Users Are Not Stupid: Six Cybersecurity Pitfalls Overturned

Julie Haney
Usable Cybersecurity Program Lead, National Institute of Standards and Technology, USA

Julie Haney conducts research about the human element of cybersecurity, including the usability and adoption of cybersecurity solutions, work practices of cybersecurity professionals, and people's perceptions of privacy and cybersecurity. She has been an invited speaker at numerous cybersecurity forums spanning industry, government, and academia, and has published peer-reviewed articles in both research and practitioner publications. Prior to joining NIST in 2018, Julie spent over 20 years working in the U.S. Department of Defense as a cybersecurity professional and technical director where she conducted vulnerability assessments, wrote widely used cybersecurity guidance, and advocated for the adoption of cybersecurity mitigations. She has a PhD in Human-Centered Computing from University of Maryland, Baltimore County, an M.S. in Computer Science from University of Maryland, and a B.S. in Computer Science from Loyola University Maryland.

National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899, USA
E-mail: julie.haney@nist.gov

Author version. Article published in Cyber Security: A Peer-Reviewed Journal, Vol. 6, No. 3, 2023, pp. 230-241

ABSTRACT

The skilled and dedicated professionals who strive to improve cybersecurity may unwittingly fall victim to misconceptions and pitfalls that hold other people back from reaching their full potential of being active partners in security. These pitfalls often reflect the cybersecurity community's dependence on technology and failure to fully appreciate the human element. This article offers cybersecurity professionals a primer so they can recognize and overcome six human element pitfalls in cybersecurity. In addition to gaining an awareness of these pitfalls, readers will learn about specific strategies on how to improve cybersecurity and empower users by addressing the human element in their organizations' cybersecurity products, processes, and policies.

KEYWORDS

cybersecurity; usability; usable security; human element; users

INTRODUCTION

Cybersecurity professionals perform a tremendous service in protecting their organizations, customers, communities, and even nations from cyber threats. Yet, despite having the noblest of intentions, they may be falling victim to misconceptions and pitfalls that hold people back from reaching their full potential of being active, informed partners in security. The six pitfalls in this paper – illustrated by real world examples and research findings – reflect the cybersecurity community's general tendency to focus and depend on technology to solve today's security problems while at the same time failing to fully appreciate the human element – the individual and social factors impacting security adoption. The intent of the article is not to criticize the cybersecurity community, but rather to prompt introspection and encourage consideration of the human element when developing and implementing cybersecurity technologies, processes, and policies.

THE HUMAN ELEMENT IN CYBER SECURITY

To appreciate the implications and importance of the human element in cybersecurity, it is helpful to first understand the foundational concepts of usability and usable cybersecurity.

Usability

The International Organization for Standardization definition of usability is “the extent to which people can use systems, products, and services with effectiveness, efficiency, and satisfaction to accomplish their goals in a specified context of use.”[1]

In the cybersecurity context, *systems, products, and services* can be many different things: traditional information technology (IT) (e.g., computers, mobile devices, software, services); processes (e.g., steps involved in authenticating to a system); cybersecurity policies and guidance documents (e.g., checklists, baselines); or cybersecurity training (e.g., awareness training).

Users are simply the people involved in or impacted by interactions with the systems, products, and services. A first inclination when hearing the term “users,” might be to think about “end users,” i.e., individuals who are not experts in IT or cybersecurity. However, in certain contexts, users can be more specific. For example, organizational decision makers (e.g., Chief Information Officers, Chief Information Security Officers, other executives, and managers) and policy makers are users of cybersecurity information, guidance, or policies. Technical staff (e.g., system administrators, help desk staff, cybersecurity analysts) can also be users as they ultimately implement and maintain cybersecurity technologies and processes and deal with the aftermath if something goes wrong. Software and hardware developers may be users of secure development guidance or security libraries when implementing mechanisms to protect their products.[2]

Goals are what people want to accomplish when using systems, products, and services. For example, an employee may have a goal of securely sending a file to a coworker or logging into a system. A policy maker may have a goal of taking a generic cybersecurity guidance document and customizing it for the organization. A security administrator may have a goal of setting up access control on a server.

Effectiveness, efficiency, and satisfaction are the core components of usability. Effectiveness is whether people can successfully achieve their goals, for example, whether an employee is able to report a phishing email to cybersecurity staff. Efficiency refers to the resources (e.g., time, cognitive) used to achieve those goals, for instance, how long it takes an employee to successfully authenticate to an application. Satisfaction is the intersection between a user’s physical, cognitive, and emotional responses when using a system, product, or service, and how well the user’s needs and expectations are met. For example, in the cybersecurity context, satisfaction could be influenced by the frustration a user experiences when being confronted with repeated security warnings.

