ADGM Academy
Research Centre

أكاديمية ريدان
Rabdan Academy

# BEYOND TECHNOLOGY:

## The Four Dimensions of the Human Firewall for Cyber-Resilient Behaviour Foundations


Authored by:

**Dr. Mathew Nicho**

Associate Professor, Research and Innovation Centre, Rabdan Academy


# Abstract

This is the second report in a three-part series, jointly produced by the Research and Innovation Centre of Rabdan Academy (RA) in association with the ADGM Academy (ADGMA), and with support from UQ Cyber, University of Queensland. The report draws on extensive research and in-depth interviews with 18 senior IT security managers from 12 institutions within the UAE financial sector, including multinational corporations operating in the UAE. Their insights, expertise, and candid perspectives have been invaluable in shaping our understanding of the cyber threats confronting the industry today. It is our hope that the findings presented herein will serve as a catalyst for continued dialogue, collaboration, and action to strengthen cybersecurity resilience across the UAE and global financial sector.

## About the Author

This report was prepared by Dr. Mathew Nicho, Associate Professor at the Research and Innovation Centre, Rabdan Academy, Abu Dhabi, UAE, and Adjunct Associate Professor at the UQ Cyber Research Centre, University of Queensland, Australia. He has also been a member of the CyberSecurity Advisors Network (CyAN) since 2024. His research focuses on socio-technical cybersecurity, ransomware resilience, and AI-enabled intrusion detection and prediction. For queries, insights, or clarification, please contact:

---

## Acknowledgements

We extend our sincere appreciation to the following individuals and organisations for their invaluable support and contributions to this report.

1. **Peter Ware:** Director of Research and Development, ADGM Academy
2. **Rauda Al Dhaheri:** Head of Research and Development, ADGM Academy
3. **Bharat Raigangar:** 1CxO-CSA, CAISO (Maseera Holding) & Board Member (CyberSecurity Advisors Network-CyAN)
4. **Professor Ryan Ko:** Chair and Director of UQ Cyber Security, School of Electrical Engineering and Computer Science, University of Queensland

# Table of Contents

# Executive Summary

Cyberattacks often begin with people rather than technology, making employees, managers, and IT staff both the first and last line of defense. This report, informed by two years of research and expert interviews across the UAE and UK explores how to embed a "security DNA" into users and build a cyber-resilient human firewall. It identifies key issues such as device diversity, an expanded attack surface, and rising concerns about AI, alongside challenges that demand cognitive security and coordinated stakeholder action. By outlining three behavioural enhancers and one inhibitor, the findings offer actionable guidance for reducing intrusions and shaping user-centric cybersecurity strategies.

Users remain a primary source of socio-technical vulnerabilities in cybersecurity, and analysis of sectoral responses highlights four critical human factors. These factors serve as both enhancers and inhibitors, guiding policymakers to design targeted awareness programmes and practical, user-centric IT policies. The three enhancers are cyber hygiene, situational awareness (as both product and process knowledge), and context-based micro training (CBMT), while the key inhibitor is technostress. Together, they shape how effectively organisations can strengthen detection, prevention, and resilience against cyber threats. Optimal levels of the first three factors namely cyber hygiene, product/process knowledge, and CBMT are enablers that collectively strengthen the human firewall and embed a culture of security awareness (security DNA) across the users. In contrast, technostress acts as an inhibitor, undermining users' ability to maintain secure behaviours.

## 1. Cyber Hygiene:

- **Enhancer of Security DNA:** Cyber hygiene strengthens and reinforces an organisation's human-centred security culture.
- **Definition:** Refers to the security practices that users should follow to protect the safety and integrity of personal information on internet-enabled devices.
- **Sector Concern:** Respondents from the financial sector noted a persistent gap in consistent cyber hygiene practices among employees.
- **Key Issue:** The gap stems from users' lack of situational awareness and preparedness when facing potential cyber threats.

## 2. Situational Awareness:

- **Enhancer of Security DNA:** Situational awareness of threats strengthens resilience by combining both the product (state of knowledge) and process (how knowledge is developed).
- **State of Knowledge Includes:**
  - Understanding of computing environments and their risks
  - Awareness of the organisational context
  - Knowledge of probable threats and vulnerabilities
- **Situational Knowledge leads to Situational Awareness:** It is built through continuous training programmes, real-time system feedback, alerts and updates, security culture, and prior incident-handling experience.


