Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The Role of the Human Factor in the Cybersecurity Ecosystem

[1]Claudio Paya Santos, [2]Víctor Rodríguez González, [3]Neidy Zenaida Domínguez Pineda, [4]Javier Diz-Casal, [5]Juan Carlos Fernández-Rodríguez, [6]Juan José Delgado Morán

[1]Valencia International University

claudio.paya@professor.universidadviu.com

https://orcid.org/0000-0002-1908-9960

[2]Isabel I University

Víctor.rodriguez.gonzalez@ui1.es

https://orcid.org/0000-0002-5348-9730

[3]Valencia International University

neidyz.dominguez@professor.universidadviu.com

https://orcid.org/0000-0002-8574-2606

[4]Alfonso X el Sabio University

jdizcas@uax.es

https://orcid.org/0000-0003-1332-8905

[5]Universidad Atlántico Medio, Spain

juancarlos.fernandez@pdi.atlanticomedio.es

https://orcid.org/0000-0003-3312-861X

[6]University Pablo de Olavide. Seville.Spain

jjdelmor@upo.es

https://orcid.org/0000-0002-9945-8235

ARTICLE INFO

Received: 08 Nov 2024

Revised: 27 Dec 2024

Accepted: 22 Jan 2025

ABSTRACT

Cybersecurity has become a critical point for the daily operation of organizations and the protection of individuals in digital environments, which are increasingly complex. Much of the efforts in this area are focused on developing defense tools against possible threats, however, they do not take into account the human factor. This article analyzes the impact of training and awareness in terms of risk reduction and control, along with the role of emotions, cognitive biases, and social engineering. All of them can cause impulsive decisions to be made that are not the most appropriate and generate a security incident. Strategies are proposed to integrate this human factor into protection and prediction models, underlining the need for a fully multidisciplinary approach to encompass all psychosocial dynamics.

Keyword: Cybersecurity; Security incident; Human factor; Social engineering.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Introduction

Cybersecurity has gone from being a purely technical topic to becoming a much broader challenge, involving social, psychological, and behavioral aspects. Today, we live in an interconnected digital world where security breaches are not always due to technological failures, but rather to human error, either due to ignorance or impulsive decisions. For example, common actions such as clicking on a suspicious link, using easy-to-guess passwords, or postponing software updates can open the door to cyberattacks, which, according to recent studies, have human error as the main cause of their success in more than 80% of cases (Verizon, 2022).

The "human factor" in cybersecurity refers to how people interact with technological systems and how their decisions, emotions, and behaviors directly influence the protection or vulnerability of these systems. Although we have made great technological advances, people are still the weakest link in the security chain due to our unpredictability, cognitive biases that affect our judgment, and the ease with which we can be manipulated (Sasse et al., 2020).

In this article, we explore the essential role people play in cybersecurity from several perspectives. We analyze how we respond to threats, how cognitive biases contribute to errors, and (evaluate the effectiveness of programs designed to educate and raise awareness among users). In addition, we review how emotions, confidence, and even impulsivity can influence our safety-related decisions. To illustrate these points, we also include examples of incidents where the human factor has been decisive in facilitating security breaches.

Our main goal is to propose effective ways to integrate the human factor into cybersecurity strategies. Beyond technological tools and solutions, it is necessary to address the role of people with innovative approaches that help reduce the associated risks and that recognize the importance of an interdisciplinary vision on this issue.

Human behaviors and their relationship with cyber vulnerabilities

One of the biggest challenges in cybersecurity is not in the technology itself, but in people's decisions and behaviors when interacting with it. Actions that seem trivial, such as reusing the same password across multiple accounts, postponing a software update, or sharing personal details on social media, can become the entry point for a cyberattack. Although these habits are common, the consequences can be devastating: identity theft, unauthorized access to sensitive data, kidnapping and encryption of information (ransomware), etc.

Why does this happen? In many cases, these behaviors reflect a lack of awareness of the real risks. Many people or organizations have false assumptions about cybersecurity, such as believing that "it will never happen to them" or that security measures are optional, complex, or even annoying. This generates a misperception that cybersecurity is secondary, ignoring that, in the digital environment, small oversights can have big repercussions.