Finally, *context of use* is a combination of user attributes, characteristics of tasks and goals, and the technical, organizational, social, and physical environments in which users are interacting with the technology. A cybersecurity context of use might include an employee in a coffee shop using a laptop to connect to their company's network.

Usable Cyber Security

In 2009, the U.S. Department of Homeland Security identified 11 hard problems in information security research, one of which was usable security.[3] The imperative in the report is still relevant today: "Security must be usable by persons ranging from nontechnical users to experts and system administrators. Furthermore, systems must be usable while maintaining security. In the absence of usable security, there is ultimately no effective security."

Usable security involves usability while also more broadly considering the perceptions, relationships, and behaviors of people when engaging with security. In other words, usable security is about considering the *human element*. Usable security should be an enabler, not a hindrance, to cybersecurity. The goal of usable security is to develop systems, products, and services that are usable *and* result in improved security outcomes.

Although organizations and cybersecurity professionals may outwardly acknowledge the significance of the human element, one wonders if real progress to help the humans in cybersecurity is being made. A recent Verizon report estimated that 82% of 2021 breaches involved the human element.[4] In 2020, 53% of U.S. government cyber incidents resulted from employees violating acceptable usage policies or succumbing to email attacks.[5]

What, then, may be holding the security community back? First, the cybersecurity field is technology-centric by nature, with technology being viewed as the ultimate solution to security problems.[6] A security evangelist at a large security awareness training firm agreed: "Humans have always been a big part of the computing picture, but for some reason, we always thought only technology solutions alone can fix or prevent issues…That is not a workable strategy."[7] Second, few security professionals have had formal or professional training about the human element or non-technical skills – like security risk communication, interpersonal skills, or usability - that facilitate interactions with security non-experts.[7] Third, taking a human-centric approach might be viewed as resource-intensive and an impediment to getting security implemented efficiently.[9] Finally, cybersecurity professionals may hold some misconceptions about the human element and the people they are ultimately supposed to be supporting.[10,11] These misconceptions, or pitfalls, are the focus of this article.

PITFALL #1: ASSUMING USERS ARE STUPID

The belief that "users are the weakest link" or "users are stupid" is prevalent throughout the cybersecurity community.[12] The reality is that, yes, people do make mistakes. However, belittling users can result in an unhealthy, "us vs them" relationship between cybersecurity professionals and the people they are ultimately tasked to support. In this dysfunctional relationship, cybersecurity professionals may be perceived as arrogant and condescending, while users are perceived as powerless, incompetent, or relegated to being rule followers.[13]

Research studies investigating the attitudes and behaviors of security non-experts reveal that users are not actually "stupid," but rather overwhelmed and ill-equipped, not necessarily through their own fault.[14,15] In particular, one research group interviewed general public individuals about their cybersecurity perceptions, challenges, and actions.[16] The group found evidence that their research subjects were suffering from a phenomenon known as “security fatigue,” which is a sense of resignation, weariness, frustration, or loss of control in people’s responses to cybersecurity.

There are several reasons for security fatigue.[17] First, cybersecurity is rarely someone’s primary task when they use a computing device or service. Some people think that cybersecurity is someone else’s responsibility, especially in organizational contexts. Cybersecurity tasks can also be seen as disruptive, for example, having to go through multiple steps to authenticate, or constantly being interrupted with security pop-up warnings. Second, most people are simply not cybersecurity experts. Yet, those who are experts may have unrealistic expectations about what users understand and how well they can make decisions based on sometimes incomplete or confusing information. Third, cognitive biases may be a factor. For example, people may suffer from an optimism bias in which they might believe, “No one would want to target me since I’m not that interesting” or an availability bias in which they think, “I can’t recall anything bad happening recently, so I don’t need to worry as much.”

Overturning Pitfall #1:

Aim to empower. Instead of the “blame game,” focus on empowering users to be active, capable partners in cybersecurity. Recognize that everyone is influenced by their experiences, goals, and expertise and that these influences do not necessarily make them incompetent or purposefully negligent. Make an effort to identify the root causes of *why* people may be struggling as a first step in determining *how* they can be better supported.

Build relationships and practice empathy*.* Practice empathy and seek to move beyond the “us vs. them” mentality. Empathy and positive relationship building between cybersecurity executives, professionals, and the users they support has two-fold benefits.[19] First, it strengthens professionals’ credibility and commitment in the eyes of users, resulting in more trust, engagement, and willingness to follow the cybersecurity guidance and seek out help if something seems suspicious. Indeed, empathetic organizations drive higher employee motivation and engagement. [18] Second, the active listening and interactions born from these relationships aid cybersecurity staff in better understanding users’ needs, perspectives, and challenges.

