Human Factors in Cybersecurity, Vol. 127, 2024, 187–197
https://doi.org/10.54941/ahfe1004778

Integrating Human Factors Into Data-Driven Threat Management for Overall Security Enhancement

Mohammed K. S. Alwaheidi[1], Shareeful Islam[2], Spyridon Papastergiou[3], and Kitty Kioskli[4,5]

[1]School of Architecture Computing and Engineering, University of East London, UK
[2]School of Computing and Information Science, Anglia Ruskin University, UK
[3]Department of Informatics, University of Piraeus, Greece Security Labs Consulting LTD, T12 W7CV, Cork, Ireland
[4]University of Essex, School of Computer Science and Electronic Engineering, Institute of Analytics and Data Science (IADS), Wivenhoe Park, Colchester CO4 3SQ, UK
[5]Trustilio B.V., Vijzelstraat 68, 1017 HL Amsterdam, The Netherlands

ABSTRACT

Human and other non-technological issues are often overlooked, which directly and indirectly contributing to many successful cyber attacks, including DoS, social engineering, download-driven attacks, and more. Considering human issues as causes for internal threats and weaknesses, a deeper understanding of these factors is essential for overall security enhancement. Therefore, organizations of all sizes need to ensure a broad range of knowledge, skills, and awareness among all user levels, from individual end-users to security practitioners. However, this task is challenging due to the evolving nature of business, systems, and threat contexts. To address this challenge, our research represents a significant advancement in holistic and comprehensive threat assessments, surpassing existing practices by considering pertinent human factors. Our approach views humans as potential weaknesses or threats, influenced by various factors. Specifically, it incorporates key human elements, such as motivation, knowledge, context, and privilege, into the threat management process to enhance overall security. These factors are systematically classified and interconnected, facilitating the identification of weaknesses and threats posed by humans within the system context. For example, depending on the context, privilege can be categorized into three levels: organizational, departmental, and unprivileged, with end-user privileges falling into these classifications. Knowledge, as a human factor in this approach, is differentiated into technological and security awareness. Our proposed approach extends data-driven threat modelling by integrating human factors to identify and assess threats related to these factors. We present a conceptual model that combines human factors with cybersecurity concepts, including data, assets, threats, weaknesses, and controls, to assess and manage threats associated with human factors and evaluated from both insider weaknesses and threat perspectives. This contributes significantly to overall security enhancement, including improving the accuracy of threat assessments, identifying new threats, and developing more effective threat mitigation strategies.

Keywords: Threat management, Insider threat, Vulnerabilities, Human factors, Context, Knowledge

INTRODUCTION

Organizations nowadays heavily rely on technology to support their business operations, and the adoption of technology has significantly increased in the post-COVID era. However, this transformation also expands the potential attack surface within the organizational context, posing security risks ranging from low to catastrophic severity. Alongside technical vulnerabilities, human factors are considered significant contributors to exploiting these attack surfaces. Despite the prevalent technology-centric approach in cybersecurity, human-related issues are often overlooked (Lahcen et al., 2018). Recognizing the importance of managing human factors, there is a growing acknowledgment that a comprehensive security assurance framework should consider both technical and non-technical perspectives. A recent ENISA report highlights that human and organizational factors are major contributors to both technical and social vulnerabilities within an organizational context (ENISA, 2020). Therefore, understanding and managing human-related issues are crucial for enhancing overall cybersecurity. Threat modelling plays a crucial role in understanding and mitigating cybersecurity threats. Despite several existing threat modelling approaches, there is a noticeable lack of focus on human factors related threats. In this context, this work extends our initial contribution, which proposed a novel data-driven threat analysis to assess and manage threats based on data generated from three different levels: management, control, and business, and extends this by considering threats stemming from human factors (Alwaheidi et al., 2022a; Alwaheidi et al., 2022b). Specifically, humans are considered as potential weaknesses or threats influenced by various factors within the overall system context.

This paper makes two main contributions. Firstly, it extends the existing data-driven threat analysis approach by incorporating relevant human factors to manage weaknesses and threats related to human factors. These factors are categorized based on whether they represent a weakness or a threat and are assessed to identify the severity of the weakness or threat driven by human factors. Secondly, the proposed approach considers key human-centric attributes, such as motivation, knowledge, context, and privilege, and identifies threats originating from these attributes. These attributes are interrelated, and individual factors are classified into different levels, allowing for the measurement of the impact of human factors on overall threat assessment.