1.1. The Role of Cognitive Biases in Security Errors

In addition, human decisions are shaped by various cognitive biases that make us more vulnerable to digital threats. One of the most common is overconfidence, which leads users to think that they can identify an attack, such as a phishing email, without problems. This bias is reinforced when they have not experienced previous incidents, which generates a false sense of control.

Another frequent bias is normality bias, which leads people to assume that "this won't affect me" or that cybersecurity incidents only happen to large companies or public figures. This thinking minimizes the perception of risk and, consequently, reduces the motivation to adopt preventive measures. For example, someone might think that you don't need to enable two-factor authentication because your account isn't "important enough" to be hacked.

On the other hand, there is security fatigue, which occurs when users are overwhelmed by the number of cybersecurity-related warnings, alerts, and recommendations. This overload can lead

to inaction or even conscious rejection of safety measures. A typical example is ignoring constant notifications to update software or skipping extra verification steps because they seem time-consuming. Although these tools are designed to protect, their excessive or unintuitive implementation can end up generating the opposite effect: total disinterest.

As can be seen, there is a wide variety of cognitive biases that can affect decision-making related to cybersecurity and that cyberattackers use to take advantage of different social engineering techniques. The following table shows a relationship between these biases and casuistry related to the field of cybersecurity.

Type of cognitive bias	Definition	Casuistry
Illusory Truth Effect	Tendency to accept as true something that is frequently repeated, even if it is false.	An employee trusts a fraudulent email because they've received similar versions multiple times and they look familiar.
Selective perception bias	Interpret new information according to previous ideas or beliefs.	A user ignores alerts from security software because they think their system is invulnerable.
Anchoring bias	Relying too much on the first information received when making decisions	A social engineering attack simulates a brand and its corporate image, which it uses as a lure or hook, since the user already had that information as known.
Bandwagon effect	Adopt decisions or behaviors based on what others do, rather than on one's own analysis.	A user accesses a link because their coworkers have done the same.
Framing bias	Influencing decisions depending on how information is presented, rather than analyzing data objectively.	An employee trusts a message that offers a "great opportunity," ignoring the potential risks associated with the link.
Ostrich effect	Avoid facing negative information or risks, preferring to ignore them.	A user checks a fraudulent email and misses a spelling mistake and domain change that would have helped them identify it as malicious.
Confirmation bias	Seek or interpret data in ways that reinforce existing beliefs.	It is impossible for us to suffer a cyberattack, since our company is small and has never happened before.
Automation bias	Tendency for people to trust information provided by automated systems or algorithms, without	An administrator ignores threat alerts because they

	properly questioning or verifying it for themselves	assume that automated tools will solve everything.
Decision fatigue	Reduction in the quality of decisions after making many in a row, due to mental exhaustion.	An analyst approves access requests without thoroughly reviewing them after hours reviewing multiple cases.
Optimism bias or illusion of invulnerability	Belief that something bad is unlikely to happen to us, underestimating the risks.	An employee trusts a suspicious message because they believe they "wouldn't be targeted" and feel immune to falling for a hoax.
Risk Compensation	Tendency to take greater risks because greater security is perceived.	A user shares personal information on a fake website because they believe that they are using a VPN or antivirus that they are completely protected.
Source attribution error or source confusion	Remembering information, but forgetting or confusing the source where it came from, which can lead to errors in judgment.	A worker opens a malicious link in an email because they assume it's from a colleague they recently exchanged messages with.
Obedience to authority	Tendency to follow instructions or suggestions from someone perceived as an authority figure, even when they are unreasonable.	An attacker poses as an employee's boss and, using an authoritarian tone, demands that he urgently transfer funds to a fraudulent bank account.
External Responsibility Bias	Blaming external factors or other people instead of taking responsibility for an action or decision.	A user who falls for a phishing attack blames security software for not detecting it, ignoring its lack of attention to the suspicious message.
Dunning-Kruger effect	Overestimating one's own skills or knowledge in a specific area, while ignoring one's own limitations.	An employee who thinks they have a good understanding of cybersecurity ignores warnings not to share passwords and, feeling safe, falls into a social engineering attack designed to exploit their overconfidence.

