NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Human-Centered Cybersecurity Guidelines and Resources Concept Paper

Information Technology Laboratory
National Institute of Standards and Technology

August 12, 2026

Note to Reviewers

This concept paper introduces NIST's goal to publish guidelines and resources[1] to assist organizations and professionals in addressing the human aspects of cybersecurity, collectively known as **human-centered cybersecurity (HCC)**. HCC aims to improve cybersecurity outcomes by putting people and their needs, abilities, and limitations at the forefront when designing, implementing, and making decisions about cybersecurity policies, processes, technologies, and services.

As input to this effort, the NIST Human-Centered Cybersecurity program team has prepared this concept paper to communicate overarching themes identified through extensive interactions with cybersecurity stakeholders, including possible options for framing and developing human-centered cybersecurity guidelines and resources.

NIST welcomes stakeholder feedback to inform the path forward. We encourage stakeholders to read this concept paper, then share their perspectives on the following.

Scope

- Which elements of HCC are most critical to address through NIST guidelines and resources?
- To which existing NIST cybersecurity guidelines, publications, or efforts (e.g., those in the NIST Computer Security Resource Center) should NIST align HCC guidelines and resources?
  - Among these, which should be prioritized for alignment?
- Which publication types and formats should NIST develop to aid organizations in implementing HCC concepts? (See **Guideline and Resource Options** section.)
- Should NIST also produce guidelines and resources related to human-centered privacy?

Ensuring Value

- What should NIST consider for ensuring HCC guidelines and resources are actionable and valuable to organizations of various sizes and sectors?
- What resources and framing are needed to effectively communicate the value of HCC approaches to organizational decision makers, cybersecurity staff, and product developers?
- What else, if anything, should NIST consider to inform the development of practical and meaningful HCC guidelines and resources?

[1] For the purposes of this concept paper, we define guidelines as suggested outcomes or ways in which human-centered cybersecurity might be realized within organizations. Resources include any materials or communications that can aid organizations (e.g., case studies, videos, and trainings).

Related Evidence and Efforts

- What kind of evidence (e.g., industry reporting, academic research) is preferred to support HCC guidelines and resources?
- What, if any, related frameworks, reports, or other resources should NIST consider when developing HCC guidelines and resources?
- With which groups and activities should NIST connect to inform its HCC efforts?

Please send feedback to human-cybersec@nist.gov with the subject line "HCC Concept Paper" through **September 30, 2026**.

NOTE: All comments are subject to release under the Freedom of Information Act (FOIA). NIST may use a variety of software tools to help summarize comments, including AI. If AI is used, comments will not be used to train AI models. Any public reporting of comments will be done in aggregate, with no attribution to individuals or organizations.

Disclaimer

Certain commercial companies, products, and views are identified to foster understanding. Such identification does not imply recommendation or endorsement by NIST, nor does it imply that these are necessarily the best available for the purpose.

Graphics Attribution

All graphics included in this paper are from Canva version 1.122.0.0.

Disclosure

Questions in Note to Reviewers and sidebar titles were edited with the assistance of Gemini (version 3), developed by Google. Gemini was used to refine language and improve clarity in accordance with the authors' instructions. All content has been reviewed and verified by the authors to ensure accuracy and originality.

Introduction

While many positive strides in cybersecurity have been made over the years, it is becoming increasingly evident that current technology-centric approaches to cybersecurity have not sufficiently progressed organizations in addressing the critical "human element" of cybersecurity.

Industry analysis and reporting reveal that a substantial percentage of cyber data breaches can be attributed to the human element [15][29]. Human errors leading to breaches may involve unintentional mistakes—such as falling for social engineering schemes or inadvertent system misconfigurations—or non-malicious actions meant to streamline workflows or reduce cognitive burden, for example, reusing passwords, postponing urgent updates, or ignoring security warnings [4][17][29]. A single lapse can result in significant organizational impacts and disruptions, substantial expenditures towards incident response and recovery, reputational damage, downtime, or regulatory fines [4][13][22][26]. Further, full recovery and resolution of the legal "long tail" of breaches can potentially take years.