PITFALL #2: NOT TAILORING COMMUNICATIONS TO THE AUDIENCE

Cybersecurity professionals must frequently communicate security-related information to others, for example informing employees about a new security policy or process, disseminating awareness information about a new threat, or trying to convince leadership to invest in security. Unfortunately, experts may suffer from “curse of knowledge,” i.e., when experts in a field have a difficult time explaining the field to non-experts.[20] Thus, it is not uncommon for cybersecurity professionals to have a difficult time translating highly technical information into a language understandable to their intended audience.[21] Unfortunately, the use of technical jargon can negatively impact people’s engagement with technical topics.[22] Likewise, professionals may fail to tailor their security communications to appeal to what their audience cares about in their day-to-day work or personal lives. When communications are not tailored appropriately, some users in the intended audience may be unable to properly use the cybersecurity product, make sound security decisions, or understand the importance of cybersecurity.

An underlying root cause for ineffectual communication is a failure to identify and understand the users of the intended audience. There may be a tendency to lump people together and not account for differences among them (e.g., motivations, needs, and level of expertise) that may impact security attitudes and behaviors. Within an organization, there may be marked differences in security preferences between employees working in different business units and with different roles. For example, scientists in a mission organization who desire to openly share information with collaborators may approach the security of information quite differently than human resource specialists who must adhere to strict rules on access to personally identifiable information.

Consider the following example related to cybersecurity guidance published by the National Institute of Standards and Technology (NIST).[23] Most NIST guidance targets technical staff within organizations and is often quite detailed, and therefore, lengthy. A larger organization may have dedicated security staff capable of digesting and acting upon a long, technical document. But what about small businesses, especially micro businesses with few employees? Some of these businesses may be required to comply with NIST guidance, for example, those with a government contract. NIST received feedback that these businesses were overwhelmed by longer guidance and could not always adequately address security issues since they often lacked dedicated cybersecurity staff. In response, NIST has been taking steps to develop supplementary resources and formats that are tailored to this population, for example, the Small Business Cybersecurity Corner website[24] and quick start guides to simplify the 50+ page Cybersecurity Framework.[25]

Overturning Pitfall #2:

Be context aware. Being cognizant of the context of the audience is an essential first step in effective communications. Identify the users, their skill levels, constraints, values, and environments where users are interacting with cybersecurity systems, products, and services.

Be a translator. Tailor communications to be understandable to the intended audience. Start with plain language; online tools and training, such as those available from plainlanguage.gov, can help. Communications may also require some additional explanation and support for users who may lack concrete understanding of cybersecurity concepts. It is also valuable to engage representatives from the intended audience to provide feedback on draft communications to ensure understandability and appropriateness.

Make a personal connection*.* Communicate why security is important, including how it impacts users' work and the organization. Explaining non-security benefits in addition to the cybersecurity benefits may also motivate users. For example, when communicating to developers, a possible message may be that implementing secure development practices from the start can significantly reduce effort and cost required to detect and fix vulnerabilities later. Storytelling, sharing personal experiences, and referencing recent events can also encourage a personal connection and overcome potential cognitive biases.

Use different formats and media. Use a variety of formats and methods to disseminate cybersecurity information to accommodate different user preferences, learning styles, and constraints. For example, some people learn better from and prefer interactive activities, so in-person awareness events may resonate with them more. Others are more visual, so posters or videos might be appropriate.

Enlist help from others. Since many cybersecurity professionals may not be trained or skilled in communications, collaborate with the communications or marketing groups within the organization to provide feedback on both language and communications media.

PITFALL #3 UNINTENTIONALLY CREATING INSIDER THREATS DUE TO POOR USABILITY

Solutions that focus on cybersecurity without considering usability can backfire. In environments where users may be already pushed to their limits by time pressures or other distractions, unusable security can increase user burden. This burden can then result in the unwitting creation of insider threats – users who are frustrated with cybersecurity, more prone to making errors and risky decisions, and more likely to try less-secure workarounds.[26]

Complex password policies are a classic example of burden caused by poor usability in cybersecurity. Especially now that people have multiple online accounts, having to maintain many complex passwords can be taxing.[27] To cope, they resort to practices that may result in reduced security, for example, writing passwords on a sticky note or keeping passwords in an unencrypted text file on their computer. Perhaps most concerning is the frequent reuse of passwords across multiple accounts,[28] particularly in light of recent cyber attacks that disclosed customer passwords (e.g., data breaches of Marriott[28] and Plex[30]) or used previously compromised passwords to hack into customer accounts (e.g., an attack against the wedding registry site Zola[31]).