Table 1. Cognitive biases and their relationship with cybersecurity. Source: Authors.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

1.2. Humanizing the problem

It's important to remember that behind every click on a malicious link, behind every weak password, there is a person with emotions, priorities, and limitations. Cybersecurity is not only a technical issue, but also a human one. For example, someone who uses the same password on multiple accounts might not be acting out of negligence, but because they feel that remembering multiple passwords is overwhelming or because they underestimate the value of their data. Likewise, someone who postpones updates could be prioritizing urgent work tasks over a protection measure that, although important, they do not perceive as immediate.

Understanding the human context behind these errors is essential to addressing the problem. Instead of blaming people for their "carelessness," it's critical that cybersecurity strategies are more accessible, clear, and empathetic. Systems should be designed to be intuitive, passwords could be replaced by more secure and less complex methods (such as biometrics), and cybersecurity trainings should focus on connecting with users' real experiences and concerns.

1.3. A more human look at cybersecurity

Addressing the **human factor in cybersecurity** does not only mean pointing out the mistakes that people make, but also delving into the reasons behind them and looking for practical solutions that minimize them.

Why does someone reuse a password or ignore a software update? Why do we fall for phishing emails that seem too obvious to the naked eye? Understanding the "why" of these actions implies recognizing that behind each mistake there is a context: lack of time, lack of knowledge, excessive confidence, or even fear of dealing with systems that they perceive as complex (Sasse, Brostoff, & Weirich, 2001).

The key to closing these gaps is not only in educating, but in **designing systems that work in favor of people, not against them**. For example, tools that simplify password management, less intrusive and clearer reminders about updates, or user interfaces that guide individuals instead of intimidating them with technical jargon. The complexity of technological systems is often the first obstacle that leads users to look for "shortcuts" that compromise their security (Beautement, Sasse, & Wonham, 2009). **Reducing this complexity** not only makes the technology more accessible, but also decreases risks.

In addition, we must **address cognitive biases through education**. It's essential that people understand how cyberattacks work, not through fear, but through a practical, empathetic perspective. Cybersecurity education should not only focus on "what not to do", but also on why it is important to adopt good practices. For example, if a person understands that reusing passwords makes it easier for an attacker to access all of their accounts, they will be more motivated to change them. **Making visible the personal and tangible impact of digital decisions** can make a big difference in how users perceive and manage their security (Mitnick & Simon, 2011).

On the other hand, **friendlier and more empathetic user experiences** are essential. If technology systems were designed with how people actually interact in mind—and not how they "should" interact—many gaps could be closed before they even existed. A user who receives a suspicious email should have clear and accessible mechanisms in place to report it or verify its authenticity without fear of feeling confused or embarrassed. Similarly, systems that automatically alert about weak passwords or block attempts at insecure behavior can prevent errors before they occur (Herley, 2009).

Finally, we must change the narrative about cybersecurity: **it is not just a technical issue, but a shared responsibility**. System designers, businesses, and end users are all part of an ecosystem where everyone has an important role to play. Instead of blaming users for their

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

mistakes, it is necessary to build a culture of **empathy and understanding**, where technology is seen as an ally that supports and protects, not as a barrier that punishes human errors (Wolff, 2016).

In this context, the **cybersecurity of the future** will not only focus on developing better technologies, but on building a bridge between technical capabilities and human needs. Because protecting ourselves in the digital world is not only a technical challenge: it is, above all, a matter of humanity.

Social Engineering: The Exploitation of the Human Factor

Social engineering is one of the most effective and widely used techniques by cyberattackers to exploit human vulnerabilities in digital contexts. In essence, this technique is based on psychological manipulation to influence people's decisions or behaviors, leading them to perform actions that compromise the security of systems. Rather than focusing on technological vulnerabilities, attackers employing social engineering target the "weakest link": the human being (Mitnick & Simon, 2011).

