadequate employee awareness and training (AET), access control, security policies and procedures and cultural awareness. Therefore, the enterprise structure can reduce the human attack surface via a combination of improving these exploit categories through education, training, access controls, security policies, effective organization, etc. to reduce the risk of human-related security breaches and strengthen the enterprise's overall security posture. However, before the assertion can be made, in this work we make the correlation amongst the human factors to discriminate and isolate the human behavior from the remaining factors: the enterprise type and the digital strategy.

METHOD

What is accomplished in this work is identifying human factors that contribute to the enterprise's physical attack surface. These factors are required to be extracted by leveraging DESM proposed by Clark et al., and then demonstrate how the behavior impacts the enterprise's physical attack surface structure. The goal, which is called the correlation process, is associating human factors that contribute to this enterprise condition as a unique component separate from the remaining factors. Additionally, we use DESM to make two observations: (1) isolating behavior functionally and then (2) isolating human factors to the enterprise's behavior.

THE CORRELATION PROCESS

The objectives for achieving the goal sub (1) isolating behavior functionally, were performed by doing the following:

1. Identifying behavior in the generalized attack surface by mapping the same behavior within the human attack surface scope. Basically, by identifying the same behavior in both attack surface classes for the superset general physical attack surface structure and within the subset human attack surface, a relationship is established amongst both attack surfaces. Additionally, we are structuring the attack surface classes via a hierarchy, where the human attack surface is a subset of the general physical attack surface class. This makes associating the human attack surface factors with the general scope that affects the enterprise condition easier to map.

    i) In this step, we breakdown the function of the human attack surface to make intersections for behavior associated with the enterprise example.
    ii) Next, we capture those functions as factors that impact the attack surface specific to the enterprise scope.

iii) Finally, we reach goal sub (1) where behavior is isolated but also supporting the opportunity to progress to goal sub (2) where connecting the human as an isolating factor of the enterprise condition can begin.

2. The objectives for achieving the goal sub (2) to isolate human factors as an indicator of an enterprise's behavior, were performed by doing the following:

   i) Begin with the established correlation derived in goal sub (1) to make the determination that both attack surfaces have a dependency relationship.
   ii) The behavior needs to completely isolate human factors as being a stand-alone indicator that can contribute to the enterprise condition.
   iii) Following the 2nd set of isolation factors, begin demonstrating the enterprise's dependency upon the human entity via operations, such as employees, contractors, and visitors that are vital end-users for the enterprise.
   iv) Lastly, make the correlation that the premises established can associate that an enterprise's behavior is affected by the human entity.

DESM MODEL EXECUTION

If we revisit how to utilize the DESM created in Clark et al., the model framework has an enterprise function axis, enterprise attack surface axis and attack surface abstraction axis (see Figure 1). As stated previously, the goal of this work is to isolate behavior as a function and human factors as a behavioral indicator to an enterprise's physical attack surface condition. What is significant about utilizing DESM in this experimentation, is that DESM's framework functions in a manner to understand, classify and map such relationships to effectively develop risk mitigation plans for the enterprise. The focus in this experiment is to make the associations of the enterprise behavior be defined under a subset attack surface class unique to the human entity.

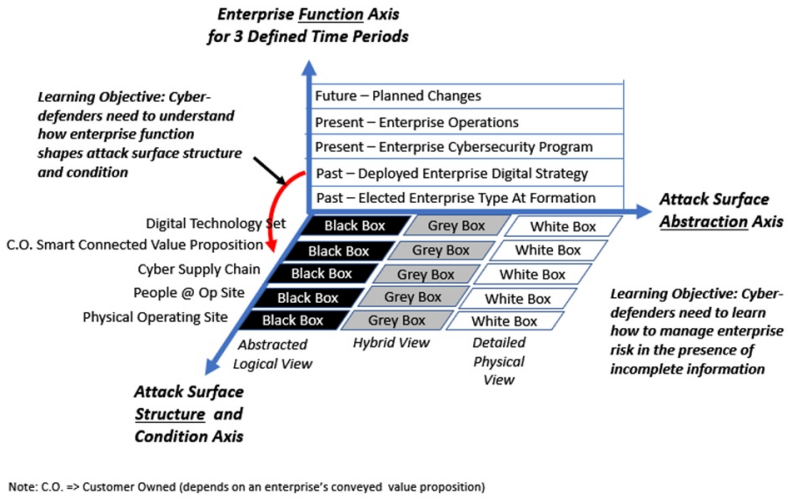

Figure 1: Adapted DESM framework (Clark et al., 2023).