RELATED WORK

Human factors-related vulnerabilities are considered one of the challenging areas for cybersecurity. Cybersecurity events posed by human factors could successfully lead to data or security breaches, and human factors are considered one of the weakest components for security (Lahcen et al., 2018).

Sheng et al. (2017) emphasizes the ongoing effectiveness of phishing attacks and underscores the need for continuous user education to enhance awareness and resilience against evolving social engineering tactics. Another contemporary human factor vulnerability is the persistence of insider threats. Insiders, whether acting maliciously or inadvertently, can pose a significant risk to an organization's cybersecurity. Recent studies, such as that by

Faily et al. (2020), stress the importance of a comprehensive approach to mitigating insider threats, including robust access controls, continuous monitoring of user behaviour, and the integration of machine learning techniques to identify anomalous activities. As the landscape of cyber threats evolves, understanding and addressing these human factors vulnerabilities remain pivotal for organizations striving to fortify their defences and safeguard against potential breaches. However, there is a limited consideration of threat assessment considering human related dimension. This proposed work contributes towards this direction. framework for organizational information security related to the human factor for the Internet of Things is proposed, including possible countermeasures to prevent or reduce data breach incidents (Hughes-Lartey et al., 2021). A structured approach aiming for the Cyber Human Error Assessment Tool (CHEAT) is developed to address human factor considerations in cybersecurity assessments (Widdowson et al., 2015). The approach considers human factors in five distinctive categories: people, organization, history, environment, and technology. Another work emphasize the importance of a socio-technical approach to cyber risk assessment, introducing a multi-dimensional, quantifiable model that incorporates principles from investigative psychology and behavioural science to enhance the accuracy of risk estimates by considering the personality traits of potential attackers and human factors (Kioskli et al., 2023).

All these works provide important contributions to tackling human factors by consolidating various human factors, classifying them into relevant groups, and proposing various methods to address the challenge.

DATA-DRIVEN THREAT MANAGEMENT AND HUMAN FACTORS

Threat modelling has traditionally been technology, threats, or data-centric, often overlooking the focus on human factors in the entire threat analysis process. For instance, the STRIDE threat model focuses on diverse types of threats that a system may face, notably Spoofing or Denial of Service, while kill chains describe the stages that constitute a successful cyberattack (Pollini et al., 2022). However, in today's complex digital ecosystem, where human-technology interactions are increasingly interconnected, there is a necessary need to reconsider this narrow focus. Human factors can be exploited by attackers to gain access to systems and data or to disrupt or damage systems. This research introduces a conceptual model integrating the human factor into the existing d-TM model, offering an advanced perspective on d-TM threat assessment.

DATA-DRIVEN THREAT MODEL (D-TM)

The d-TM aims to comprehensively evaluate threats from all perspectives of data, including extraction, processing, and storage in various systems. This approach enables the identification of potential risks, allowing for the implementation of necessary measures within the overall operational process (Alwaheidi et al., 2022a). The benefit of employing d-TM for threat modelling is its emphasis on the data life cycle within the existing infrastructure.

Specifically, d-TM categorizes data into three abstraction levels: management, control, and business. Each level comprises three distinct phases—at rest, in process, or in transit. This level of abstraction assigns equal importance to data in all stages and identifies attacks from any of these phases. The rationale behind incorporating abstraction levels and phases in d-TM is to ensure the security of data regardless of its location or status within the digital infrastructure. The model recognizes threats, identifies weaknesses, and offers strategies for mitigation. Moreover, the model considers multiple relevant concepts, such as actor, asset, threat, weakness, control, and data, collectively providing a robust framework for identifying and assessing threats within an organization. It adopts common security knowledge for threat assessment.