While human error and risk are often emphasized—skewing the perception of humans as only being vulnerabilities [6]—people also play a positive role in organizational cybersecurity. They can be active partners in cybersecurity via various roles such as cybersecurity and IT professionals, human "sensors" and reporters of suspicious activity, and security champions. As cybersecurity expert Phil Venables noted [28]:

> "In every incident or close-call I've ever worked on, where there was an assignment of root cause to human error it actually turned out, when you looked at it more deeply, to be a situation where **the humans were in fact performing heroics**. These were heroics in the face of a poorly designed environment, terrible user interface, system operation issues or other factors."

While employees undoubtedly impact organizational cybersecurity, the converse is also true: cybersecurity interactions can impact employees and their ability to accomplish organizational objectives [21]. From a positive perspective, a strong cybersecurity culture can result in greater overall job satisfaction, motivation, productivity, and sense of responsibility for the security of the organization [3][12].

Negatively, in the face of dynamic and constant cyber threats, work pressures, and growing complexity in the cybersecurity ecosystem, cybersecurity professionals increasingly experience stress and burnout. Stress and burnout can adversely impact professionals' cognitive state, health, and job performance [7][31], ultimately undermining organizational productivity, workforce stability, and resilience [20]. Beyond cybersecurity professionals, general employees' work satisfaction, productivity, and engagement may be negatively impacted if they become frustrated or fatigued with cybersecurity processes and technologies they view as difficult to use or understand, disruptive to their work tasks, punitive, or not relevant to them [16][24][30].

Taking a Human-Centered Approach

Cybersecurity is typically developed, implemented, and used by humans, existing to protect the economic security, information, and quality of life of people and the organizations they depend upon. Therefore, cybersecurity programs ought to recognize the importance of considering human nature and needs—rather than solely relying on technology—when developing cybersecurity strategies and solutions.

NIST uses the term **human-centered cybersecurity (HCC)** to describe an approach to cybersecurity that focuses on people (all individuals influencing and influenced by cybersecurity). At a high level, human-centered cybersecurity is about improving cybersecurity outcomes by putting people and their needs, abilities, and limitations at the forefront when designing, implementing, and making decisions about cybersecurity policies, processes, technologies, and services.

While there is growing recognition of the importance of human-centered approaches, there are few, if any, community standards or practitioner-focused guidelines and resources for realizing HCC in practice [23]. NIST intends to address these gaps by:

- Developing a community-informed description and value proposition for HCC
- Providing actionable guidelines and other resources to help organizations implement HCC practices

NIST will develop HCC guidelines and resources in collaboration with a broad range of cybersecurity stakeholders representing both practitioner and researcher communities. This work is consistent with NIST's broader cybersecurity efforts—as called for by the Cybersecurity Enhancement Act of 2014—to develop voluntary, consensus-based standards and procedures to reduce cyber risks to critical infrastructure by supporting cybersecurity awareness and preparedness and advancing cybersecurity technical standards.

NIST requests community feedback to ensure future HCC efforts and outputs are valuable and actionable for organizations of varying sizes and sectors.

Intended Audiences

The intended audience of future NIST HCC guidelines and resources is broad, including:

- individuals who develop, implement, lead, and govern organizational cybersecurity programs, systems, policies, training programs, and workforce initiatives
- designers and developers of cybersecurity technologies and products
- stakeholders involved in risk, technology, and resource management
- individuals who set and influence policy and standards at a higher level

The guidelines and resources can be tailored to different organizations and stakeholder groups.

Desired Outcomes

The planned effort to produce HCC guidelines and resources seeks to achieve the following outcomes.

- A common understanding of the scope and value of human-centered cybersecurity is established and communicated.
- Clarity is provided on whether HCC is primarily an approach—measured by indicators of adoption and maturity—or an outcome—requiring other measures of success such as culture, trust, usability, or resilience.
- Actionable, practical guidelines and resources to help organizations of varying sizes and sectors implement HCC in their cybersecurity programs are established and communicated.
- The relationship between HCC and specific existing NIST cybersecurity guidelines and frameworks is established and communicated.

NIST is open to suggestions on how these outcomes may be achieved and if there may be other desired outcomes for this effort.