A particularly striking example of a workaround for a security measure was found in a reader-submitted article in a technical newsletter.[32] The reader worked in an organization that had mandated that a screen be automatically locked after five minutes of inactivity to prevent viewing of desktop contents when a user was away from their office. As a scientist, he often read papers or did other non-computer related tasks at his desk. Therefore, the screen lock was activating many times throughout the day, requiring him to reauthenticate each time. Frustrated, he devised a way to automatically move the computer mouse to avoid the lockout: a watch with a sweep second hand placed under the mouse. The scientist was so proud of his accomplishment that he told his colleagues, and they, too, implemented this solution. However, this workaround reduced security in the organization. Might this workaround been avoided if cybersecurity policy makers had taken the time to understand the context of use of their employees, how the policy might have negatively impacted them, and possible alternatives that were both secure and usable?

Overturning Pitfall #3:

Conduct basic usability testing. Usability expertise or formal usability testing are not required to identify potential usability issues. Do some simple piloting of proposed security solutions or communications with representative users; even testing with just five users is usually enough.[33] During piloting, observe the errors users make or the confusion they express. Then, apply these insights towards improving the security solution.

Provide concrete, achievable guidance. Provide tools and actionable guidance to help people make the right security decisions. Avoid a long laundry list of "to-dos" with complicated steps that may not be achievable by some users. Rather, break recommendations and security tasks down into manageable, prioritized chunks.

Offload burden when possible. Think about what can be done to lessen the burden on end users so that they are not forced to make decisions they may not be equipped to make or may cause significant effort and cognitive load. For example, can more filtering be done at the mail server so fewer phishing emails get delivered? How can authentication be simplified to alleviate burden on users while maintaining a high level of cybersecurity?

PITFALL #4 HAVING TOO MUCH SECURITY

Cybersecurity professionals, not surprisingly, want to make systems, products, and services as secure as possible, so they may implement a plethora of security solutions throughout the enterprise. Or they may take a "one-size-fits-all" approach in which they believe the most secure solution or configuration should always be implemented. However, there is such a thing as "too much" security. The most secure solution may not be necessary in every situation and may be impractical from both a resource and usability perspective. [34] Overly rigid and restrictive security rules and solutions often create the illusion of security but may result in unanticipated negative consequences for both technical and end users, including an increase in complexity and a decrease in users' understanding.

A survey of over 3,600 IT and cybersecurity professionals around the world found that complexity in security is rampant.[35] Over half of organizations deployed more than 30 security tools in their enterprises, with 30% deploying more than 50 security tools and 45% utilizing more than 20 tools just to respond to a typical security incident. Yet over half still reported a significant data breach in the preceding year, and over 60% of organizations fell victim to ransomware. Unsurprisingly, almost two-thirds said that fragmented IT and security infrastructure was a reason why cyber resiliency had not improved in their organization. Cybersecurity professionals are often overwhelmed by the lack of usability in this amalgamation of tools, resulting in an inability to quickly collect, filter, correlate, and assess data.[36] This shortfall is clearly illustrated by the 21-day average time between when an attacker infiltrates a network and when they are detected by organizational staff.[37]

From an end user perspective, stringent security measures can sometimes lead to greater insecurity as they are viewed as counterproductive and an impediment to flexibility in users' day-to-day operations.[38] Therefore, many employees violate cybersecurity policies at least occasionally. [39] This non-malicious negligence can put organizations at greater risk of cyber attack. For example, the Equifax breach, which exposed the sensitive data of over 140 million Americans, resulted from a single individual failing to "heed security warnings."[40]

Overturning Pitfall #4:

Take a risk-based approach. Avoid a "one-size-fits-all" stance on what security solutions are implemented within organizations. Performing a risk assessment (e.g., using a risk management framework[41]) can help determine what level of cybersecurity is appropriate for the environment.

Understand and support the capability of users. To help determine solution feasibility and likelihood of success, it is critical to understand how well the users (both technical staff and end users) are equipped to implement and react to the security measures. Select interoperable solutions and increase automation to reduce complexity and increase usability for technical staff so they can make effective and efficient use of security tools. Furthermore, attempt to understand the current constraints and stresses of end users and how added security processes may negatively impact their work.

PITFALL #5 DEPENDING ON PUNITIVE MEASURES OR NEGATIVE MESSAGING TO GET USERS TO COMPLY

Cybersecurity professionals and organizations may use punitive measures or focus on negative messaging to prompt users to comply with recommended security practices. Despite non-expert users' challenges when interacting with security solutions (due to lack of usability, knowledge, etc.), cybersecurity professionals may hold unrealistic expectations that users will *always* make good decisions and then punish them when they do not.