ADOPTION OF HUMAN FACTOR TO d-TM

As stated before, threat can not only originate from system and other technical element, but human issues can also significantly contribute for potential attack surface. The existing d-TM approach considers the human as an actor within its conceptual model within three types, i.e., business end user, operator, and system. These actor types represent the role of any entity that could interact with business services and system. In particular, end user and operator are considered as human-to-technology interaction, while system reflects the system-to-system interaction. This proposed approach considers human-to-technology interaction as an extension of the d-TM. Note that, exiting d-Tm approach does not consider human factors to the threat analysis. In this context, the proposed work extends the d-TM by incorporating human factors for the threat analysis. Humans, whether as end-users or IT operators, influence the threat landscape and play a pivotal role in safeguarding or carelessly compromising security. Ignoring these variables can lead to incomplete and often misleading threat assessments. There are several benefits to integrating human factors into the d-TM. **Improved accuracy of threat assessments:** By considering human factors, d-TM models can provide more accurate and holistic assessments of the overall potential threats. **Identification of new threats:** New potential threats can be identified based on the human context which are not considered existing d-TM approach. **Enhanced mitigation strategies:** Organizations can develop more effective mitigation strategies by understanding how attackers can exploit human factors.

CONCEPTUAL VIEW OF HUMAN FACTORS ADOPTED d-TM

This research proposes a novel approach to integrating human factors into d-TM. The conceptual view provides a common understanding of the concepts used for the human factors adopted in d-TM. Hence, it accurately and precisely assigns meaning to the concepts and models them in a way that anyone with no prior knowledge will understand human factors for threat analysis. The presented conceptual view in Figure 1 seamlessly integrates human-centric attributes such as ‘Motivation,’ ‘Knowledge,’ ‘Context,’ and ‘Privilege’ into the d-TM model. This integration underscores the influence

between humans and technological components, emphasizing the interconnected nature of threats in the modern digital paradigm. By integrating human attributes with the d-TM model, this research pioneers a holistic approach to threat modelling by recognizing humans not just as passive entities but as active influencers of threat landscapes. It highlights the dynamic nature of threats when human variables are introduced.

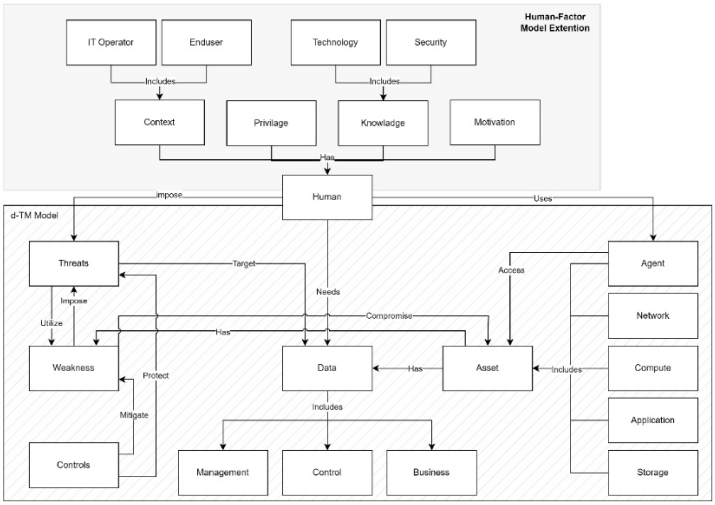

Figure 1: The integrated conceptual model.

The conceptual model illustrates the symbiotic relationships between human attributes such as knowledge, context, privilege, and motivation and their interplay with the d-TM initial concepts such as data, asset, weakness, threat, and control, which are presented in Alwaheidi et al., 2022a; Alwaheidi et al., 2022b. Data is a core concept with a focus on three abstraction levels: management, control, and business for threat assessment. Asset represents any hardware or software utilized by the organization to access or operate underlying business services. Assets are categorized into five types: agent, network, compute, application, and storage. Threats refer to the potential of performing malicious acts that could harm the organization's infrastructure or data, exploiting weaknesses within the system. These weaknesses could be related to code, configuration, or architecture flaws in the system. Controls are determined to mitigate the identified threats; these controls represent a set of policies, procedures, techniques, or technology designed to reduce or eliminate the impact of cyber threats on the organization.