Paper Structure

In this concept paper, we first describe the catalysts for the HCC efforts: themes identified through NIST's extensive interactions with a wide range of cybersecurity stakeholders. We then present possible approaches to developing and publishing HCC guidelines and resources. Throughout the paper, we include examples of real-world HCC approaches—in the words of stakeholders—within sidebars.

Co-Creating Cybersecurity

An internal, company workshop exploring how staff perceive cybersecurity as a barrier to productivity "started an initiative within the company where staff were actively involved in co-creating the security processes.

Rather than the security team sitting in a dark room, thinking, 'Okay, what's the security process for this, for that?' they created a draft, worked with a little small staff team, and they created and adapted it in a way that sort of was less onerous than it was previously.

So, it was very successful. But the most important thing, I think, was the sense that people within [the company] were going to be listened to. And that is really, really powerful."

– Human Factors/Behavior Practitioner working in industry

People-First Software Development

"I always start with the development team understanding why we're developing software, and it doesn't have anything to do with technology…Technical pieces facilitate and serve the people, and so cybersecurity needs to be the same way...

I've had to do a lot of advocating across my career in, 'Is that usable?' You can put all those things on the screen,… but if it doesn't flow correctly, then the people aren't going to like it, even if all the information they asked for was there.

So that's a way of looking at the user interface as the eighth layer: how we touch the human."

– Software Development Consultant working in industry

A Community-Driven Effort

A broad range of input sources from cybersecurity stakeholders in industry, government, academia, and non-profits catalyzed and informed the decision to develop HCC guidelines and resources. Through this feedback, we identified several overarching themes related to current community observations, needs, and challenges.

Input Sources

We synthesized direct stakeholder input from several sources, including the following:

- Two NIST survey research studies on the HCC research-practice gap with over 280 cybersecurity practitioners and HCC researchers [9][10]
- Recent NIST interviews and a survey exploring HCC from the perspectives of over 360 participants in different stakeholder groups to identify current interpretations of HCC and how HCC might be realized in practice
- Workshops co-organized with NIST focused on identifying HCC challenges and strategies [2][8]
- Stakeholder feedback communicated via: many meetings and conversations with cybersecurity and HCC experts and organizational representatives; comments on dozens of NIST HCC publications, blogs, and other media; and interactions during over 100 NIST presentations on HCC topics
- Other NIST Human-Centered Cybersecurity program research evidence from interviews and surveys about people's challenges, successes, understandings, and needs in cybersecurity, including perspectives from individuals with and without specialized cybersecurity expertise

We also augmented NIST's own first-hand stakeholder interactions with insights from other credible research and industry institutions, including:

- A large body of research evidence from external groups working in HCC and related disciplines (e.g., work published in academic conferences [1][25][27])
- Government, nonprofit, and industry reports signaling the need for and importance of addressing the human element in cybersecurity (e.g., [5][18][19])

What We Heard

We identified the following overarching themes based on community input.

People should be at the center of organizational cybersecurity programs.

As with all complex systems, an organization's cybersecurity program involves and must consider technology, process, and people. Organizations should not focus on just one or two components of this triad, but rather on the relationships between all three. Importantly, HCC is not separate from cybersecurity; rather it is an approach to cybersecurity that ensures people are at the core of the triad.

Taking a human-centered approach is critical for achieving better cybersecurity outcomes.

By considering people's needs and challenges, instilling a sense of ownership for cybersecurity, and designing systems that make secure behaviors easier, organizations can reduce the likelihood of cyber incidents and improve cybersecurity resilience.

HCC can promote industrial competitiveness and be a strategic advantage for organizations.

Beyond facilitating a stronger cybersecurity posture, HCC can enable organizational success by: informing risk management strategies; reducing incident-related costs and reputational harm; protecting organizational assets (e.g., people and intellectual property); improving employee satisfaction and motivation towards achieving organizational goals; and boosting productivity by eliminating cybersecurity friction and reducing burnout among security professionals.

HCC is multi-faceted.

HCC requires a multi-pronged approach that goes beyond cybersecurity awareness and training and includes: security culture; human-system interactions; communications; human cognition, behaviors, and perceptions; human vulnerabilities; and human strengths.