## 3. Training Needs:

- **Enhancer of:** CBMT addresses the shortcomings of traditional Security Education, Training, and Awareness (SETA) programmes, which are often compliance-driven and only marginally effective.
- **Effective Training Needs:** Respondents stressed the importance of real-world case examples, interactive role plays, and assessments to build practical, lasting awareness.
- **Knowledge Gaps:** A lack of situational awareness in training leads to two risks:
  - **Incomplete knowledge:** Employees simply don't know certain things (blind spots).
  - **Imperfect knowledge:** Employees think they know but hold misconceptions or false confidence.
- **Consequence:** These gaps increase the likelihood of employees bypassing security policies (e.g., unsafe downloads), leaving vulnerabilities open and potentially leading to serious breaches.

## 4. Technostress

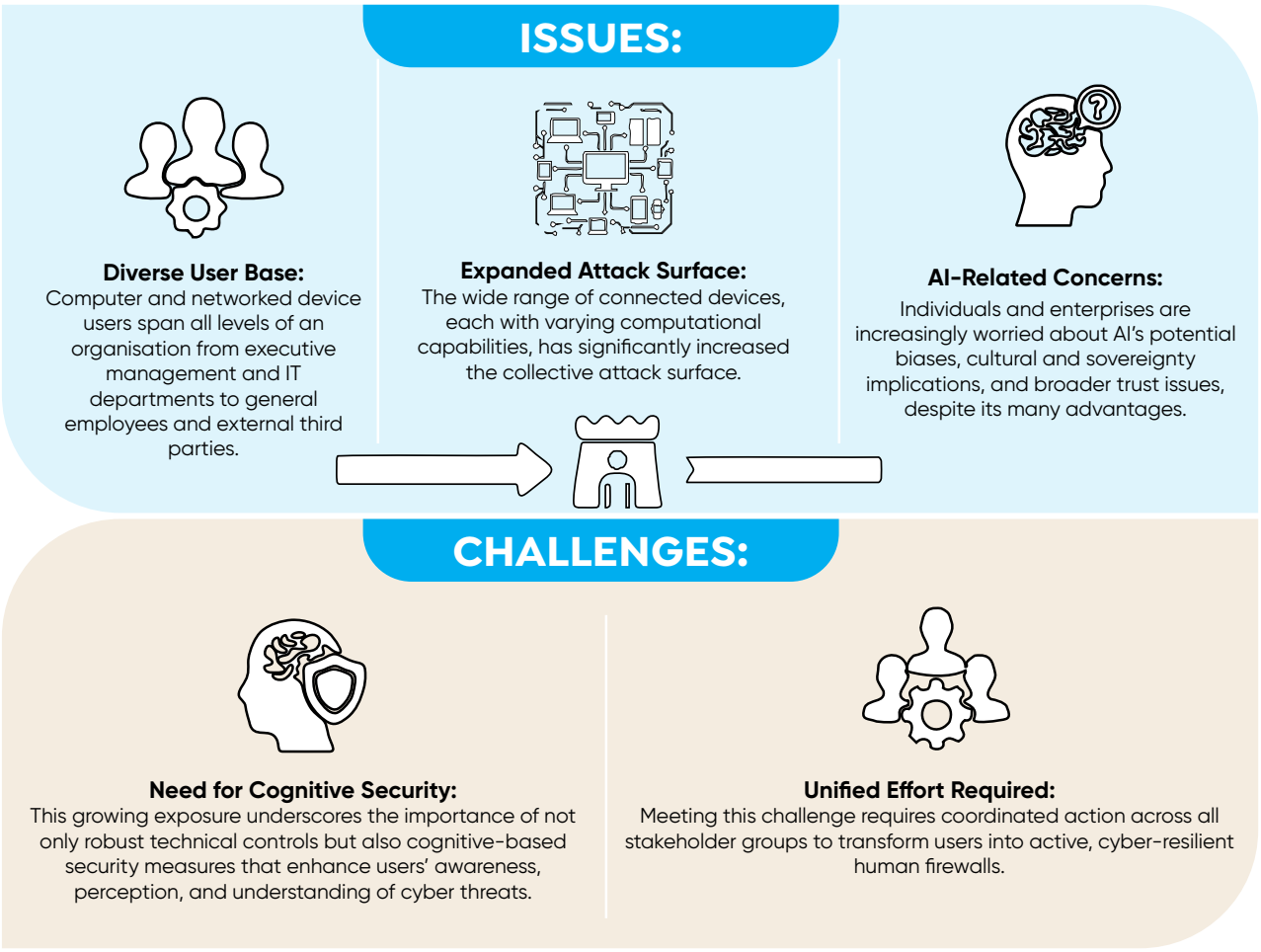
- **Inhibitor of Security DNA:** Technostress undermines efforts to embed secure behaviour and awareness, counteracting the benefits of enhancers like cyber hygiene, situational awareness, and CBMT.
- **High-Pressure Environments:** Critical infrastructure organisations operate in highly technology-intensive settings, often under tight deadlines and constant time pressure.
- **Multiple Device Dependence:** Users frequently juggle several digital devices for both personal and professional tasks, leading to increased cognitive load.
- **Consequence**: Elevated stress levels and divided attention raise the risk of security lapses, making users more vulnerable to errors and oversight.