The human attributes are defined as follows: **Context**: It represents the organizational role of the human interacting within an organization. The role plays a significant value in defining the nature of the risk to organizational business, where a privileged system admin could lead to a superior business impact compared to regular end users in case of compromising the system. It includes two roles: **Business End user** (**BE**): Represents an individual in charge of the organization's business operations and has no role in providing

administrative tasks to the organization's infrastructure. This human could hold high privilege access to business-critical operations such as managers. This role can pose a potential threat to the business data level. **Business IT Operator (BO)**: Represents an individual in charge of the organization's technical and administrative tasks. This human is crucial to business operations, which have a massive impact due to privileged access to business-critical infrastructure such as system admin. This role can pose a potential threat to the management data level. **Privilege**: Refers to the scope and depth of access granted to an individual within a system or organizational operation. This access, while imperative for functionality, can also introduce potential vulnerabilities. Therefore, determining the level of privilege is crucial for assessing associated risks. As per the model, the privilege levels are outlined based on distinct contexts: 'Business End user Context' and 'Business IT Operator Context'. Each context is further granulated into three levels of privileges, each bearing its own implications for business or digital services.

CONTEXT 1: BUSINESS END USER

Organization-Level Privileged End User (OPE): An OPE is a business end user granted extensive system privileges across the organization. Their access is not restricted to specific departments but encompasses the entire organizational landscape, including C-levels or general managers. Any intentional or accidental misuse can have an extreme organizational-wide effect, potentially compromising a multitude of departments and overarching business functions.

Privileged End User (DPE): A DPE is a business end user with elevated access privileges, albeit restricted to a specific department or functional unit within the organization. The impact of such privilege is generally localized to their designated department. However, any adverse actions can disrupt the specific department's functions or data, impacting business processes reliant on that department.

Unprivileged End User (UPE): UPEs represent the majority of business end users, possessing only standard access rights. They can utilize systems and resources pertinent to their roles without elevated permissions. Risks associated with UPEs are minimal since their capacity to influence systems or processes is limited. However, mass actions by multiple UPEs or exploits targeting them can still demonstrate significant disruptions.

CONTEXT 2: BUSINESS IT OPERATOR

Multi-system Privileged Operator (MPO): MPOs are IT operators endowed with privileged access across multiple systems within the organization. They can traverse, modify, and control various interconnected systems. Due to their multi-system access, MPOs hold significant influence. Any mistakes or security breaches concerning an MPO can threaten multiple systems, leading to a cascading effect on business operations and digital services. **Single-system Privileged Operator (SPO)**: SPOs are granted elevated access but are limited to a single, specific system. Their domain of influence is limited to that particular system. While an SPO's influence is limited, any concerns arising

from them may disrupt a particular system they manage. Also, any business process or digital service that depends on that system may be impacted. **Unprivileged Operator (UPO)**: UPOs are business operators with standard access rights. They perform routine tasks without any heightened system permissions. Risks associated with UPOs are generally contained due to their restricted access. Nevertheless, any widespread issues affecting multiple UPOs or vulnerabilities targeting them can introduce disruptions.

Knowledge refers to an individual's competence in technological and security-related paradigms. An individual's knowledge is an essential metric in evaluating the maturity of members within an organization. The deficiency of requisite knowledge, particularly in technologies that underpin business operations or security, has been identified as a fundamental cause of various cyber-attacks. The d-TM considers the 'Agent' as a tool used by 'End user' and 'Operator' for day-to-day activities, providing a guide to the technological understanding of the organization. While the rest of the threat layers in d-TM focus on 'Operator' knowledge. In addition to technological awareness, security awareness must also be incorporated. To holistically address potential vulnerabilities arising from knowledge gaps, the proposed model divides knowledge into two distinct types: Technological Awareness (TA): It aims to measure the level of knowledge of the technology used or operated by the organization's individuals. The technology is identified by the process of the d-TM threat analysis that this model leverages. Security Awareness (SA): It aims to measure the level of knowledge of recent cybersecurity attacks targeting humans, such as social engineering. Security awareness is not limited to the business 'End user' but also includes the business 'Operator'; for instance, secure infrastructure deployment. The knowledge level is shown below:

- High - High competence level of technical and security understanding of the system and surrounding infrastructure that the organisation is operating. They are typically well-versed with the latest technology trends, systems, and software and have a proactive approach to security, often anticipating potential vulnerabilities and threats before they appear.
- Medium - Medium competence level of technical and security understanding of the system and surrounding infrastructure that the organisation is operating. Their technical knowledge allows them to use systems less efficiently than well-knowledge individuals, and their security awareness enables them to recognize and counteract common cyber threats.
- Low - Basic level of technical and security understanding of the system and surrounding infrastructure that the organisation is operating. Their technical knowledge might be limited to routine tasks or using particular software and tools. Similarly, their security awareness might be focused on recognizing obvious threats like generic phishing attempts.