Social engineering exploits human emotions such as trust, fear, curiosity, or urgency to persuade people to perform harmful activities, such as revealing credentials, downloading infected files, or transferring funds to fraudulent accounts. This is achieved through tactics that appeal to basic psychology, such as pretending to be a reliable authority, generating crisis scenarios that demand an immediate response, or taking advantage of the victims' lack of technical knowledge (Cialdini, 2001).

A widely known example is **phishing**, a type of attack that involves sending emails or messages designed to appear legitimate, with the aim of tricking users into providing sensitive information. This method poses a significant threat globally and is responsible for economic losses amounting to billions of dollars each year. According to the *Verizon Data Breach Investigations Report* (2022), approximately 36% of cybersecurity incidents involve some form of phishing, highlighting the prevalence and effectiveness of this tactic.

One of the main factors facilitating the effectiveness of social engineering is the **lack of digital security training**. Many people do not recognize the signs of an attack and are therefore more likely to fall into these traps. In addition, attackers use advanced persuasion techniques, such as "reciprocity" or "commitment and consistency," which are key psychological principles that increase the likelihood that victims will act in accordance with the attacker's wishes (Cialdini, 2001).

Another important factor is users' **overconfidence** in their ability to detect threats. Many people believe that they will not be victims of an attack, which makes them let their guard down. According to studies, this overconfidence is a recurring factor that attackers exploit (Sasse, Brostoff, & Weirich, 2001). In addition, attackers often create highly convincing and urgent scenarios, such as emails pretending to be from banking or technical support institutions, asking for the immediate update of passwords or the confirmation of suspicious transactions (Herley, 2009).

The consequences of social engineering-based attacks are devastating. In the business environment, a single click on a malicious link can trigger a ransomware attack that paralyzes the operations of an entire organization, with economic losses that are often irreparable (Kaspersky, 2022). On a personal level, victims may experience identity theft, unauthorized access to their bank accounts, or loss of sensitive information.

Moreover, the psychological impact of these attacks should not be underestimated. People who fall for these deceptions often experience feelings of shame, guilt, and helplessness, which can affect their confidence in using digital tools in the future (Wolff, 2016).

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

To mitigate the impact of social engineering, it's critical to take a preventative approach that combines technology and education. First, organizations should implement advanced security tools, such as email filters that detect phishing attempts and multi-factor authentication systems. However, these technical measures are insufficient without **adequate training of users**.

Training programs should include simulations of real attacks, so that employees and users learn to identify red flags and react appropriately. Likewise, fostering a culture of cybersecurity in organizations, where employees feel comfortable reporting suspicious incidents without fear of retaliation, is key to building an effective first line of defense (Beautement, Sasse, & Wonham, 2009).

Cybersecurity training and awareness programs have established themselves as an essential strategy to reduce human errors, responsible for a large proportion of digital security incidents. Beyond being a simple educational tool, these initiatives seek to change habits and attitudes in the face of digital threats, empowering people to make safer decisions. However, the effectiveness of these programs is not automatic or universal, as it depends on factors such as the quality of the content design, the periodicity of the training, and the capacity of the scenarios proposed to reflect real and relevant situations for users (Bada, Sasse, & Nurse, 2019).

1.4. Key factors for successful training programs

A. **Content design**: The quality of the content is critical. Effective programs not only present technical information, but also appeal to users' emotions and experiences. For example, explaining how a seemingly innocuous action, such as clicking on a link, can trigger a massive ransomware attack, can lead to a deeper understanding of the impact of threats. In addition, language should be accessible and avoid technical jargon that may alienate participants (Bada et al., 2019).

B. **Practical simulations**: Incorporating simulations of real attacks, such as phishing exercises, has proven to be a highly effective practice. These simulations allow users to experience in a controlled environment how they might be affected by an attack, increasing their perception of risk and improving their ability to identify and prevent similar threats in the future. According to a study by Canham et al. (2020), employees who participated in regular simulations showed a significant reduction in malicious link clicks compared to those who only received theoretical training.

C. **Periodicity and continuity**: Training cannot be a single event. Cybersecurity knowledge tends to deteriorate over time if it is not continuously strengthened. Programs that offer frequent reminders, short modules, and updates on new threats manage to keep participants engaged and consolidate long-term learning (Bada et al., 2019).