The "human-in-the-loop" will not be going away with the growing use of AI or other technology advancements.

HCC can help fortify organizations against the risks that the continually evolving technology landscape presents. While artificial intelligence (AI) and other emerging technologies have the potential to improve efficiency and reduce human burden in cybersecurity, people will remain the linchpin of a robust cybersecurity strategy. As a NIST interview study participant explained, "A lot of the things that make or break the tools, the protections, the outcomes, and the operational components of cybersecurity are dependent entirely on people [and] teams." Furthermore, the intersection of AI and HCC must be carefully considered as AI can both positively and negatively impact people's cybersecurity interactions.

Responsibility for HCC extends across multiple roles.

Organizational leadership, technologists, policy makers, risk managers, human resource specialists, cybersecurity educators and trainers, and HCC experts all hold some responsibility for ensuring HCC is implemented. Collaboration and open communication between these roles and with employees are key.

The Security Balancing Act

"I do...external consulting with people in healthcare. And so this is always on my mind about balancing having too much security or to balance their compliance and sort of security and privacy needs with the things they actually need to do.

So if this is a healthcare provider and they choose not to have personal cell phones in the environment, we have a conversation about, 'Okay, what are the alternative mechanisms for authentication, if that is your decision?'

I'm very cognizant that more security is not always better, that even as a computer scientist, optimal cybersecurity is not always the best choice. And so I'm very cognizant of those choices when I talk to them."

– Cybersecurity Professional working in industry

Testing Training, Not People

A company's punitive phishing simulation training resulted in employees being afraid to respond to email. Therefore, "I advised the management to drop their punishment thing entirely and instead to reframe what the phishing exercise was meant to do.

The phishing exercise isn't meant to test the human. The phishing exercise is designed to test the training and the supports for the human. And...if the human incorrectly or did the thing that they weren't supposed to do with the phishing exercise, then to launch an investigation to get them to tell the security team what support they needed, what support failed in order for them to have a different behavior next time.

And once we swapped that around,...we solved the problem of people being afraid of email entirely. We were no longer losing random business as a result. And we were able to engage with the humans, with the staff, and have fruitful conversations and realizing that there were other supports that were needed for certain people in certain departments because of the way they functioned, and what the company had in place just wasn't sufficient for their needs."

– Chief Information Security Officer working in industry

Stakeholders highlighted a number of **challenges** to widespread acceptance and adoption of HCC that need to be acknowledged and addressed, including the following.

There are inconsistent interpretations of HCC.

Different stakeholders may have differing views on the scope of HCC, who HCC includes (e.g., just "end users" or everyone, including security professionals), and its value to organizations.

Cybersecurity is a technology-dominated field, with the role and importance of people often diminished.

A common, long-standing adage within the cybersecurity community is that humans are a "weak link" that must be mitigated by technical solutions. This mindset can be limiting and harmful. Yet, shifting away from this view is a nontrivial undertaking.

Many organizations rely solely on annual, computer-based cybersecurity awareness and training to address the human element.

These organizations operate under the flawed assumptions that 1) employees always pay attention to and retain the information presented via training and 2) lack of knowledge is the biggest reason employees do not behave securely.

The current cybersecurity workforce lacks the skills needed to effectively implement HCC.

There is little HCC expertise within organizations, with cybersecurity professionals rarely trained in the human aspects of cybersecurity and few human factors or psychology experts embedded within cybersecurity teams.

Few cybersecurity frameworks and guidelines address HCC.

Beyond mentions of security awareness and training, cybersecurity frameworks and guidelines tend to focus on technical controls and seldom explicitly call out HCC practices. Thus, organizations are unsure how to take a human-centered approach.

There is uncertainty among organizations about how to measure HCC outcomes and show positive impact.

There are few standards relating to measuring the effectiveness of HCC efforts. For example, within industry reporting, there are inconsistent categorizations and scope related to the role of the human element in cybersecurity breaches [6].

There is a large body of scientific evidence on HCC and related fields (e.g., usable security, psychology, sociology) that may not be accessible to practitioners.

There is a substantial research-practice gap in HCC. Research may not be easily found by practitioners and is seldom translated into practices actionable enough for organizational implementation.