Motivation reflects the existence of factors that could drive malicious actions. Organizational individual motivation is an essential element to be assessed. Motivation could be due to internal or external factors, such as financial situations or gain. Identifying and assessing this factor equips

organizations with the ability to proactively mitigate potential cybersecurity vulnerabilities. There are three motivation levels as shown below:

- High - high motivation with an intense drive to potentially abuse or compromise digital assets. Such individuals are likely to be persistent in their actions and might utilize sophisticated means to achieve their objectives.
- Medium - medium motivation with a moderate drive to potentially abuse or compromise digital assets. Such individuals are less insistent than highly motivated individuals, whose motivation is influenced by occasional circumstances and might not go extreme to achieve their objectives.
- Low - limited motivation with a minimal drive to potentially abuse or compromise digital assets including lack a strong reason to act maliciously.

MEASURING HUMAN FACTOR IMPACT

Assessing the human factor is a challenging task. These factors are subjective and personal, making it hard to quantify them accurately. Instead, the research considers an approach that depends on expert judgment and a thorough comprehension of each individual's background, history, and personality with three impact levels. The categorization of impact levels—high, medium, and low—serves as a structured framework to gauge the potential consequences of human actions or oversights within an organization. This differentiation acknowledges the spectrum of human influence, from actions that can jeopardize the very foundation of an organization to minor oversights that, while not critical, offer valuable learning opportunities.

- High - Individuals demonstrate a high impact on organisational business continuity. Such Human actions or oversights lead to severe consequences, often affecting the core functionality or integrity of an organization.
- Medium - Individuals demonstrate a moderate impact on organisational business continuity. Such Human actions or oversights lead to limited consequences, often compromising specific departments or services, but could be contained with no impact on the core functions of the organization.
- Low - Individuals demonstrate a minor impact on non-critical organisational business services. Such Human actions or oversights cause inconveniences rather than genuine disruptions. They are usually addressed promptly and serve as learning points rather than critical incidents.

HUMAN AS AN INSIDER-THREAT

The model considers an individual a potential threat to an organization if 'Motivation' exists. Hence, each individual must be assessed to be cleared or addressed by the organization's security strategy. 'Context' and 'Privilege' are also factors that must be considered when assessing humans as an insider threat. The impact of this threat can be presented in three levels: High, Medium, and Low. Table 1 illustrates the correlation between 'Context,' 'Privilege,' and 'Motivation' to determine the impact of insider threats.

Table 1. A motivation factor impacts levels.

Insider Threat		MOTIVATION		
CONTEXT	PRIVILEGE	High	Medium	Low
Business End user(BE)	OPE	H	H	M
	DPE	H	M	L
	UPE	M	L	L
Business IT Operator(BO)	SPO	H	H	M
	MPO	H	M	L
	UPO	M	L	L

HUMAN AS AN INSIDER-WEAKNESS

The model considers an individual as a potential weakness for an organization if their 'Knowledge' level is not properly maintained. Therefore, each individual must be assessed and addressed by the organization's security strategy. 'Context' and 'Privilege' are also other factors that must be considered when assessing humans as insider weaknesses. The impact of this weakness can be categorized into three levels: High, Medium, and Low. Table 2 illustrates the correlation between 'Context,' 'Privilege,' and 'Knowledge' to determine the impact of insider weaknesses from Business End User (BE) and IT Operator (BO) perspectives.

Table 2. A knowledge factor impacts levels.