Within the enterprise function axis are three time periods to consider: past, present and future, with each being categorized by relevant management decisions and actions. All the determinations made in this axis, effect the enterprise's attack surface and its condition. The enterprise attack surface has five elements that involve digital technology, the enterprise's customer owned smart connected IoT products (depending upon the enterprise's value proposition), the cyber-supply chain, people associated with the enterprise and physical operations. Lastly, is the abstraction of the attack surface, which aids when dealing with complexity. In this axis, individual categories can be decomposed with much detail. An example would be when full detailed information is required for managing operations (Clark et al., 2023).

PHYSICAL ATTACK SURFACE

After DESM requirements are established to use the model, the physical attack surface is decomposed to emphasize the human factors subset and to create human related elements that are a condition of the DESM framework. Figure 2 provides the subset attack surfaces for the holistic physical attack surface. Human factors are a subset of the physical attack surface, where people associated with the enterprise represent potential vulnerabilities in the physical attack surface.

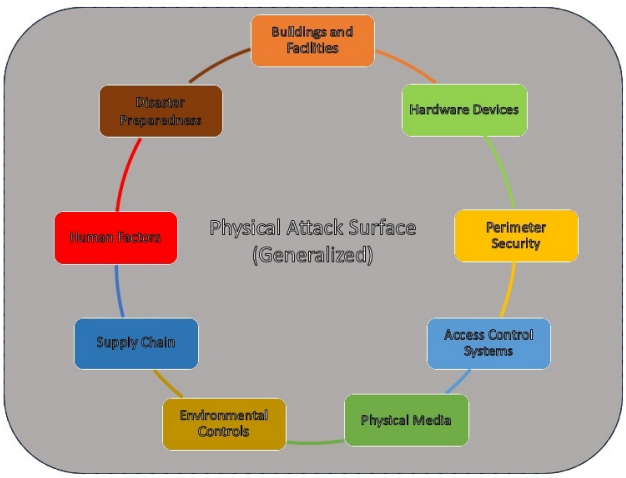

Figure 2: Physical attack surface subcomponents.

Table 2 describes the human factors occurring with DESM. The enterprise function axis uses states in time, however the determinations that result from this axis are dependent upon managerial inputs, which are conducted by human entities. Even for systems that might employ administrative decisions to be automated or determined by an intelligent agent, there is often a 'human-in-the-loop' associated with final determinations. Also, a human would at minimum act as an authoritative entity within the decision chain. Therefore, the enterprise function axis is impacted by human factors that contribute to its attack surface condition and structure. Lastly, the generalized

time provisions created to assess the enterprise function axis are also dependent upon human factors since the notion of time is not associated with a uniquely coded time stamp that digital entities utilize. The notion of past, present and future are relative terms that ultimately have more context with human cognition and levels of understanding.

The enterprise attack surface examines the digital technology set deployed for mission achievement, customer owned smart connected IoT products, a cyber-supply chain focused on enterprise digital needs, people aligned with the enterprise and the physical operating site being defended (Clark et al., 2023). In the table, digital technology is impacted by humans in technology reviews and selections. Also, the cultural awareness needed to appropriately conduct 'bake-offs' require experience in knowing which technologies to acquire or deploy for specific usability factors. Device technology and the cyber-supply chain are affected by the human entity because the human entity is the primary or purposed end-user of the devices. The cyber-supply chain is also a subset in the physical attack surface and integrates with the human factors' subset. There is an opportunity for future research here because the alignment of intersecting attack surface subsets demonstrates how each contribute to the interworking's of the holistic physical attack surface. People associated with the enterprise and physical operations are a given understanding that human factors apply here. People are the enterprise and the physical operations, which include the other eight subsets illustrated in Figure 2 that are also describing the enterprise personnel that physically run the enterprise.