D. **Customization of scenarios**: The scenarios proposed in the programs must reflect specific and relevant contexts for users. For example, an employee of a financial organization should be trained on how to identify fraud attempts related to wire transfers, while a professional in the education sector may require training on protecting sensitive student data. This personalization increases the perception of usefulness of programs and encourages greater participation (Kaspersky, 2022).

While training and awareness programs have great potential, they are not without their challenges. One of the biggest hurdles is the phenomenon known as "security fatigue," which occurs when users feel overwhelmed by the amount of information and warnings they receive, which can lead them to ignore security best practices. According to Beautement, Sasse, and Wonham (2009), to overcome this problem, it is crucial to integrate cybersecurity into users' daily routines, making secure practices intuitive and not an additional burden.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

In addition, the effectiveness of programs can be compromised if they do not have the active support of senior management in organizations. When leaders promote a culture of safety and actively participate in training initiatives, employees tend to take them more seriously and adhere to best practices with greater commitment (Verizon, 2022).

Cybersecurity training and awareness programs are an indispensable tool to address the human factor in digital security. However, its effectiveness depends on careful design that includes practical simulations, relevant content and a continuous implementation strategy. Personalization of programs and institutional support are key elements to maximize their impact. In a digital landscape where threats are constantly evolving, investing in user training not only protects organizations, but also empowers people as the first line of defense against cyberattacks.

4. Emotions, confidence and decision-making

In a constantly evolving digital environment, where threats are becoming increasingly sophisticated, the emotional dimension of the human being plays a crucial role in cybersecurity. Although this field has historically been approached from a technical perspective, recent research highlights that emotions significantly influence how people perceive and react to digital risks (Sasse, Brostoff, & Weirich, 2020).

Emotions are a central component in the decision-making process. In the context of cybersecurity, situations of stress, urgency, or even fear can lead users to act impulsively, ignoring established protocols, or overlooking warning signs. For example, when faced with an email that pretends to be from a superior requesting urgent access to a system, the fear of work repercussions or the urgency to comply with the request can lead the employee to ignore clear indicators of a phishing attempt (Canham et al., 2020).

On the other hand, emotions such as confidence also have a significant impact. Over-reliance on technological systems, such as automatic security applications, can lead to a false sense of invulnerability. Users, fully relying on these tools, might neglect other basic measures, such as regularly updating passwords or manually verifying suspicious communications (Sasse et al., 2020).

Stress and urgency are emotions frequently exploited by cybercriminals. These factors are often present in social engineering techniques, where attackers design scenarios to elicit quick, thoughtless responses. For example, a message stating that "your account will be blocked within 24 hours if you do not verify your identity" is designed to trigger an emotional panicked response that leads the user to act impulsively (Verizon, 2022).

A study by Woods et al. (2021) showed that people under stress are 45% more likely to make mistakes related to digital security. This finding underscores the importance of educating users not only in technical skills, but also in emotional regulation techniques that allow them to manage these situations effectively.

Trust is not only directed towards technological systems, but also towards other people. In the workplace, for example, employees tend to trust colleagues or superiors, which can be used by attackers to facilitate deception. *Business Email Compromise* (BEC) fraud is a clear example of this: attackers impersonate a high-ranking executive to request money transfers or confidential information, taking advantage of the existing relationship of trust (FBI, 2022).

4.1. Strategies to address the emotional impact on cybersecurity

I. **Emotional awareness**: Cybersecurity training campaigns should include components that sensitize users about how their emotions can influence their behavior in the face of digital risks. This includes identifying signs of stress, urgency, or overconfidence and how to manage these emotions consciously.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

II. **User-friendly interface design**: User interfaces should be designed to reduce stress at critical moments. This includes clear, non-alarmist messaging, simplified decision-making processes, and visual cues to guide users in potentially risky situations (Beautement, Sasse, & Wonham, 2009).