Insider Weakness		KNOWLEDGE		
CONTEXT	PRIVILEGE	High	Medium	Low
Business End user(BE)	OPE	L	M	H
	DPE	L	M	H
	UPE	L	L	M
Business IT Operator(BO)	SPO	L	H	H
	MPO	L	M	H
	UPO	L	L	M

RUNNING EXAMPLE

As an example of an insider threat, a financial analyst with "Direct Privilege Execution (DPE)" rights, becomes disappointed with his career at a multinational corporation, and his access to sensitive financial data and transaction capabilities poses a significant insider threat. His growing dissatisfaction serves as a motivational factor, leading to the potential misuse of his privileges to manipulate financial reports or leak confidential information. This intersection of his role, privileges, and personal motivations categorizes him as a "High" impact insider threat, highlighting the critical need for organizations to pre-emptively address such risks through their security strategies to safeguard their interests and ensure continuity. Overall, it is essential to comprehend the value of human factors in an organization's

cybersecurity strategy. They provide insights into potential threats and underlying vulnerabilities posed by insiders. The models emphasize the importance of 'Motivation' in identifying threats and the role of 'Knowledge' in recognizing weaknesses. Additionally, considering the interplay between 'Context' and 'Privilege' further refines these assessments. The effectiveness of any security strategy relies on its ability to comprehend and address the complexities associated with human factors, ensuring strength and adaptability in a changing threat landscape.

CONCLUSION

This research endeavours to address this critical gap by identifying and quantifying the impact of human parameters in the overall threat assessment process. The study extends the existing d-TM approach, recognizing that augmenting the d-TM model with human factors is not merely an extension but a necessity in the contemporary threat landscape. By acknowledging and addressing the interplay between human attributes and technological components, this integrated approach aims to enhance an organization's ability to prepare for, predict, and protect its digital assets effectively. The envisioned outcome is a more resilient and comprehensive cybersecurity framework that takes into account both technology-driven and human-enabled threats. To validate the efficacy of the proposed human factors related threat assessment, the research intends to conduct evaluations within real world scenarios based on existing organizational contexts and threat profiles.

ACKNOWLEDGMENT

The research conducted in this paper was triggered by the authors' involvement in the project 'SECurity And privacy protectioN in Internet of Things devices' (SECANT) under grant agreement No. 101019645, 'Secure OPen source softwarE and hardwaRe Adaptable framework' (SecOPERA) under grant agreement 101070599, and 'Collaborative, Multi-modal and Agile Professional Cybersecurity Training Program for a Skilled Workforce In the European Digital Single Market and Industries' (CyberSecPro) under grant agreement No. 101083594.

REFERENCES

Ait Maalem Lahcen, Rachid, Ram Mohapatra, and Manish Kumar. "Cybersecurity: A Survey of Vulnerability Analysis and Attack Graphs." Springer Proceedings in Mathematics & Statistics, 2018, 97–111.

Alwaheidi, Mohammed K., and Shareeful Islam. "Data-Driven Threat Analysis for Ensuring Security in Cloud Enabled Systems." Sensors 22, no. 15 (2022): 5726.

Alwaheidi, Mohammed K., Shareeful Islam, and Spyridon Papastergiou. "A Conceptual Model for Data-Driven Threat Analysis for Enhancing Cyber Security." Advances in Intelligent Systems and Computing, 2022, 365–74.

ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected." ENISA, August 26, 2021. https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020.

Faily, Shamal, Maria Theocharidou, and Vasilis Katos. "An Exploration of Insider Threat Taxonomies." In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20), 1–10, 2020.

Hughes-Lartey, Kwesi, Meng Li, Francis E. Botchey, and Zhen Qin. "Human Factor, a Critical Weak Point in the Information Security of an Organization's Internet of Things." Heliyon 7, no. 3 (2021). https://doi.org/10.1016/j.heliyon.2021.e06522

Human factors in cybersecurity: Protect yourself - telefónica tech. Accessed November 29, 2023. https://telefonicatech.com/en/blog/human-factors-in-cybersecurity

Kioskli, Kitty, Haralambos Mouratidis, and Nineta Polemi. "Bringing Humans at the Core of Cybersecurity: Challenges and Future Research Directions." AHFE2023, Human Factors in Cybersecurity, 2023. https://doi.org/10.54941/ahfe1003722

Sheng, Steve, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. "Who Falls for Phish?" Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2010. https://doi.org/10.1145/1753326.1753383

Widdowson, A. J., and P. B. Goodliff. "Cheat, an Approach to Incorporating Human Factors in Cyber Security Assessments." 10th IET System Safety and Cyber-Security Conference 2015.