# Introduction

Cyberattacks rarely begin with technical vulnerabilities; they begin with people including employees, IT personnel, management, and even extended stakeholders with system access. More than technical security layers, an organisation's own users often serve as both the first and last line of defense, the human firewall. Yet vulnerabilities in user behaviour can create critical weak points, potentially leading to data breaches with devastating consequences. In response, senior management and cybersecurity leaders continue to grapple with two questions:

- How can we embed a "security DNA" into every user?
- How can we transform organisational users into an active, cyber-resilient human firewall?

This report addresses the issues and challenge in accessible, actionable terms. It draws on two years of research involving in-depth interviews with senior cybersecurity, risk management, and IT professionals from both regional and multinational financial institutions in the UAE and the UK. The findings have also been independently validated, ensuring the insights are both globally relevant and locally grounded. Issues and challenges:




This report focuses on strengthening the cognitive dimension of cybersecurity to foster cyber-resilient behaviour and reinforce the human firewall. For the purposes of this analysis, the term 'users' refers specifically to individuals within the first three categories: management, IT personnel, and general staff and can extend to other relevant stakeholders as well.

In today's dynamic threat landscape, users are expected to serve as security enhancers, yet even inadvertent lapses or oversights acting as inhibitors can result in serious breaches. Based on professional insights from both regional and multinational respondents in the UAE and UK, this report identifies four key dimensions. In this report we give three enhancers and one inhibitor for answering the two questions. When addressed strategically, these dimensions can:

- Significantly reduce the likelihood of system intrusions and organisational compromise.
- Assist policymakers in shaping more targeted, user-centric cybersecurity strategies and awareness programmes.

# Enhancers and Inhibitors

In the cybersecurity landscape, users continue to be recognised as a primary source of human-induced socio-technical vulnerabilities. A deeper analysis of sectoral responses revealed four key factors that critically influence the human element in organisational cybersecurity. These factors not only provide the foundation for answering the questions posed earlier, but also offer valuable guidance to policymakers by enabling them to:

(1) design actionable and targeted awareness programmes, and
(2) craft practical, user-centric IT policies that enhance the ease and effectiveness of threat detection and prevention across the workforce.

## Enhancers (E) and Inhibitors (I)

1. Cyber Hygiene (E)
2. Situational Awareness (Product and Process Knowledge) (E)
3. Context-Based Micro Training (CBMT) (E)
4. Technostress (I)

Optimal levels of the first three factors namely cyber hygiene, product/process knowledge, and CBMT are **enablers** that collectively strengthen the human firewall and embed a culture of security awareness (security DNA) across the users. In contrast, technostress acts as an **inhibitor**, undermining users' ability to maintain secure behaviours. The following sections explore these four dimensions in detail, offering actionable insights and industry-relevant strategies to address the dual challenge of empowering users while minimising risk. An overview of the relationships among these factors is illustrated in Figure 1.

