

# How can Design Thinking benefit Cybersecurity?: Insights from Don Norman's The Design of Everyday Things

Mrudula Arunkumar <sup>1</sup>, Christian Schunck <sup>1</sup>, Salma Ben Mamia<sup>1</sup>, Heiko Roßnagel <sup>1</sup>

**Abstract:** Human error and insufficient security awareness remain the largest cyber-risk factors for organizations. Despite the prevalence of security training, employees often fail to translate knowledge into secure behavior leading to a gap between security awareness and secure behaviour. Hence, the integration of human factors beyond awareness in cybersecurity is crucial wherein the focus lies on steering the actions executed by people rather than the technical protection offered by the security systems. Donald A. Norman's *The Design of Everyday Things* is one of the pioneering books that introduces how intended actions can be achieved through a user-centric product design. Consequently, it provides a lens to rethink the various security policy designs that are developed to enforce cybersecurity. This short paper therefore proposes a new framework involving design thinking principles to help design better security policies with a human factor focus.

**Keywords:** Human Factors, Design thinking, Cybersecurity, Human Behaviour, Security Policy

## 1 Introduction

The increasing prevalence of cyberattacks necessitates improved cybersecurity measures, and most companies of late have focussed on strengthening the human defense against cyber attack [ZR19] through security awareness training. However this still does not translate to employees behaving securely due to the persistent gap that exists between having awareness and behavioural actions. Therefore, there needs to be additional methods to capitalize on the human factors beyond awareness to promote secure behaviour in the work environment. Having in depth knowledge on the general

---

<sup>1</sup> Fraunhofer IAO, Fraunhofer Institute for Industrial Engineering IAO, Team Identity Management, Nobelstraße 12, Stuttgart, 70569, [firstname.lastname@iao.fraunhofer.de](mailto:firstname.lastname@iao.fraunhofer.de),

 <https://orcid.org/0000-0002-6441-9623>

 <https://orcid.org/0000-0002-7917-8180>

 <https://orcid.org/0000-0001-7057-8404>

cognitive factors that influence the behavioural actions and user interaction with technology first paves a way into assessing the key issues that determine the security compliance. From a security perspective, this could entail (re)designing security policies. Making security measures more intuitive and usable, termed as *usable security*, has been a topic of research since early 2000s [PE08, SF05] focussing on the design vulnerabilities that are present especially concerning specific aspects of security like authentication and encryption methods. However, based on a recent literature review [DTO23] it is clear that the research field lacks a concrete and systematic approach to implement better design for security applications. The current approach to address the human factor in security often fails [BSN19] because it focuses solely on knowledge delivery and compliance enforcement, neglecting the empathetic and intuitive understanding of employees' daily workflows. Therefore, applying the concepts and insights from design thinking on cybersecurity policy engineering that deeply affect everyday workflows for employees should provide more tangible outputs .

Donald A. Norman's *The Design of Everyday Things* [No13] is one of the pioneering book on product design from a human factors perspective, making it a valuable resource for creating security policies in cybersecurity. Given that cyberattacks stem from human error and intentional policy violations, it is crucial to optimize solutions that encourage secure behaviors. Norman emphasizes that design must accommodate human tendencies and has infact noted the lack of usability in the cybersecurity field namely the issues of authentication such as password design [No09]. However his insights in *The Design of Everyday Things* can be used as a template to apply design thinking at a much more systemic level to cyber security especially in the context of security policy design to promote secure behavioural actions. Thus, this short paper will overview design thinking principles relevant to empowering the human factor in cybersecurity and provide guidelines to expand their application. An improved security design should promote compliance, thus serving as a useful tool for security officers responsible for policy design and compliance.

## **2 Gaining insights from The Design of Everyday Things**

One of the key insights from the book *The Design of Everyday Things* is that human behaviour cannot be effectively altered through coercion or unrealistic expectations. This highlights the necessity of designing systems that are aligned with human cognition and typical behavioural patterns. This principle is particularly relevant in cybersecurity, where employees often face competing demands for attention, leading to security fatigue and reliance on automatic actions that attackers exploit. In cybersecurity, these "everyday things" refer to the security policies and systems that employees interact with. Therefore, the principle of designing systems based on an understanding of human behaviour—rather than relying on coercion or intensive training to modify human actions—should be pursued to promote positive change towards secure behaviour.