> ### Stakeholders called upon NIST to take an active role in addressing these challenges by providing clarity, guidelines, and resources on HCC.
>
> Stakeholders suggested that these guidelines and resources be aligned with existing, widely-adopted cybersecurity frameworks and standards. Guidelines and resources would also benefit from being developed in collaboration with external stakeholders and HCC experts.

Guideline and Resource Options

To address the identified community needs and gaps, NIST proposes the development and publication of guidelines and resources to aid organizations in incorporating human-centered cybersecurity approaches in practice. As guiding principles, we will aim for these outputs to be:

- community-informed and driven by community needs
- complementary to existing NIST cybersecurity guidelines, with any applicable mappings to these publications provided as a National Online Information Reference (OLIR)
- supported by evidence and widely-accepted principles[2]
- valuable and actionable to organizations of varying sizes, resource levels, and sectors
- focused on non-prescriptive outcomes while also providing exemplars to aid organizations in envisioning how HCC might fit within their own cybersecurity programs
- clearly communicated in engaging, easy-to-understand, and usable formats

The following non-exhaustive approaches and formats have been suggested by stakeholders, with further community feedback on the desirability and scope of these or alternative options requested. The most suitable path forward may be to pursue multiple or a combination of options.

[2] Due to the current lack of authoritative, practitioner-focused HCC resources, extensive cross-referencing to other established HCC-related publications may not always be possible. That being said, international usability standards (e.g., ISO [14]) and extensive interdisciplinary research (e.g., works published in [1][25][27]) already exist in this domain. This body of knowledge also includes evidence drawing on proven principles from related behavioral sciences like psychology and sociology, as well as applicable human factors lessons from sectors such as aviation and healthcare.

The Power of Listening First

"We held focus groups across campus to understand: what do people know about cybersecurity? Where do they feel like there are gaps? What's hard about it? What do they want to know more about? So we'd listen and ask questions, gain clarity.

I felt like that was so important to understand because one of the things that people told us is that they wanted information that felt streamlined so they knew what to do. They didn't understand what to do. And they told us that cybersecurity seemed very complicated, and they were confused by it.

So, that informed our thinking about how to approach things [in our security awareness program]."

– Security Awareness Program Manager working at a university

Potential Publication Types

NIST is planning an initial, foundational publication that communicates the scope, goals, and organizational benefits of HCC. This publication will establish common ground on an HCC description and the importance of HCC to organizational cybersecurity programs.

Subsequent guidelines and resources will provide more detail on how organizations can take a human-centered approach in their cybersecurity programs. These may take multiple forms, such as the following:

- **Direct integration of HCC guidelines into existing NIST cybersecurity publications:** HCC guidelines would be "baked into" the publications alongside the technical guidelines. An example of this approach is the NIST Special Publication 800-63 Digital Identity Guidelines series, which includes sections on customer experience (usability and customer success considerations). An addendum to an existing publication might also be a suitable alternative.

- **Standalone publications aligned with existing NIST cybersecurity publications:** HCC guidelines or resources would be presented in their own separate documents but would show direct mappings to other NIST cybersecurity guidelines. Standalone publications might be similar to overlays (e.g., NIST Risk Management Framework Security and Privacy control Overlay) or community profiles (e.g., NIST CSF Community Profiles), which allow for guideline customization for specific circumstances or conditions or for groups of organizations with shared interests, goals, and outcomes. A standalone publication option might also be especially appropriate when HCC guidelines cannot be immediately integrated into a NIST publication, for example, because the publication is not slated for near-term revision.

- **Short, standalone publications on specific HCC topics:** HCC guidelines or resources would be published on their own—possibly aligned with existing NIST publications—and provide information on specific HCC topics (e.g., cybersecurity culture, usable cybersecurity, human-centered cybersecurity communications). These publications might include handouts that provide high-level takeaways (e.g., handout on human-centered cybersecurity pitfalls [11]) or narrative documents that provide a deeper dive into a topic.

- **Case studies:** These would be documented, real-world examples of 1) how HCC has been successfully integrated into organizations of varying sizes, sectors, and resources or 2) negative consequences of a lack of HCC. For example, the National Initiative on Cybersecurity Education (NICE) Framework resources include a Success Story Catalog.