III. **Simulations and contextualized training**: Including simulations of real emotional scenarios in training programs can prepare users to handle high-stress or urgent situations. These simulations help desensitize users to common attacker tactics and develop more thoughtful responses (Canham et al., 2020).

The impact of emotions on cybersecurity is a critical area that needs further attention in both research and practice. By recognizing and addressing emotions such as stress, urgency, and trust, organizations can design more effective strategies that not only focus on technological tools, but also on strengthening the emotional resilience of their users. Ultimately, cybersecurity is as much a technical as it is a human issue, and only by integrating these two dimensions can we move towards safer digital environments.

4.2. Organizational culture: safety as a shared responsibility

One of the most necessary transformations in cybersecurity is the creation of an organizational culture that promotes security as a shared responsibility among all members of an organization. This implies that security should not fall exclusively on the IT department, but that each employee, regardless of their role, understands their role in preventing incidents.

Fostering this culture requires ongoing education, led by interactive training programs tailored to the needs of each team. Studies have shown that regular trainings, combined with realistic simulations such as phishing exercises, can significantly improve employees' awareness of cyber risks and how to mitigate them (Bada et al., 2019).

In addition, open communication is essential. Employees should feel comfortable reporting potential bugs or threats without fear of retaliation, which fosters a consistent learning environment. Leadership also plays a critical role, as leaders who model safe behaviors and encourage active participation can strengthen this organizational culture (Hagen, Albrechtsen, & Hovden, 2008).

Integrating the human factor into cybersecurity models is not limited to treating users as weak points. On the contrary, their ability to be critical allies in the fight against digital threats must be recognized. From designing intuitive interfaces to implementing accessible technologies such as multi-factor authentication and fostering a strong organizational culture, combining technical, educational, and psychological measures can transform the cybersecurity landscape. This comprehensive approach not only strengthens protection, but also empowers people to be active participants in creating a safer digital environment.

Ideal model of the human factor in cybersecurity

Talking about an ideal model that integrates the human factor in cybersecurity implies understanding that users are not simply a "weak link", but a key piece with the potential to significantly strengthen digital security. This model should not only focus on technical tools and protocols, but also address the human dimensions: psychology, education, and cultural values that influence how people interact with systems. Designing strategies that recognize and value human strengths, while minimizing their vulnerabilities, is essential to moving toward safer digital environments.

An accessible and intuitive design can make the difference between a barrier that generates frustration and a tool that effectively protects. Cybersecurity systems must adapt to the capabilities and limitations of users, helping them to make safe decisions in a simple way. For example, the implementation of multi-factor authentication (MFA) has shown great effectiveness

in preventing unauthorized access, but its success depends on how easy it is for users to incorporate it into their daily routines (Sasse et al., 2020).

In addition, systems must provide clear feedback in real-time, so that people understand how their actions impact the security of the system. This approach not only reduces errors, but also fosters a more positive relationship with security tools, eliminating the perception that they are intrusive or unnecessary.

Educating does not simply mean filling users with information; it's about empowering them. Cybersecurity training programs should go beyond data transmission and focus on creating secure habits, adapting to the specific needs of each person or team.

Practical simulations, such as phishing exercises, have proven to be a powerful tool for teaching users how to identify threats in a controlled environment (Bada et al., 2019). These activities, combined with educational campaigns that reinforce learning over time, are much more effective than one-off sessions. The key is to teach users not from fear, but from confidence in their ability to protect themselves and the systems they use.

For cybersecurity to be a reality, it must be perceived as a priority by all levels of an organization, not just technical teams. This requires organizations to foster a culture where safety is a shared value, integrating it into daily operations and strategic decision-making.

Leaders play a crucial role in setting an example and actively supporting safety initiatives, but also in listening to and addressing employee concerns. An open culture, where mistakes or risks can be communicated without fear of reprisal, reinforces trust and collaboration (Wright et al., 2017). This approach not only improves safety, but also strengthens employees' sense of belonging and engagement.

Human behavior in cybersecurity is deeply influenced by cognitive and emotional biases that can put even the most advanced systems at risk. For example, normality bias, which leads people to believe that an attack "won't happen to them," can be countered by regularly exposing them to realistic scenarios that illustrate potential risks (Kahneman, 2011).