## 2.1 *To err is human* – non-compliant employee or bad security design?

Human error is frequently cited as the cause of many cyberattacks. However, it is often prematurely concluded that the issue ends with human error. A crucial question to consider, as Norman emphasizes, is *why* these human errors occur. To effectively address human error, it is imperative to understand its root causes that can enlighten about the type of the error. This is especially evident in cybersecurity incidents, such as phishing attacks, which are often attributed solely to user negligence. Such assessments halt root-cause analysis at the point of human error.

As Norman describes, while ultimately executing an action, an error can occur either as an *action-slip* or as a *mistake*. In cybersecurity, an action slip occurs when habitual actions override intended ones, such as opening a phishing email attachment or mistakenly sending sensitive data to the wrong recipient due to autofill. Notably, *description similarity slips*, are particularly relevant; like clicking on a phishing link may resemble the routine action of clicking a trusted link. Conversely, a *mistake* involves sharing credentials to attackers due to misjudgement of trustworthiness indicating a false intention of doing the typical action. To address human error in cybersecurity, one must delve into the "why" behind actions to determine whether they stem from automatic tendencies or poor choices. Both types of errors can arise from poorly designed systems.

Users may deliberately violate security policies due to poorly designed systems that hinder compliance. Norman notes that ineffective designs can lead users to bypass security measures to meet their needs, often prioritizing work over policy adherence, resulting in *deliberate violations*. Awareness is not necessarily the issue as employees could intentionally choose to override policies due to work priorities and these *deliberate violations* are often dismissed as recklessness. Security measures that neglect user experience push individuals toward insecure behaviors like password reuse or disabling security features. Consequently, employees may resort to intuitive actions that support their workflows, ignoring security protocols despite being trained on them [KFR18]. Therefore, re-training the employees with a blame-and-train approach will be ineffective when deliberate violations stem from complex security policies.

Norman also warns of hindsight bias that skews perceptions of security non-compliance, leading to the mislabeling of such slips and violations that resulted from overly restrictive policies or routine behaviour patterns as negligence following an incident. This mindset is prevalent in the cybersecurity field, that focusses on retrospective evaluations rather than proactive planning. Organizations should recognize these errors as indicators of design failure rather than personal failings and adjust policies to support secure behavior without imposing unnecessary friction.

## 2.2 **Information overload burdens the user**

The aspect of cognitive load is a crucial factor that is especially relevant in the realm of

cybersecurity given how fluctuating this can be in the day-to-day work environment. Norman argues that high cognitive load can significantly contribute to errors, leading to security fatigue. This fatigue restricts employees' ability to act securely, as high cognitive load creates a narrow focus where individuals rely on automatic actions that may diverge from intended security policies [No22, Pa16]. Organizations often respond with intensive training that increases the burden through a blame-and-punish approach, telling employees to "be more careful," which fails to scale and does not prevent non-compliant behavior. Another prevalent design flaw in cybersecurity is the overuse of security warnings. While Norman emphasizes the importance of affordances and signifiers in guiding user behavior, excessive warning messages can overwhelm employees. Constant system warnings and policy reminders may lead to a "click-through" habit, where individuals disregard essential security steps, facilitating non-compliant behavior. Additionally, constant exposure to warnings can desensitize users, leading to risky behaviors that could have been prevented if warnings were applied more judiciously. Consequently, users may perceive warnings as excessive or unnecessary, undermining their intended role as affordances or signifiers for secure actions.

### 3 Applying Design Thinking in Cybersecurity

The above-mentioned insights from *The Design of Everyday Things*, can be directly applied within the cybersecurity context especially in the domain of exploring the human error and designing security policies that enable intuitive secure actions.

#### 3.1 Error-tolerant systems

First and foremost, it is important to acknowledge that human error is inevitable and that many errors – slips or mistakes can be prevented through design. Adaptive security policies should guide users toward recovery rather than penalizing failure, an approach Norman describes as "designing for error." By introducing restrictions or limitations in a system already through its design, what Norman refers to as *constraints*, it can help guide users towards the intended secure action. Errors can be prevented by halting action at early stages of interaction with the policy or a security system, allowing for reflection and correction. Effective security policies embed constraints that subtly steer users from unsafe behaviour. Norman discusses the significance of natural mappings in error prevention, suggesting that security design should provide intuitive corrections that align with natural workflows and integrate seamlessly with existing behavioural actions. To address specific types of errors, such as action slips, design adaptations can force a change in routine procedures when encountering malicious threats, reducing the likelihood of habitual responses. Rather than assuming users can avoid errors through training alone, cybersecurity should prioritize better feedback, intuitive design, and safeguards that minimize the impact of human fallibility. Cognitive load management is also crucial; security policies and protocols should reduce mental strain, ensuring

compliance. Intuitive interfaces and minimal decision fatigue enhance security adherence without imposing excessive cognitive burdens. This principle applies to warning announcements. A well-designed warning signifier (e.g., an icon or color) can help users quickly grasp the importance of the warning and the necessary actions. Norman aptly states that, "Designers must strive to find a balance between providing necessary warnings and overwhelming users with unnecessary information," to prevent warning desensitization and negligence. By leveraging affordances, reducing cognitive load, and embedding security into workflows, organizations can create policies that are both effective and user-friendly.