Potential Formats

Stakeholders also suggested options for guidelines and resource formats and communication channels, including the following non-exhaustive list.

- **Quick start guides**, similar to CSF 2.0 Quick Start Guides
- **Videos**, similar to Small Business Cybersecurity and Privacy Videos
- **Tools and methodologies**, similar to NICE Framework Tools or NIST Phish Scale
- **Checklists and templates**, similar to the CSF 2.0 Organizational Profile template
- **Training modules on HCC** for cybersecurity professionals and organizational decision makers, similar to NIST Risk Management Framework Introductory Courses

Engaging with NIST

Feedback on this concept paper, particularly those addressing the questions posed at the beginning of this publication in **Note to Reviewers**, may be submitted to human-cybersec@nist.gov with the subject line "HCC Concept Paper" through **September 30, 2026**.

Additionally, we invite interested parties to:

- Join the NIST Information Technology Lab (ITL) Human-Centered Cybersecurity GovDelivery mailing list for future updates on this and other HCC efforts.
- Join the NIST Human-Centered Cybersecurity Community of Interest, an online forum for practitioners and researchers to discuss and share information on HCC topics.
- Visit the NIST Human-Centered Cybersecurity website to view publications and resources developed by our program team.

References

1. Association for Computing Machinery (2026). *CHI Conference on Human Factors in Computing Systems*. https://dl.acm.org/conference/CHI

2. Cognitive Security Institute (2026). *CognectCon Tampa '26*. https://www.cognectcon.com/

3. D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, 22(5), 474-489. https://doi.org/10.1108/IMCS-08-2013-0057

4. Federal Bureau of Investigation. (2025). *FBI Internet Crime Complaint Center (IC3) 2025 annual report*. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

5. Gartner. (2023). *Gartner identifies the top cybersecurity trends for 2023: Security leaders must pivot to a human-centric focus to establish an effective cybersecurity program*. https://www.gartner.com/en/newsroom/press-releases/04-12-2023-gartner-identifies-the-top-cybersecurity-trends-for-2023

6. Grandhi, S.R., & Still, J. D. (2025). Deciphering human error: Improving cybersecurity reporting. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vo. 69, No. 1, pp. 234-239). https://doi.org/10.1177/10711813251358790

7. Gupta, V., Rangarajan, A., & Nobles, C. (2024). Burnout in the cybersecurity profession: a scoping review. In *Proceedings of the 19th Midwest Association for Information Systems Conference*. 2024. https://aisel.aisnet.org/mwais2024/20

8. Haney, J., Canham, M., Elkins, M., Flynn, L., Gordin, M., Granova, V., Huang, W., Jacobs, J., Moody, G., Rangarajan, A., Ross, M., Thomson, R., & Uchill, J. (2025). *Workshop summary report for ConnectCon 2024: "Minding the gaps in human-centered cybersecurity"*. US Department of Commerce, National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1332

9. Haney, J., Cunningham, C., & Furman, S. M. (2024, February). Towards integrating human-centered cybersecurity research into practice: a practitioner survey. In *Proceedings of the Symposium on Usable Security and Privacy (USEC)*. https://doi.org/10.14722/usec.2024.23013

10. Haney, J. M., Cunningham IV, C., & Furman, S. M. (2024). Towards bridging the research-practice gap: Understanding researcher-practitioner interactions and challenges in human-centered cybersecurity. In *Proceedings of the Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)* (pp. 567-586). https://www.usenix.org/system/files/soups2024-haney.pdf

11. Haney, J., & Furman, S. (2023). *Handout: Users are not stupid: Six cybersecurity pitfalls overturned.* https://csrc.nist.gov/pubs/other/2023/01/30/handout-users-are-not-stupid-six-cybersecurity-pit/final

12. Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. In *Proceedings of the 52nd Hawaii International Conference on Systems Science* (pp. 6398-6407). https://doi.org/10.24251/HICSS.2019.769