Similarly, stressful or urgent situations often generate impulsive decisions that compromise safety. Designing systems that reduce pressure on critical tasks, along with educational modules that explain how emotions affect decision-making, can help users respond more thoughtfully to threats.

Technology should be designed to complement and strengthen human performance, not replace it. Tools such as artificial intelligence (AI) and automated detection systems can ease the burden on users, managing repetitive or complex tasks efficiently.

However, for these tools to be effective, they must be transparent and understandable. Users need to trust these technologies, which is achieved by providing clear explanations about their operation and benefits. According to Chesney (2021), when people understand how tools make decisions, the adoption and responsible use of these tools increases significantly.

Achieving an ideal model of the human factor in cybersecurity requires the collaboration of experts from various disciplines. Psychology can provide insights into human behavior and cognitive biases, while education helps design effective training strategies, and technology offers innovative solutions to address emerging threats (Beautement et al., 2009).

In addition, this model must be dynamic, able to adapt to transformations in the cybersecurity landscape. Threats are constantly evolving, and strategies to deal with them must evolve as well. Regularly evaluating and adjusting practices is essential to ensure their long-term effectiveness.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

An ideal model that integrates the human factor into cybersecurity is not a utopia, but an urgent need in an increasingly interconnected world. Designing accessible tools, educating users, fostering a culture of safety, and leveraging human strengths are key steps in transforming the human factor from a weakness into a strategic asset. In the end, cybersecurity is not just about protecting systems, but about protecting people and the values that these systems represent.

Conclusions

Cybersecurity, a discipline historically focused on technical aspects, has evolved into a more holistic understanding that includes the complexities of human behavior, cognitive biases, and emotions. This broader approach recognizes that technological advances, alone, are not enough to mitigate cyber risks. Instead, it is critical to address the role of the human factor, which continues to be one of the biggest challenges in digital protection.

One of the most revealing aspects of this analysis is how cognitive biases affect safety-related decisions. Biases such as overconfidence, normality bias, and security fatigue reveal that users, often unconsciously, make decisions that compromise the integrity of systems (Kahneman, 2011; Sasse et al., 2020). For example, while most people recognize the importance of strong passwords, many continue to reuse them or choose easy-to-remember combinations for the convenience it represents. This behavior, while seemingly harmless, opens the door to vulnerabilities that attackers successfully exploit.

Likewise, emotions have a significant impact on cybersecurity. The stress and urgency generated by phishing threats or fraudulent messages lead users to act impulsively, ignoring security protocols (Sasse et al., 2020). This finding underscores the need to design systems that are not only technically robust, but also capable of minimizing rash decisions that arise under emotional pressure.

On the other hand, trust, an essential element in any social or technological interaction, can backfire when it translates into a sense of invulnerability. Users who fully trust their colleagues, technological systems, or even their own knowledge, often underestimate the risks and end up compromising the security of the organization (Chesney, 2021). This dynamic highlights the importance of fostering ongoing risk awareness, even among the most experienced users.

Training and awareness programs have proven to be effective tools for reducing human error in cybersecurity, but their success depends largely on how they are designed and implemented. Trainings that include practical simulations, such as phishing exercises, and that are tailored to the specific needs of users, tend to generate better results (Bada et al., 2019). However, for these programs to be truly effective, they must go beyond the transmission of technical information and address the psychological and emotional factors that influence people's behavior.

At the organizational level, cultural change is critical. Cybersecurity cannot be seen solely as a responsibility of the IT department, but as a collective effort involving all levels of the organization. Fostering a culture where security is part of daily routines and where employees feel empowered to report potential threats without fear of retaliation is key to strengthening the protection of systems (Wright et al., 2017).

In addition, the design of security tools and systems should focus on the user experience. Intuitive interfaces, streamlined processes, and clear feedback can significantly reduce human error. For example, the implementation of multi-factor authentication, although initially perceived as a barrier, has become a crucial measure to protect accounts and reduce the risks associated with weak passwords (Sasse et al., 2020).