Punitive measures are common within organizations today. These measures may include disabling user accounts for not completing security training[42] or publicly shaming employees who cause cybersecurity incidents, for example by posting offenders' names in common workspaces.[43] In more extreme, but increasingly common situations, companies are firing employees who fall for phishing emails or make other cybersecurity errors.[44]

While appropriate in some situations, in others, punitive measures and focusing too much on negative consequences may be counterproductive. In fact, usable security researchers have found that, while fear appeals – scaring people into taking a recommended action by emphasizing potential negative outcomes of not complying – may have short term behavioral effects, they ultimately elicit longer term, negative emotions towards security.[45,46] Most concerning, punitive measures may fail to consider the root causes and motivations behind users' actions and the capacity of users to be able to avoid the incident.

A case in point is phishing. With an increase in the sophistication and precision targeting of phishing, anyone can fall prey to a phish. In recent years, researchers have been investigating why people click or do not click on phishing emails. In one study, a research team found that, in addition to typical phishing cues (e.g., spelling errors, sense of urgency), how an email aligned with the user context was a critical factor in determining whether someone clicked. [47] If the phishing email topic was relevant to a user's work role, the user was more likely to click because they did not want to neglect their duties. This observation played out in a real-world phishing scam against Facebook and Google.[48] Employees who regularly initiated monetary transactions with a vendor responded to a phishing email appearing to be from that vendor, resulting in a loss of over $100 million. While the perpetrator was ultimately brought to justice, who else in this case holds liability? Should the employees be punished for attempting to be diligent in their jobs?

Overturning Pitfall #5:

Motivate and empower users to take action. To motivate people to take action, cybersecurity professionals should honestly communicate the severity of the threat and potential consequences, while being careful not to overstate those. In addition to motivation, users must have confidence in their ability to do something about the threat, which requires providing them with specific instructions and tools. If people do not feel their actions will mitigate the threat, they are likely to choose not to act. [49]

Do not rely on fear or punishment alone. Organizations that offer positive incentives (e.g., virtual badges, small trinkets, formal recognitions, or a personal "thank you") to employees who demonstrate strong security behaviors have experienced encouraging shifts in security attitudes and behaviors.[50,51] Likewise, taking a collaborative, rather than punitive, approach can also be effective in spurring the adoption of security practices. In the book *Phishing Dark Waters*,[52] the authors provide an example of one organization's successful paradigm shift in addressing repeat phishing clickers. The organization moved from a penalizing stance to one that was more collaborative and involved one-on-one interactions with repeat clickers to better understand what challenges they were facing and personally walk them through tips for recognizing fraudulent emails.

PITFALL #6 NOT CONSIDERING USER-CENTRIC MEASURES OF EFFECTIVENESS

Collecting meaningful security metrics is a well-known challenge, with security return on investment often being difficult to measure.[53] Common security metrics include patches deployed, risk assessment scores, number of malware infections, and mean time to remediate risks. However, in this techno-centric field, organizations may neglect to seek out data about user behaviors and attitudes. Without this data, organizations are left in the dark about areas in which employees are doing well or shortfalls for which they may need more support.

Cybersecurity awareness training is an example of a security initiative necessitating user-centric data to gauge effectiveness. Many organizations, including those in the U.S. government, require their workforce to complete annual awareness training. These training requirements are intended to result in positive impacts on workforce cybersecurity behaviors.

In a survey of 96 government security awareness professionals and security leaders who oversee awareness programs,[51] about half believed that compliance (i.e., employee completion of training) was the most important indicator of success for their awareness programs. However, compliance metrics tell little about how employee behaviors and attitudes have changed. Furthermore, while over two-thirds of surveyed organizations relied on compliance-based indicators such as training completion rates and audit reports, only about 40% examined user security incident trends to identify behavioral impacts of awareness efforts. Less than a quarter surveyed their workforce to obtain first-hand feedback on whether training was valuable.

Employees often find security awareness training to be a boring, "check-the-box" activity.[55,56] How much of the training, then, are users are actually retaining? How engaged are users with the training? Is learning being translated into action? Without direct user feedback and concrete indicators of their behaviors, organizations will likely struggle to answer these important questions.

