Leyah Knox

Human Factor/Behavior in Cybersecurity

As an example, the human element is one of the key components of cybersecurity. This is due to the fact that people make decisions that can both increase and decrease security. Even though a company may have good technology, one employee clicking a phishing link, having a poor password, providing information or disregarding a security procedure could provide a potential attacker with an opportunity. Schaltegger et al. (2025) state that many serious cybersecurity incidents can be traced back to human behavior on either the attacker's or victim's side. The authors also show that cybersecurity behaviors are influenced by uncertainty, risk perception, social context and decision making.

Companies need to focus not only on technological controls but also on training, communication, procedures and work culture. The Human Element in Cybersecurity. The human element in cybersecurity is the manner in which peoples' actions, decisions, habits and errors negatively impact the security of information and computer systems. While technology is essential, it is people that utilize the technology and decide upon its utilization. Because of this, cybersecurity is also a social and behavioral issue. Schaltegger et al. (2025) demonstrate that a singular individual's action in a digital environment can produce large negative consequences. A single malicious email click or suspicious download can result in a larger security incident. The authors also introduce the concept of epistemic uncertainty, which stems from limited knowledge and unpredictable human choices.

For instance, people choose to use different passwords, respond to suspicious emails differently and install updates differently. Schaltegger et al. (2025) identify user behavior as a

main contributor to this uncertainty since users may open malicious attachments, provide passwords, utilize unsecure networks and fail to install necessary updates. This exemplifies why cybersecurity cannot be viewed as exclusively a technical problem. Vulnerabilities Created by Human Behavior Human behavior can result in various forms of vulnerabilities leading to cybersecurity incidents. One common form of vulnerability created by human behavior is phishing. A phishing email and message may appear to originate from a trustworthy person, organization, and service. Phishing messages typically create a sense of urgency in employees and prompt employees to click a link, attachment, and account information. The assigned article describes phishing as a persistent threat and describes an employees wrong click on a malicious email attachment as a typical explanation for why attacks occur Schaltegger et al., 2025.

Another example of vulnerabilities created by human behavior is weak and reused passwords. Employees frequently choose passwords that are easy to remember, utilize the same password for numerous accounts or disregard warnings regarding the need to change passwords following a security alert. Schaltegger et al. (2025) provide an illustration of how security policies can sometimes result in unintended outcomes. The authors illustrate that enforcing password complexity can improve password strength but can also encourage employees to reuse passwords or write passwords down should the complexity requirements become burdensome. This serves as an illustration of why organizations need to consider human behavior when establishing security policies. Insider threats or Social Engineering insider threats represent another way human behavior creates vulnerabilities. An insider threat can consist of an individual intentionally misusing authorized access and accidentally exposing confidential information. Employees require authorized access to systems to perform their job duties. Even though organizations must strike a balance between usability and security. Limiting access based

upon job duty assignments and monitoring for unusual activity or establishing formal reporting procedures can minimize harm stemming from intentional, misuse, and inadvertent exposure. The authors similarly identify employee behavior, security policies, and organizational governance as significant factors contributing to managing cybersecurity risk. Schaltegger et al. (2025). Although employees do not make cybersecurity decisions in isolation, psychological factors such as fear, curiosity, trust, stress, and urgency can affect employee behavior. Schaltegger et al. (2025) indicate that risk perception can be affected by employees feelings and immediate reactions to security warnings rather than solely by employees assessments of likelihood and severity. This is significant because employees may react differently to identical security warnings depending upon how serious and convenient the situation appears to be for them.

Work culture also affects employee cybersecurity behavior. The authors state that employee cybersecurity behaviors exist within social contexts such as workplaces and that supervisory personnel and security culture can affect employee behavior. If employees believe that security regulations are merely hindrances slowing down their productivity, they may be less inclined to adhere to them. Conversely, an organization that promotes employees asking questions or reporting suspicious activities can foster employee cybersecurity behaviors as routine practices. Methods for Minimizing Human Related Cybersecurity Risks Organizations can minimize human-related cybersecurity risks through frequent training and clear policies and strong communication and technical controls. Training should employ realistic examples rather than merely presenting employees with lists of rules. The assigned article suggests that simply informing employees about risks does not always alter employee behaviors rather, applying the Mental Models Approach can identify discrepancies between experts understandings and non

experts beliefs, allowing organizations to develop more targeted risk communications Schaltegger et al., 2025. Policies should also be clear and realistic. Organizations can utilize access control,multifactor authentication,password managers,email filters, and monitoring technologies to establish additional layers of protection.

However, organizations should consider how employees are likely to react to these protective technologies. Schaltegger et al. (2025) indicate that employees may react unexpectedly to protective technologies, therefore policies should be developed taking into account actual employee behaviors. The objective should not be to assume employees will never commit errors, rather the objective should be to minimize the frequency and severity of those errors. Communication represents another means for minimizing risk. Employees should understand who they should contact if they suspect wrongdoing and feel comfortable reporting incidents. The authors suggest that cybersecurity professionals struggle with communicating complex risks to diverse audiences, additionally, security recommendations do not consistently translate into secure behaviors Schaltegger et al., 2025, therefore organizations should communicate security information in a manner that employees can comprehend or apply to their daily activities.

Conclusion The human element represents an integral component of cybersecurity because technology alone cannot prevent all incidents. Employee behaviors can generate vulnerabilities through phishing and weak passwords and social engineering and insider threats and negligent workplace practices. Employee responses to security situations can be influenced by psychological or social factors whereas organizational culture can either encourage and discourage secure employee behaviors. The assigned article clearly illustrates that understanding employee behaviors and risk perceptions can enable organizations to develop more effective

security technologies,policies,and communications. Cybersecurity should combine technical safeguards with an understanding of how individuals actually think and make decisions and react to risks.

Citations

Schaltegger, T., Ambuehl, B., Bosshart, N., Bearth, A., & Ebert, N. (2025). Human behavior in cybersecurity: an opportunity for risk research. *Journal of Risk Research*, *28*(8), 843–854. https:andanddoi.organd10.1080and13669877.2025.2539109