From a broader perspective, addressing the human factor in cybersecurity requires an interdisciplinary approach that combines technology, psychology, and education. This includes not only identifying and correcting mistakes, but also understanding the motivations and barriers

that lead people to act unsafely. By integrating this knowledge into security strategies, we can develop solutions that are not only technically effective, but also humane and sustainable in the long term.

Finally, it is important to note that cybersecurity is an ever-evolving challenge. Attackers will continue to look for new ways to exploit human vulnerabilities, making it imperative for organizations to take a proactive and adaptive posture. Investment in technology must be accompanied by an investment in people, not only as users of systems, but as partners in building a safer digital environment. Ultimately, digital security isn't just about protecting data or systems, it's about protecting the people and organizations that depend on them.

Bibliographic references

[1] Beautement, A., Sasse, M. A., & Wonham, M. (2009). The compliance budget: Managing security behaviour in organisations. Proceedings of the 2008 Workshop on New Security Paradigms (pp. 47-58). https://doi.org/10.1145/1595676.1595684

[2] Canham, G., Nurse, J. R. C., & Blythe, J. M. (2020). How do users perceive phishing training? Exploring the impact of various simulation types. Proceedings of the 2020 Workshop on Usable Security (pp. 1-10).

[3] Chesney, D. (2021). The psychological effects of cyber threats and their implications for cyber security strategies. Journal of Cybersecurity, 6(1), 45-58. https://doi.org/10.1093/cybsec/tyaa015

[4] Cialdini, R. B. (2001). Influence: Science and Practice. Allyn & Bacon.

[5] FBI. (2022). Internet Crime Report 2022. Retrieved from https://www.fbi.gov

[6] Hagen, J., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. Information Management & Computer Security, 16(4), 377-397. https://doi.org/10.1108/09685220810908789

[7] Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. Proceedings of the 2009 workshop on New Security Paradigms (pp. 133–144). https://doi.org/10.1145/1719030.1719050

[8] Kahneman, D. (2011). Thinking, Fast and Slow. Farrar, Straus and Giroux.

[9] Kaspersky. (2022). Cybersecurity training for employees: A critical defense mechanism. Retrieved from https://www.kaspersky.com

[10] Kaspersky. (2022). The ransomware threat: Why organizations are targeted. Retrieved from https://www.kaspersky.com

[11] Mitnick, K. D., & Simon, W. L. (2011). The art of deception: Controlling the human element of security. Wiley.

[12] Nielsen, J. (2012). Usability engineering. Elsevier.

[13] René van Bavel, Rodríguez-Priego, N. Vila, J. Briggs, P. (2019) Using protection motivation therory in the designo f nudges to improve online security behaviour. International Journal of Human-compute Studies. 123. pp. 29-39. https://doi.org/10.1016/j.ijhcs.2018.11.003

[14] Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link': A human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122-131. https://doi.org/10.1023/A:1011902718709

[15] Sasse, M. A., Brostoff, S., & Weirich, D. (2020). Transforming the 'weakest link'—A human/computer interaction approach to usable and effective security. Journal of Cybersecurity, 1(1), 79-95. https://doi.org/10.1093/cybsec/tyaa002

[16] Tsohou, A., Karyda, M., Kokolakis, S., (2015). Analazyng the role of the cognitive and cultural biases in the internalization of information security policies: Recomendatios for information security awareness programs. 52. pp. 128-141https://doi.org/10.1089/cyber.2017.0059

[17] Verizon. (2022). 2022 Data Breach Investigations Report. Retrieved from https://www.verizon.com/business/resources

[18] Wolff, J. (2016). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

[19] Woods, D., Blythe, J., & Johnson, C. W. (2021). Stress and cybersecurity: A systematic review of the literature. International Journal of Human-Computer Studies, 152, 102628. https://doi.org/10.1016/j.ijhcs.2021.102628

[20] Wright, J. R., Neuman, C., & Whitty, M. T. (2017). Understanding the role of cognitive and emotional biases in cyber security. Journal of Cyberpsychology, Behavior, and Social Networking, 20(10), 601-606. https://doi.org/10.1089/cyber.2017.0059