### 3.2 Enhancing security culture

Another critical factor in fostering secure and compliant behavior is the environmental influences that shape motivation and emotional engagement with intended secure actions. Norman posits that design should encompass not only functionality and usability but also emotional responses and experiences. Security training and policies must be crafted to resonate with emotional intelligence, making security personally meaningful. This approach enhances satisfaction, loyalty, and overall user experience. By emphasizing positive reinforcement over punitive measures, organizations can cultivate intrinsic motivation for secure behavior [VD15]. Positive reinforcement encourages the repetition of desirable actions rather than focusing on mistakes through blame-based approaches. Feedback loops can support these positive reinforcements, helping individuals understand correct actions and increasing motivation. A robust security culture should be established as a collective norm, where secure behaviour is perceived as an inherent organizational value rather than an externally imposed obligation. This can be achieved by empowering users to take responsibility for their interactions with security systems through clear and transparent policies. Providing visibility into security operations, particularly regarding the design process, is essential so that the people feel personally involved and thus, responsible. Norman's emphasis on emotional engagement in learning reinforces the importance of narratives, scenarios, and experiential learning in embedding security within one's own identity.

## 4 Guidelines to implement Human-Centered Security Policies

Implementing human-centred security policies thus requires a structured approach that aligns with organizational workflows, minimizes friction, and fosters a culture of security. The following steps provide a pragmatic guide to designing and deploying security policies that align with Norman's principles and human behavioral tendencies:

**Conducting User Research:** Understanding user behavior is crucial for designing effective security policies. Organizations should conduct stakeholder analysis, surveys, and user experience testing to identify common security pain points, habitual

workarounds, in security protocols. Observing users in real-world work environments can provide insights into natural behavior patterns that should inform policy design. **Prototyping and Testing Policies:** Security policies should be treated as dynamic prototypes rather than rigid mandates. By developing low-friction security solutions and testing them with small user groups, organizations can evaluate user experience, compliance rates, and unintended consequences before full-scale implementation. Iterative testing ensures that security policies evolve to meet both security and user experience needs. **Training Through Experiential Learning:** Traditional security training is often ineffective because it lacks engagement and real-world relevance. Security policies should be reinforced through hands-on experiential learning, simulations, and scenario-based training. Employees should experience simulated security threats in a controlled environment to better internalize secure practices. **Establishing Feedback Loops:** Security policies should be continuously refined based on real-world application. Organizations should create feedback mechanisms where employees can report security challenges, inefficiencies, or workarounds without fear of reprisal. Regular user feedback sessions help identify gaps and ensure that security measures remain practical and effective. **Measuring and Adjusting Policies:** Key performance indicators (KPIs) should be used to evaluate the effectiveness of security policies. Metrics such as policy adherence rates, frequency of security incidents, and user-reported friction points should be analyzed regularly. Security policies should remain flexible, adapting to emerging threats, technological advancements, and evolving user behavior.

## 5 Discussion

Integrating design thinking and user-centric principles offers a fresh perspective for enhancing cybersecurity. This paper primarily emphasizes on the need for integrating design thinking principles into improving cybersecurity. With Don Norman's book *The Design of Everyday things* emphasizing on the idea on how systems need to be designed for the human and not human redesigning themselves for a system, it provides resources to have a guideline to integrating design thinking principles into cybersecurity. This fosters and builds the idea that security policies should facilitate, rather than hinder, user activities thus naturally encouraging secure behaviour without introducing unnecessary complexity.