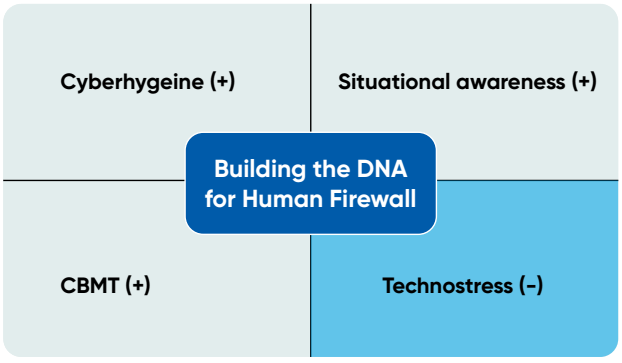



Fig. 1 Factors shaping security DNA and enabling the human firewall

# 1. Cyber hygiene

The presence of cyber hygiene enhance and reinforce the security DNA. (Vishwanath et al., 2020) defined cyber hygiene as the cyber security practices that online consumers should follow to protect the safety and integrity of their personal information on Internet enabled devices from being compromised in a cyberattack through unintentional acts. Several respondents from the financial sector highlighted a significant and ongoing gap in consistent cyber hygiene practices among employees. This concern centres around the users' lack of situational awareness and preparedness when faced with potential cyber threats.

## Specifically, respondents noted that some users:

- Often describe themselves as being completely in the dark regarding the type and nature of cyberattacks (the product; i.e., the state of knowledge);
- Do not know what actions they are expected to take;
- Are uncertain about the correct course of action when confronted with a potentially harmful situation;
- Frequently claim to have no idea how to respond to incidents;
- Are unaware of the major threats to individuals and corporations arising from the abuse of AI tools such as Deepfakes;
- Lack awareness and transparency regarding the use of their personal data; and
- Are often unaware of the recourse available once they provide consent, unknowingly exposing themselves to malicious intent.

The accumulation of cyber threat information builds situational knowledge, which provides the foundation for situational awareness which is the ability to perceive, interpret, and respond to threats in real time. In this regard, practicing cyber hygiene is the first step toward developing both knowledge and awareness. (Fig. 2)

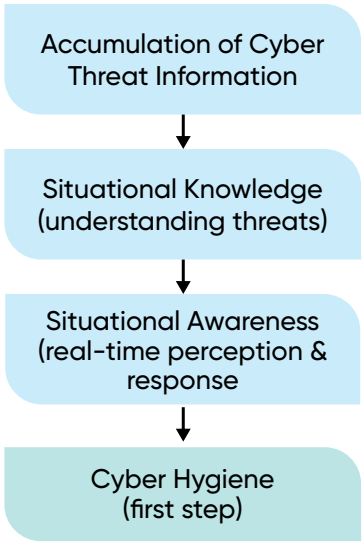



Figure 2. Relationship between Cyber Threat Knowledge, Awareness, and Cyber Hygiene

This disconnect between knowledge as both a product and a process, and the development of that knowledge through interaction and training, creates a critical vulnerability in an organisation's human-centred cybersecurity framework. When hackers exploit employee naivety through social engineering tactics, the absence of clear understanding about what constitutes "secure behaviour" in real-time scenarios often results in unintentional insider threats. So, the critical question becomes:

**What targeted initiative can effectively elevate cyber hygiene among users to the level required for a truly resilient human firewall?**

- The fist dimension introduces the concept,
- The second-dimension outlines what needs to be addressed,
- The third dimension explains how it can be achieved, and
- The final dimension serves as a cautionary note on what to avoid.

# 2. Situational awareness (product and process knowledge)

Situational information security awareness thus considers both the product (i.e. state of knowledge) and process (how that knowledge is created through interaction with the environment) of situation awareness (Jaeger & Eckhardt, 2021).

### The state of knowledge includes the user's understanding of:

- Their computing environment and the associated risk *(for every computing environment, there is an associate risk),*
- The organisational environment which it operates,
- The probable threats and vulnerabilities, and
- The organisational security policies and potential consequences of its overlook.

### The state of knowledge can be created through the continuous interaction with:

- Organisational training programmes
- Real-time feedback from systems
- Alerts or updates
- Organisational culture
- Experience handling incidents

## Situational Awareness and Cyber Hygiene: Enhancing the Human Firewall

1. **Nature of Cyber Threats**
   - Cyber threats are dynamic, innovative, and context-specific, ranging from phishing and ransomware to device deception and AI-generated attacks.
   - Therefore, situational awareness is increasingly recognised as a critical factor in promoting cyber hygiene.

2. **Creating the contextual awareness of the digital environment**

   - Understanding the computing environment and its associated threats, collectively referred to as the product is foundational.
   - This includes situational knowledge derived from real-world interactions between benign and malicious activities involving computing devices and IT processes (the process).