Overturning Pitfall #6:

Gather user-centric data*.* Collect both quantitative and qualitative indicators of users' security attitudes and behaviors, for example, those identified by security awareness training vendors SANS and Living

Security.[57,58] Think of concrete metrics as an initial identification of the problem (symptoms). For example, help desk calls can reveal user pain points, anduUser-level security incidents like phishing clicks or security violations can inform where users may need more support or training or better solutions. Then, try to get to the root cause of the symptoms, which requires understanding the context and going straight to the source (the users). Gather user feedback (e.g., via surveys, focus groups, one-on-one meetings) about their experiences and where they may be struggling. Provide feedback mechanisms so that employees can anonymously communicate their thoughts about security solutions without fear of reprisal.

Use the data to drive improvements. Use insights gained from the data to improve security solutions. To facilitate employees feeling valued and involved, communicate to them what was done to ensure their input was considered. This creates a sense of ownership and assurance that all stakeholders are viewed as respected partners in security.

SUPPORT IN OVERCOMING THE PITFALLS

Orienting an entire organization towards considering the human element in cybersecurity is, obviously, a non-trivial undertaking. While cybersecurity executives and professionals may have noble intentions of wanting users to be active partners in security, they may not know where to start or what to do. Additionally, addressing the human element may be perceived as “one more thing to do” in an already-long list of responsibilities.

How can cybersecurity professionals arm themselves with the knowledge and resources they need to address the human element? In addition to those resources mentioned in the “overturning” recommendations above, there are human-element forums, training materials, and guidance from SANS,[59] EDUCAUSE,[60] National Cybersecurity Alliance,[61] and NIST,[62,63] among others. Furthermore, cybersecurity groups can consider hiring team members with diverse skillsets more attuned to the human element (e.g., communications, psychology) to complement their existing technical expertise. Finally, for future impact, cybersecurity community leaders can advocate the inclusion of human-technology coursework within university IT, cybersecurity, and computer science programs to ensure the next generation of cybersecurity professionals is aware of the importance of the human element.

CONCLUSION

Considering the human element ultimately leads to what should be one of cybersecurity professionals most important goals: empowering users to be informed, capable, and active partners in security rather than seeing them as hopeless, ill-equipped victims or obstructionists. After all, cybersecurity professionals cannot hope to solve today’s cybersecurity challenges on their own; cybersecurity is a group effort requiring the commitment of everyone within an organization.

DISCLAIMER

Certain commercial companies or products are identified in this paper to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology (NIST). Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of NIST or the U.S. Government.

REFERENCES

1. International Organization for Standardization (2018), ‘ISO 9241-11:2018 - Ergonomics of human-system interaction – Part 11: usability: definitions and concepts’, available at https://www.iso.org/standard/63500.html (accessed 6th September, 2022).

2. Green, M. and Smith, M. (2016), ‘Developers are not the enemy! The need for usable security APIs’, *IEEE Security & Privacy*, Vol. 14, No. 5, pp. 40-46.

3. Department of Homeland Security (2009), ‘A Roadmap for Cybersecurity Research’, available at https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap_0.pdf (accessed 6th September, 2022).

4. Verizon (2022), ‘Data breach investigations report’, available at https://www.verizon.com/business/resources/reports/2022/dbir/2022-dbir-data-breach-investigations-report.pdf (accessed 24th October, 2022).

5. Office of Management and Budget (2021), ‘Federal Information Security Modernization Act of 2014 annual report to Congress’, available at https://www.whitehouse.gov/wp-content/uploads/2021/05/FY-2020-FISMA-Report-to-Congress.pdf (accessed 24th October, 2022).

6. Pfleeger, S.L. and Caputo, D.D. (2012), ‘Leveraging behavioral science to mitigate cybersecurity risk’, *Computers & Security*, Vol. 31, No. 4, pp. 597-611.

7. Montalbano, E. (May 2022), ‘Verizon Report: Ransomware, human error among top security risks’, Threat Post, available at https://threatpost.com/verizon-dbir-report-2022/179725/ (accessed 24th October, 2022).

8. Dawson, J. and Thomson, R. (2018), ‘The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance’, *Frontiers in Psychology*, Vol. 9, p. 744.

9. Post, G.V. and Kagan, A. (2007), ‘Evaluating information security tradeoffs: Restricting access can interfere with user tasks’, *Computers & Security*, Vol. 26, No. 3, pp. 229-237.

10. West, R., Mayhorn, C., Hardee, J. and Mendel, J. (2008), ‘The Weakest Link: A Psychological Perspective on Why’, In Gupta M, Sharman R, editors, *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*. IGI Global, Hershey, PA.

11. Zimmermann, V. and Renaud, K. (2019), ‘Moving from a “human-as-problem” to a “human-as-solution” cybersecurity mindset’, *International Journal of Human-Computer Studies*, Vol. 131, pp. 169-87.