### 5.1 Beyond usable security

The approach outlined here extends well beyond traditional studies in *usable security*, which primarily focus on improving user interfaces, authentication mechanisms, and reducing friction in security interactions [DTO23]. While the field of usable security has made significant strides in enhancing the user experience of security systems—by refining authentication methods, aiding developers in usability improvements, and

influencing user security behaviour through design strategies — these efforts often operate within the constraints of existing security paradigms rather than rethinking the fundamental structure of security policies themselves. In contrast, the proposed framework leverages Norman’s cognitive and behavioural design principles to reimagine security policies at a systemic level. Rather than merely improving compliance through better user experiences, this approach integrates human error tolerance, workflow alignment, and intrinsic motivation to create policies that are not just *usable* but *intuitively adoptable* by users. By embedding security measures seamlessly into existing work processes and leveraging natural affordances, this framework moves beyond surface-level usability enhancements and addresses the root causes of policy circumvention, to foster sustainable, long-term security behaviour. This shift from static usability testing to an adaptive, *human-centred security policy design* represents a significant departure from conventional approaches, positioning this framework as a next-generation model for cybersecurity policy design.

## 5.2 The Security vs. User Experience Trade-off: A False Dichotomy

The conventional argument that security and user experience must always be traded off against each other is flawed because it assumes that one is simply reducing as the other increases. However, a security policy that is highly secure in theory but so ill-conceived that users routinely circumvent is not secure at all. Security is not measured by theoretical robustness but by its real-world implementation. A policy that accounts for actual user behaviour, cognitive load, and work processes—thereby ensuring compliance—is objectively more secure than a stricter policy that is routinely ignored, bypassed, or undermined through workarounds. A policy that balances security with human-centred design does not trade security for user experience — it ensures security by making compliance intuitive and natural. This approach recognizes that user experience is not a competing priority but a fundamental enabler of security.

## 6 Conclusion

Expanding the horizons into understanding the various cognitive factors in play during work can throw more light on how to enable employees to behave securely through security policy design. Traditional security policies often fail due to their misalignment with human cognitive behaviour, leading to non-compliance and circumvention. Insights from *The Design of Everyday Things* reveal fundamental principles on what influences behavioural actions. Instead of treating violations as human errors, organizations should view them as signs of design failure and explore root causes in depth, adjusting policies to support secure behavior without unnecessary friction. This paper presents a holistic framework built on the design thinking principles from *The Design of Everyday Things* and provides a roadmap for designing security policies that are intuitive, user-friendly, and effective. By focusing on human-centred design, error tolerance, and behavioural

integration, cybersecurity policies can promote secure behaviour without overwhelming users, thus fostering a secure environment.

## Bibliography

- [BSN19] Bada, M.; Sasse, A. M.; Nurse, J. R. C.: Cyber Security Awareness Campaigns: Why do they fail to change behaviour?, arXiv:1901.02672 [cs], 2019.
- [DTO23] Di Nocera, F.; Tempestini, G.; Orsini, M.: Usable Security: A Systematic Literature Review. In: *Information* Bd. 14, Nr. 12, S. 641, 2023.
- [KFR18] Kurowski, S.; Fähnrich, N.; Roßnagel, H.: On the possible impact of security technology design on policy adherent user behavior-Results from a controlled empirical experiment. In: *SICHERHEIT 2018*, 2018.
- [No22] Nobles, C.: Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. In: *HOLISTICA – Journal of Business and Public Administration* Bd. 13, Nr. 1, S. 49–72, 2022.
- [No09] Norman, D. A.: The Way I See It, When security gets in the way. In: *Interactions* Bd. 16, Nr. 6, S. 60–63, 2009
- [No13] Norman, D. A.: The design of everyday things. Rev. and expanded edition. Cambridge (Mass.) : MIT press, ISBN 978-0-465-05065-9, 2013.
- [PE08] Payne, B. D.; Edwards, W. K.: A Brief Introduction to Usable Security. In: *IEEE Internet Computing* Bd. 12, Nr. 3, S. 13–21, 2008
- [Pa16] Parkin, S.; Krol, K.; Becker, I.; Sasse, M. A.: Applying Cognitive Control Modes to Identify Security Fatigue Hotspots. In: *(Proceedings) Workshop on Security Fatigue, [part of] SOUPS 2016: Twelfth Symposium on Usable Privacy and Security*, 2016.
- [SF05] Sasse, M.A.; Flechais, I.: Why Do We Need It? How Do We Get It? In: Cranor, LF and Garfinkel, S, Security and Usability: Designing secure systems that people can use, S.13-30, 2005.
- [VD15] Vlaev, I.; Dolan, P.: Action Change Theory: A Reinforcement Learning Perspective on Behavior Change. In: *Review of General Psychology* Bd. 19, Nr. 1, S. 69–95, 2015.
- [ZR19] Zimmermann, V.; Renaud, K.: Moving from a ‘human-as-problem’ to a ‘human-as-solution’ cybersecurity mindset. In: *International Journal of Human-Computer Studies* Bd. 131, S. 169–187, 2019