3. **Formation of Expected Behaviours**

   - The interplay between product and process knowledge shapes user behaviours, enabling more informed responses to threats.
   - This dual awareness enhances the development of the human firewall, both in organisational settings and in personal digital spaces.

4. **Impact of Limited Situational Knowledge**

   - A lack of awareness about evolving cyber-attack methods leads to unintentional user errors.
   - Users may not be equipped to recognise or respond to advanced deception techniques, especially in real-time.

As noted by respondents:

- "If there's a genuine deception happening, you cannot expect the users to know everything and detect it."
- "People are not aware of what they're doing with their computer or the emails they receive."

When asked about the nature of situational awareness, respondents emphasised the importance of:

- Contextual training programmes simulating real-world threats.
- Regular awareness campaigns with updates on emerging attack vectors.
- Interactive platforms for users to practice safe behaviours in simulated threat environments.
- User-centric feedback systems that explain mistakes and encourage learning.
- Cross-device awareness strategies addressing both work and personal device use.

When queried further on the major components of situational awareness, respondents cited the concept of:

- Product knowledge and
- Process knowledge

Product knowledge refers to an understanding of various types of cyber threats, past, present, and emerging. Since hackers often customise attack vectors based on an organisation's specific context, the first step for users is to develop situational awareness. This awareness helps users anticipate the types of attack vectors most likely to target them, based on the organisational environment in which they operate.

The organisational environment plays a critical role in shaping situational awareness, which in turn provides insight into the specific types of threats that could impact the organisation (Fig. 3).

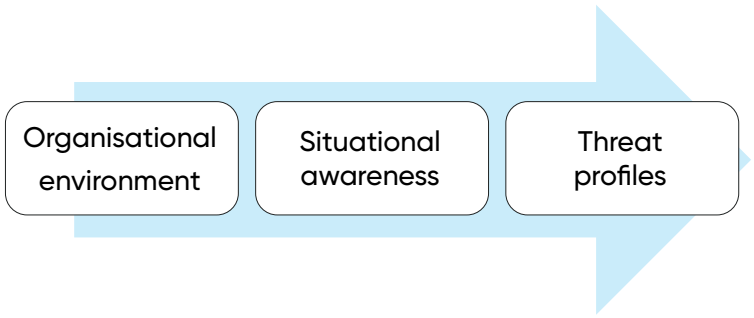



Fig. 3 Product process of situational knowledge awareness

The success of social engineering is cited as a critical factor in facilitating the threats affecting the financial sector. The critical nature of social engineering was highlighted by stating "very high-profile cyber incidents were facilitated almost entirely by social engineering of colleagues." Lack of situational awareness on cyber-attacks is thus a critical factor that leads to unintentional mistakes where the users may not be fully aware of all the techniques employed by the hackers. In this respect "if there's a genuine deception that is happening you cannot expect the users to know everything and detect it." When this happens "people are not aware what they're doing with their computer or with the emails that they get.

**Process knowledge:** The process of how users interact with their organisational and its computing *environment* through training, IT communications, feedback, past experiences lead to the formation of the product, which is their current state of security knowledge and awareness. That knowledge then drives the desired or IT policy complied behaviour, such as:

- Detecting and identifying threat attempts
- Following security protocols
- Reporting anomalies

A recurring theme among respondents was the critical role of situational awareness in shaping users' responses to cyber threats. The absence of situational knowledge awareness was consistently identified as a **primary factor contributing to security breaches.**

- Respondents emphasised that security incidents can be significantly reduced if all stakeholders understand how to behave when confronted with malicious scenarios. One participant noted: *"Everyone (all stakeholders) should be aware of how they're to behave in malicious situations."*
- When users possess the knowledge and awareness to appropriately respond to suspicious online communications whether emails, pop-ups, or login requests—security can be maintained. Conversely, a lack of vigilance or failure to maintain a vigilant mindset creates exploitable vulnerabilities.
- A consistent finding across interviews was the gap in awareness of cyber risks associated with *legitimate-looking attack vectors*. These deceptive threats exploit trust and routine behaviours, often bypassing conventional technical safeguards.
- Furthermore, while compliance with organisational security policies is important, it alone does not ensure the development of a robust information security mindset among employees. Policies must be accompanied by:
  - Contextualised training that reflects real-world threat scenarios.
  - Reinforcement mechanisms that support day-to-day vigilance.
  - A culture that promotes proactive awareness, not just passive compliance.