12. West, ref 10 above

13. Zimmerman, ref 11 above

14. Busse, K., Schäfer, J. and Smith, M. (2019), 'Replication: no one can hack my mind - Revisiting a study on expert and non-expert security practices and advice', Proceedings of the 15th Symposium on Usable Privacy and Security.

15. Kang, R., Dabbish, L., Fruchter, N. and Kiesler, S. (2015), '"My data just goes everywhere:" User mental models of the internet and implications for privacy and security', Proceedings of the 11th Symposium on Usable Privacy and Security.

16. Stanton, B., Theofanos, M.F., Prettyman, S.S. and Furman, S. (2016), 'Security fatigue', *IT Professional*, Vol. 18, No. 5, pp. 26-32.

17. *Ibid.*

18. BusinessSolver (2022), '2022 State of workplace empathy', available at https://resources.businessolver.com/2022_empathy_executive_summary/2022-empathy-executi (accessed 24th October, 2022).

19. Haney, J.M. and Lutters W.G. (2018), '"It's scary…It's confusing…It's dull": How cybersecurity advocates overcome negative perceptions of security', Proceedings of the 14th Symposium on Usable Privacy and Security.

20. Heath, C. and Heath, D. (2007), *Made to stick: Why some ideas survive and others die*, Random House, New York, NY.

21. Haney, ref 19 above

22. Shulman, H.C., Dixon, G.N., Bullock, O.M. and Colón Amill, D. (2020), 'The effects of jargon on processing fluency, self-perceptions, and scientific engagement', *Journal of Language and Social Psychology*. Vol. 39, No. 5-6, pp. 579-97.

23. National Institute of Standards and Technology (2022), 'Computer security resource center', available at https://csrc.nist.gov/ (accessed 6th September, 2022).

24. National Institute of Standards and Technology (2022), 'Small business cybersecurity corner', available at https://www.nist.gov/itl/smallbusinesscyber (accessed 6th September, 2022).

25. National Institute of Standards and Technology (2019), 'Manufacturer extension partnership national network – cybersecurity', available at https://www.nist.gov/system/files/documents/2019/03/06/2018_cybersecurity_framework_overview.pdf (accessed 6th September, 2022).

26. Yayla, A. (2011), 'Controlling insider threats with information security policies', Proceedings of the European Conference on Information Systems.

27. Choong, Y.Y. and Theofanos, M.F. (2015), 'What 4,500+ people can tell you – Employees' attitudes toward organizational password policy do matter', Proceedings of 3rd International Conference on Human Aspects of Information, Security, Privacy, and Trust.

28. Harris Poll (2019), ‘Online security survey’, Google, available at https://services.google.com/fh/files/blogs/google_security_infographic.pdf (accessed 24th October, 2022).

29. Marriott International (March 2020), ‘Marriott International notifies guests of property system incident’ available at https://news.marriott.com/news/2020/03/31/marriott-international-notifies-guests-of-property-system-incident (accessed 24th October, 2022).

30. Whittaker, Z. (August 2022), ‘Plex warns users to reset passwords after data breach’, available at https://techcrunch.com/2022/08/24/plex-streaming-breach-passwords/ (accessed 24th October, 2022).

31. Page, C. and Whittaker, Z. (May 2022), ‘Hackers compromised some Zola user accounts to buy gift cards’ available at https://techcrunch.com/2022/05/23/zola-accounts-hacked/ (accessed 24th October, 2022).

32. Altshuler, E. (December 2021), ‘A countermeasure to overcome a mandated screen saver’, IEEE Life Members Newsletter.

33. Nielsen, J. (March 2000), ‘Why you only need to test with 5 users’, Nielsen Norman Group, available at https://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/ (accessed 6th September, 2022).

34. Donaldson, S., Siegel, S., Williams, C.K. and Aslam, A. (2015), *Enterprise cybersecurity: how to build a successful cyberdefense program against advanced threats*, Apress, New York, NY.

35. IBM Security (2021), ‘Cyber resilient organization study’, available at https://www.ibm.com/resources/guides/cyber-resilient-organization-study/ (accessed 24th October, 2022).

36. Staddon, J. and Easterday, N. (2019), ‘“It's a generally exhausting field”: A Large-Scale Study of Security Incident Management Workflows and Pain Points’, 17th International Conference on Privacy, Security and Trust.

37. Mandiant (2022), ‘M-Trends 2022’, available at https://www.mandiant.com/m-trends (accessed 24th October, 2022).

38. Post, ref 9 above

39. Posey, C. and Shoss, M. (January 2022), ‘Research: Why employees violate cybersecurity policies’, Harvard Business Review, available at https://hbr.org/2022/01/research-why-employees-violate-cybersecurity-policies (accessed 24th October, 2022).