13. IBM. (2025). *Cost of a Data Breach Report: The AI Oversight Gap*. https://www.ibm.com/reports/data-breach

14. International Organization for Standardization (2018). *ISO 9241-11:2018 Ergonomics of human-system interaction, Part 11: Usability: Definitions and concepts*. https://www.iso.org/standard/63500.html

15. Mandiant. (2026). *Mandiant M-Trends 2026 report*. https://cloud.google.com/security/resources/m-trends

16. Mizrak, F., Demirel, H.G., Yaşar, O., & Karakaya, T. (2025). Digital detox: exploring the impact of cybersecurity fatigue on employee productivity and mental health. *Discover Mental Health*, *5*(1), 25. https://doi.org/10.1007/s44192-025-00149-x

17. Morgan, P. L., Asquith, P. M., Bishop, L. M., Raywood-Burke, G., Wedgbury, A., & Jones, K. (2020). A new hope: Human-centric cybersecurity research embedded within organizations. In *International Conference on Human-Computer Interaction* (pp. 206-216). https://doi.org/10.1007/978-3-030-50309-3_14

18. National Academies of Sciences, Engineering, and Medicine. (2025). *Cyber hard problems*. https://nap.nationalacademies.org/resource/29056/CyberHardProblems-2025.pdf

19. Networking and Information Technology Research and Development Subcommittee of the National Science and Technology Council. (2023, December). *Federal cybersecurity research and development strategic plan*. https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2023.pdf

20. Nobles, C. (2025, March). Exploring mitigative strategies to prevent burnout in cybersecurity. In *Proceedings of the 19th International Conference on Cyber Warfare and Security*. https://doi.org/10.34190/iccws.20.1.3347

21. Pattnaik, N., Nurse, J. R., Turner, S., Mott, G., MacColl, J., Huesch, P., & Sullivan, J. (2023, July). It's more than just money: The real-world harms from ransomware attacks. In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 261-274). https://doi.org/10.1007/978-3-031-38530-8_21

22. Peters, J. (2023, November). *Human error is responsible for 74% of data breaches*. Infosec Institute. https://www.infosecinstitute.com/resources/security-awareness/human-error-responsible-data-breaches/

23. Rangarajan, A., Haney, J., Canham, M., Elkins, M., Flynn, L., Gordin, M., Granova, V., Huang, W., Jacobs, J., Moody, G., Ross, M., Thomson, R., & Uchill, J. (2026). Advancing human-centered cybersecurity: Challenges and pathways forward. IEEE Security & Privacy, 24(3), 81-87. https://doi.ieeecomputersociety.org/10.1109/MSEC.2026.3676927

24. Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE open, 11*(1), 21582440211000049. https://doi.org/10.1177/21582440211000049

25. Symposium on Usable Privacy and Security. (2025). *Twenty-First Symposium on Usable Privacy and Security*. https://www.usenix.org/conference/soups2025

26. Tambe-Jagtap, S. N. (2023). Human-centric cybersecurity: Understanding and mitigating the role of human error in cyber incidents. *SHIFRA*, 2023, 53-59. https://doi.org/10.70470/SHIFRA/2023/007

27. USENIX. (2026). *USENIX Security Symposium*. https://www.usenix.org/conferences/byname/108

28. Venables, P. (2022). *Human error. Risk & Cybersecurity Thoughts from the Field*. https://www.philvenables.com/post/human-error

29. Verizon. (2025). *2025 Data breach investigations report*. https://www.verizon.com/business/resources/reports/dbir/

30. Von Preuschen, A., Schuhmacher, M. C., & Zimmermann, V. (2024). Beyond fear and frustration: Towards a holistic understanding of emotions in cybersecurity. In *Proceedings of the Twentieth Symposium on Usable Privacy and Security (SOUPS 2024*) (pp. 623-642). https://www.usenix.org/system/files/soups2024-von-preuschen.pdf

31. Walter, E. (2022). After the Crisis Comes the Blow – *The mental impact of ransomware attacks*. Northwave Cyber Security. https://northwave-cybersecurity.com/hubfs/ENG%20Whitepaper%20-%20Mental%20Impact%20Online.pdf

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

CONTACT US:

https://csrc.nist.gov/projects/human-centered-cybersecurity

human-cybersec@nist.gov