In summary, enhancing situational awareness at both individual and organisational levels is essential for reducing the success rate of cyberattacks and fostering a resilient security culture. Therefore, organisations should tailor their security policies to be (1) practical (hands on involving multiple senses), (2) relevant (contextual to the organisations, business environment), and (3) easily understandable (irrespective of user levels), while also highlighting their benefits in both professional and personal contexts. Such an approach can support the cultivation of a stronger and more resilient security mindset among employees (Sebescen & Vitak, 2017) leading to cyber situational awareness (Fig. 4)

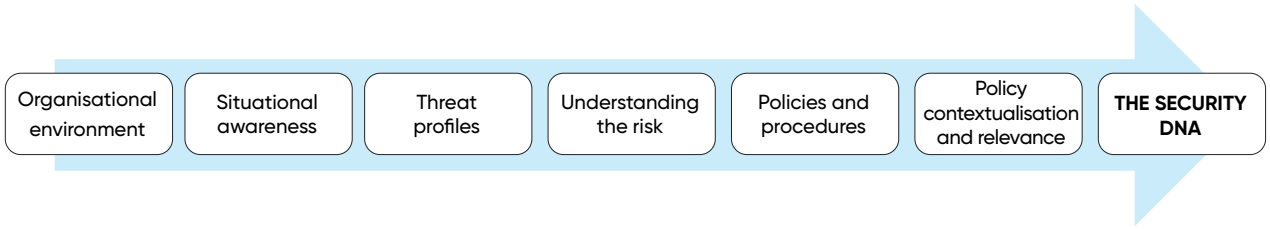



Fig. 4 The product and process knowledge leading to cyber situational awareness

# 3. Context Based Micro Training (CBMT)

Organisations implement Security Education, Training, and Awareness (SETA) programmes primarily to comply with relevant standards and regulations that mandate due diligence and care among users. However, feedback from respondents indicated that current SETA initiatives are only marginally adequate. Participants emphasised the need to continuously enrich the training content with:

- Real-world use case examples,
- Interactive role plays, and
- Assessments.

**A recurring concern was the lack of cyber situational awareness among employees. When employees possess:**

- Imperfect knowledge (knowledge refers to IT policies, situation and desirable actions) or
- Incomplete knowledge, of an IT-related situation, they are more likely to disregard security policies such as downloading content without exercising appropriate caution. As one respondent noted, "every time something happens in your network, you leave a vulnerability that is open," potentially leading to serious consequences.
    - Incomplete knowledge means employees don't know certain things at all (gaps or blind spots).
    - Imperfect knowledge means they think they know, but some of that knowledge is wrong (misconceptions or false confidence).

(Note the difference between imperfect knowledge and incomplete knowledge of a 'product' or 'process' with imperfect knowledge being more dangerous)
Respondents consistently referred to the challenges posed by imperfect and incomplete user knowledge in the context of cybersecurity training. One key issue identified was the ineffectiveness of Security Education, Training, and Awareness (SETA) programmes when delivered through non-interactive or passive formats, such as standard email communications.

- In such cases, employees often fail to comprehend the core message, particularly in relation to recognising and responding to deceptive content (e.g., phishing emails).
- Some users may misinterpret the message entirely, resulting in unintended security breaches.

To address these shortcomings, CBMT has been proposed as a strategic enhancement to existing SETA frameworks.

- Perceive security-related cues,
- Process information and threats, and
- Respond appropriately to cyber incidents,

thereby promoting deeper engagement, better knowledge retention, and more informed decision-making in real-world cyber situations.

The core issue raised by respondents is not merely the delivery format of SETA programmes, but the lack of a systematic understanding of the nature and structure of SETA itself (Hu, Hsu, & Zhou, 2022). This ambiguity makes it difficult to determine which SETA strategies are effective in specific organisational contexts (Alshaikh et al., 2021).

**In this regard, employees may:**

- Fail to understand the message when SETA is delivered in a non-interactive manner, or
- Misinterpret the message, leading to imperfect situational knowledge.

Such misunderstandings can result in what Kaptein and Van Helvoort (2019) describe as a "lack of intentionality," where individuals claim they had no information that could have guided or contradicted their behaviour.