Table 2. Correlations from DESM attack surface axes to human factors.

Human factors	Enterprise Function	Enterprise Attack Surface	Attack Surface Abstraction
Social Engineering Phishing Insider Threats	N/A	Device technology & the cyber-supply chain are affected by the human entity; the human is the purposed device end-user.	All boxes in this axis (white, black & gray) are dependent upon human factors because each scenario requires a human entity.
Poor AET Access Control Security Policies & Procedures	Management decisions are impacted by human entity	Supply chain is also subset in the physical attack surface & integrates with the human factors' subset. People are the enterprise and physically run the daily operations	
Cultural Awareness	Notion of time is a cultural concept only understood by a human entity	Digital technology set deployed for mission achievement is impacted by humans during procurement & acquisitions	N/A

The attack surface abstraction axis presents the cyber defender that leverages the framework the autonomy to abstract the attack surface classes to an underlying detail that would normally be complicated to capture. This axis allows for decomposition of the categories, where three levels are illustrated via white, black and gray boxes. The entire axis is dependent upon human

factors because the abstraction is only relevant to human entities. In this axis the human entities have varying levels of visibility within the enterprise. The black box has very limited information as would the malicious entity attacking the enterprise. The white box has much detail at the physical level such as the network administrator, system developer or some super user. The gray box is in the middle where some information is available, and some is not.

CONCLUSION

Human factors play a considerable role in the behavior of an enterprise's physical attack surface structure. In this work, we demonstrated the process to isolate behavior as a function of an enterprise's physical attack surface structure by using a Descriptive Enterprise System Model (DESM) framework. In addition, the behavior was based upon human factors that contribute to these conditions. Contributors to these conditions were a combination of education, training, access controls, security declarations and policies, organizations, etc. The primary goal of this work was to leverage DESM to accomplish the following: (1) isolate behavior functionally as a factor impacting the enterprise's physical attack surface and (2) isolate human factors as an indicator of an enterprise's behavior. DESM was selected for this method because the DESM framework demonstrates how enterprise function or behavior impacts the structure and condition of its attack surface to increase cybersecurity proficiency for cyber professionals. By addressing the human attack surface via a model helped to segregate behaviors affecting the attack surface structure of an enterprise from other remaining factors prescribed by Clark et al., being the enterprise type and the digital strategy.

NEXT STEPS

The behaviors evaluated in this work encompass a wide range of actions and practices within the human attack surface subset as employees, contractors, and other individuals associated with the enterprise. These behaviors can either increase or decrease an organization's vulnerability to cyber threats and the combination of education, training, access controls, and policies, organizations can reduce the risk of human-related security breaches and strengthen their overall security posture. Such determinations were not the primary focus of this work. However, future iterations of this research will dive deeper into the outcome of these behaviors that impact the enterprise's physical attack surface structure.

REFERENCES

Bharath Aiyer, Jeffrey Caso, Peter Russell, and Marc Sorel. (2003) "Human systems integration in army systems acquisition", [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

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.

Fly, Robert. (2021). "What is Human Attack Surface Management?", [Online]. Available: https://elevatesecurity.com/blog-what-is-human-attack-surface-management/#: ∼: text=Human%20attack%20surface%20is%20the, that%20impact%20an%20organization's%20risk

International Business Machines (IBM). (2022). "What is an attack surface?", [Online]. Available: https://www.ibm.com/topics/attack-surface#: \protect$\relax\sim$:text=An%20organization's%20attack%20surface%20is,to%20carry%20out%20a%20cyberattack.

MITRE Corporation. (2023). "Common Attack Pattern Enumerations and Classification", [Online]. Available: https://capec.mitre.org/index.html

National Institute of Standards and Technology (NIST). (2005). "National Vulnerability Database", [Online]. Available: https://nvd.nist.gov/

Verizon Communications. (2022, 2023). "Data Breach Investigations Report", [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/2023/industries-intro/