40. Bernard, T.S. and Cowley, S. (October 2017), ‘Equifax breach caused by lone employee’s error, former CEO says’, New York Times, available at https://www.nytimes.com/2017/10/03/business/equifax-congress-data-breach.html (accessed 24th October, 2022).

41. National Institute of Standards and Technology (2022), ‘NIST Risk Management Framework’, available at https://csrc.nist.gov/projects/risk-management/about-rmf (accessed 6th September, 2022).

42. Haney, J., Jacobs, J., Furman, S. and Barrientos, F. (March 2022), ‘NISTIR 8420A Approaches and Challenges of Federal Cybersecurity Awareness Programs’, available at https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8420A.pdf (accessed 6th September, 2022).

43. Powers, B. (April 2022), ‘Some companies still fire people for getting phished. It doesn’t make them more secure’, Grid, available from https://www.grid.news/story/technology/2022/04/19/some-companies-still-fire-people-for-getting-phished-it-doesnt-make-them-more-secure/ (accessed 6th September, 2022).

44. Brooks, L. (March 2022), ‘New research: one in four employees who made cybersecurity mistakes lost their jobs last year’, Tessian, available at https://www.tessian.com/blog/new-research-psychology-of-human-error/ (accessed 6th September, 2022).

45. Dupuis, M.J., Renaud, K. and Jennings, A. (2022), ‘Fear might motivate secure password choices in the short term, but at what cost?’, 55th Hawaii International Conference on Systems Sciences.

46. Renaud, K. and Dupuis, M. (2019), ‘Cybersecurity fear appeals: Unexpectedly complicated’, New Security Paradigms Workshop.

47. Greene, K.K., Steves, M., Theofanos, M.F. and Kostick, J. (2018), ‘User context: an explanatory variable in phishing susceptibility’, Proceedings of the 2018 Workshop on Usable Security.

48. Huddleston, T. (March 2019), ‘How this scammer used phishing emails to steal over $100 million from Google and Facebook’, CNBC, available at https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html (accessed 24th October, 2022).

49. Sommestad, T., Karlzén. H. and Hallberg, J. (2015), ‘A meta-analysis of studies on protection motivation theory and information security behaviour’*, International Journal of Information Security and Privacy*, Vol. 9, No. 1, pp. 26-46.

50. Haney, ref 19 above

51. Haney, ref 42 above

52. Hadnagy, C. and Fincher, M. (2015*), Phishing dark waters: The offensive and defensive sides of malicious emails*. John Wiley & Sons, Hoboken, NJ.

53. Onwubiko, C. and Onwubiko, A. (2019), ‘Cyber KPI for return on security investment’, Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment.

54. Haney, ref 42 above

55. Bada, M., Sasse, A.M. and Nurse, J.R.C. (2019), ‘Cybersecurity awareness campaigns: Why do they fail to change behaviour?’, *arXiv preprint*, available at https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf (accessed 6th September, 2022).

56. Haney, J.M. and Lutters, W.G. (October 2020), ‘Security Awareness Training for the Workforce: Moving Beyond “Check-the-box” Compliance’, *IEEE Computer*, Vol. 53, No. 10, pp. 91-95.

57. Spitzner, L. (November 2021), ‘Security awareness metrics – what to measure and how’, SANS Institute, available at https://www.sans.org/blog/security-awareness-metrics-what-to-measure-and-how/U (accessed 24th October, 2022).

58. Living Security (September 2021), ‘How to measure cybersecurity behavior and drive long-lasting cultural change’, available at https://www.livingsecurity.com/blog/how-to-measure-cybersecurity-behavior-and-drive-long-lasting-change (accessed 24th October, 2022).

59. SANS Security Awareness (2022), ‘Resources’, SANS Institute, available at https://www.sans.org/security-awareness-training/resources/ (accessed 24th October, 2022).

60. EDUCAUSE (2022), ‘Security awareness’, available at https://library.educause.edu/topics/cybersecurity/security-awareness (accessed 24th October, 2022).

61. National Cybersecurity Alliance (2022), ‘Resources’, available at https://www.stopthinkconnect.org/resources (accessed 24th October, 2022).

62. National Institute of Standards and Technology (2022), ‘Federal Information Security Educators (FISSEA)’, available at https://www.nist.gov/itl/applied-cybersecurity/fissea (accessed 24th October, 2022).

63. National Institute of Standards and Technology (2022), ‘Usable Cybersecurity’, available at https://csrc.nist.gov/projects/usable-cybersecurity (accessed 24th October, 2022).