## The Solution?

CBMT has been proposed as a structured method for conducting SETA programmes. The fundamental idea behind CBMT is to provide users with interactive, context-specific training when they encounter situations where that training becomes directly relevant (Kävrestad, Furnell, & Nohlberg, 2024). One practical approach to delivering CBMT is through 15 minutes micro training, which typically includes:

- An active start to engage the participant on a threat,
- A demonstration or hands-on exercise to simulate realistic scenarios,
- Feedback or discussion to reflect on actions taken, and
- A shared plan for next steps to reinforce learned behaviours.

**These micro-training sessions usually last around 15 minutes and can be delivered:**

- Face-to-face,
- Online, or
- Through a blended format, depending on the organisational context and available resources (De Vries & Brall, 2008).

# 4. Technostress

While the active presence and successful implementation of the first three dimensions serve as enablers in cultivating a strong security DNA among users, the presence of technostress within an organisation function as a significant inhibitor, undermining efforts to embed secure behaviour and awareness. Organisations operating in critical infrastructure sectors function within highly technology-intensive environments, often working under constant time pressure due to tight deadlines. In such contexts, users frequently depend on multiple digital devices to manage both personal and professional responsibilities, increasing cognitive load and the potential for security lapses (Fig. 5).


Fig. 5 intersection of multiple devices managing personal and professional responsibilities, increasing vulnerabilities

Simultaneously, attackers exploit advancements in generative AI to create sophisticated, benign-looking attack vectors that are difficult to distinguish from legitimate content. As one respondent observed: *"The root causes of why we see these threats growing all the time and morphing and changing shape is the emergence of the Internet, digital technologies, the sheer rise of digital channels in everyday life, the complexity, and the speed at which people are processing information..., where human factors are perhaps more vulnerable to these ever-changing profiles of crime."*

Technostress is defined as the stress experienced by individuals due to the use of information and communication technologies (ICTs). While ICTs have made many aspects of work more efficient, they have also introduced cognitive challenges that can degrade the quality of decision-making, attention, and situational awareness.

- The term technostress was first introduced by Craig Brod (1984), who described it as a modern disease arising from the inability to cope with ICTs in a healthy way.
- Later research by Ayyagari, Grover, and Purvis (2011) emphasised that technostress is caused by the complexity, pace, and demands associated with technology use in modern workplaces.
- Sellberg and Susi (2014) further noted that prolonged exposure to ICTs can negatively affect the cognitive work environment.

## Impact on Situational Awareness

**Technostress directly impacts users' situational awareness, particularly in security-sensitive environments:**

- Cognitive Overload – Users may become overwhelmed by multiple digital inputs, reducing their ability to detect anomalies or potential threats.
- Imperfect Knowledge of the Situation – As Kaptein and Van Helvoort (2019) observed, users under stress often fail to understand either the situation they are in or the appropriate course of action.
- Reduced Intentionality – When faced with complex or fast-changing information flows, users may act without full awareness or fail to act entirely.
- Increased Vulnerability to Deception – The rise of AI-generated phishing emails makes it increasingly difficult for users to distinguish between genuine and malicious content (Eze & Shamir, 2024).

## The Dual Role of Generative AI

**While generative AI introduces new challenges in the form of realistic, automatically generated phishing attacks, it also holds potential as a defensive tool:**

- Offensive Use: Attackers employ generative AI to mimic legitimate communication, thereby increasing deception (Alabdan, 2020).
  - Threat/Challenge: Any increase in the use of AI by hackers can increase the cognitive load on the users.
- Defensive Use: Organisations are beginning to leverage generative AI to detect and counter phishing attacks, improve content filtering, and assist in user training (Das, 2024).
  - Opportunity: Use of AI in threat detection and its use in CBMT can decrease the cognitive load

**The rapid evolution of technology in workplace environments has introduced a dual challenge:**

- Employees are expected to remain vigilant and compliant while navigating complex digital systems.
- Meanwhile, attackers are innovating at speed, using AI to exploit human cognitive limitations.
- As a result, understanding and mitigating technostress is not only a matter of employee wellbeing but a strategic requirement for enhancing cybersecurity posture in critical infrastructure sectors.

# Conclusion

User-related errors, whether called human error, user vulnerability, or inadvertent policy violations remain a persistent cybersecurity risk, especially as devices like smartphones, IoT tools, and wearables expand the attack surface. While technology can detect and mitigate threats, the human factor is decisive, making cognitive and behavioural resilience essential. This report identifies three enhancers namely cyber hygiene, situational awareness, and context-based micro training and one inhibitor, technostress, as the critical dimensions shaping a strong organisational security DNA.

# References


1. Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet, 12(10), 168.*
2. Alshaikh, M., Maynard, S. B., & Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organisations. *Computers & security, 100, 102090.*
3. Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological antecedents and implications. *MIS quarterly, 831-858.*
4. Brod, C. (1984). Technostress: The human cost of the computer revolution. *(No Title).*
5. Das, R. (2024). *Generative AI: Phishing And Cybersecurity Metrics: CRC Press.*
6. DeVries, E. J. (2005). *Epistemology and Methodology in Case Research: A Comparison between European and American IS Journals* Paper presented at the Thirteenth European Conference on Information Systems Regensburg, Germany.
7. Eze, C. S., & Shamir, L. (2024). Analysis and prevention of AI-based phishing email attacks. *Electronics, 13(10), 1839.*
8. Hu, S., Hsu, C., & Zhou, Z. (2022). Security education, training, and awareness programs: Literature review. *Journal of Computer Information Systems, 62(4), 752-764.*
9. Jaeger, L., & Eckhardt, A. (2021). Eyes wide open: The role of situational *information security awareness for security-related behaviour. Information Systems Journal, 31*(3), 429-472.
10. Kaptein, M., & Van Helvoort, M. (2019). A model of neutralization techniques. *Deviant behavior,* 40(10), 1260-1285.
11. Kävrestad, J., Furnell, S., & Nohlberg, M. (2024). User perception of Context-Based Micro-Training–a method for cybersecurity training. *Information Security Journal: A Global Perspective, 33*(2), 121-137.
12. Sebescen, N., & Vitak, J. (2017). Securing the human: Employee security vulnerability risk in organizational settings. Journal of the Association for Information Science and Technology, 68(9), 2237-2247.
13. Sellberg, C., & Susi, T. (2014). Technostress in the office: a distributed cognition perspective on human–technology interaction. *Cognition, Technology & Work, 16,* 187-201.
14. Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems,* 128, 113160.

# ADGM ACADEMY RESEARCH CENTRE

## Innovating Knowledge, Empowering Change

The **ADGM Academy Research Centre**, part of ADGM Academy, unites academics, financial practitioners, government, and technology experts to drive innovation and enhance the financial landscape in the UAE, MENA region, and beyond. As the financial sector evolves with new technologies, disruptors, and opportunities, independent research is vital to harness these changes for the benefit of businesses, customers, and society. Through collaborative insights with the academic community, the Research Centre delivers the expertise needed to navigate and capitalise on this dynamic transformation.

**ADGM Academy,** the knowledge hub of Abu Dhabi Global Market (ADGM), is shaping the future of banking, finance, digital innovation, and public services in the region. Committed to aligning with the UAE's vision for economic leadership, we deliver cutting-edge experiential programmes that empower both graduates and professionals and drive industry growth. As a trailblazer in financial and digital training, we collaborate with top industry experts, leading professional organizations, and renowned academic institutions to create innovative, certified programmes. Join us on a transformative journey where world-class education meets opportunity, paving the way for a stronger, smarter financial industry.

**ADGM** is a globally recognised international financial centre that brings unique value to the emerging economy of Abu Dhabi and the broader region. Established in 2015, ADGM has significantly enhanced Abu Dhabi's stature as a leading financial centre and business hub, bolstering its role as a key player in the Falcon Economy. It serves as a vital strategic link between the growing economies of the Middle East, Africa, South Asia, and global markets.

Stay up to date with ADGM Academy Research Centre.

adgmacademy.com research@adgm.com

**FOLLOW US**
ON OUR SOCIAL NETWORKS

Level 20, Al Maqam Tower, ADGM Square, Al Maryah Island, PO Box 111999 Abu Dhabi, UAE
الطابـق 20، بـرج المقام، مربعة أبوظبي العالمي، جزيرة الماريـه، ص ب 111999، أبوظبي، الإمارات العربية المتحدة

T +971 2 333 8500 adgmacademy.com

**adgmacademy.com**