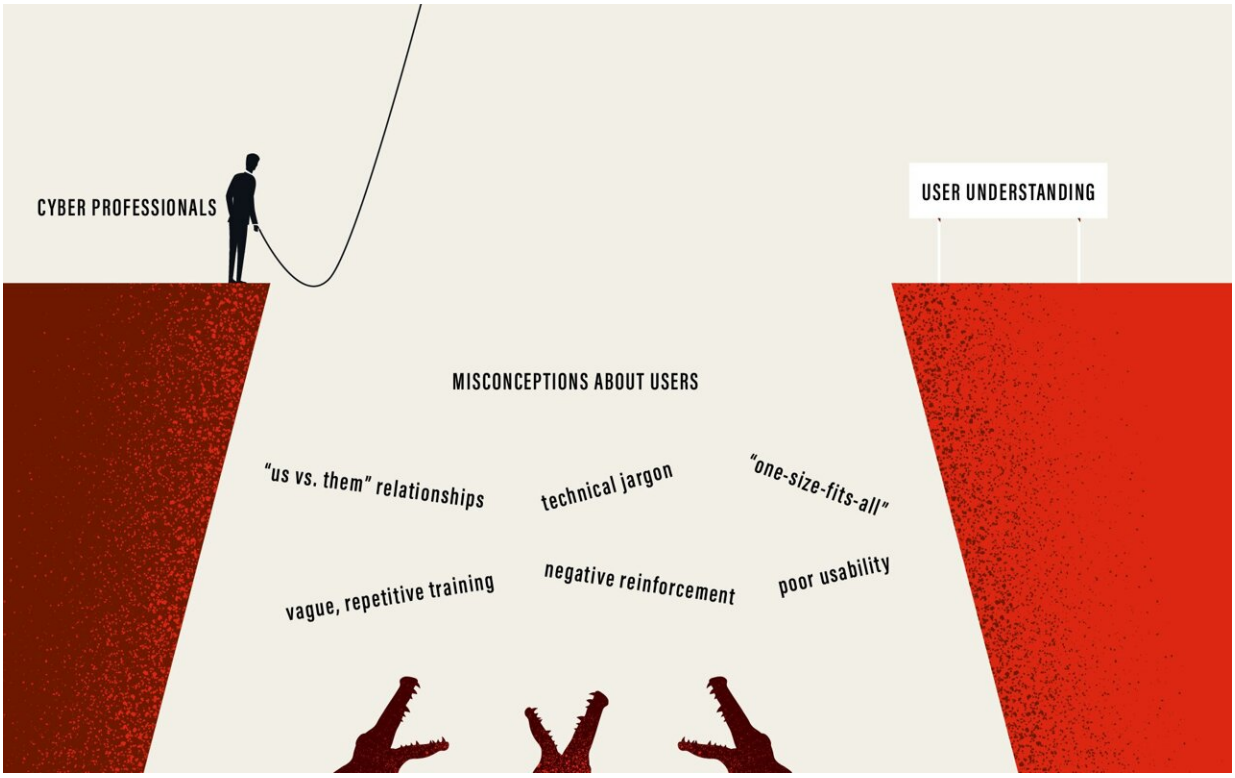
Is your cybersecurity strategy falling victim to these six common pitfalls?

March 21 2023



NIST research reveals misconceptions that can affect security professionals — and offers solutions. Credit: B. Hayes/NIST

Here's a pop quiz for cybersecurity pros: Does your security team consider your organization's employees to be your allies or your enemies? Do they think employees are the weakest link in the security

chain? Let's put that last one more broadly and bluntly: Does your team assume users are clueless?

Your answers to those questions may vary, but a recent article by National Institute of Standards and Technology (NIST) computer scientist Julie Haney highlights a pervasive problem within the world of computer security: Many security specialists harbor misconceptions about lay users of information technology, and these misconceptions can increase an organization's risk of cybersecurity breaches. These issues include ineffective communications to lay users and inadequately incorporating user feedback on security system usability.

"Cybersecurity specialists are skilled, dedicated professionals who perform a tremendous service in protecting us from cyber threats," Haney said. "But despite having the noblest of intentions, their community's heavy dependence on technology to solve security problems can discourage them from adequately considering the human element, which plays a major role in effective, usable security."

The human element refers to the individual and social factors impacting users' security adoption, including their perceptions of security tools. A security tool or approach may be powerful in principle, but if users perceive it to be a hindrance and try to circumvent it, risk levels can increase. A recent report estimated that 82% of 2021 breaches involved the human element, and in 2020, 53% of U.S. government cyber incidents resulted from employees violating acceptable usage policies or succumbing to email attacks.

Haney, who has a comparatively unusual combination of expertise in both cybersecurity and human-centered computing, wrote her new paper, "Users Are Not Stupid: Six Cyber Security Pitfalls Overturned," to help the security and user communities become allies in mitigating cyber risks.

"We need an attitude shift in cybersecurity," Haney said. "We're talking to users in a language they don't really understand, burdening them and belittling them, but still expecting them to be stellar security practitioners. That approach doesn't set them up for success. Instead of seeing people as obstructionists, we need to empower them and recognize them as partners in cybersecurity."

The paper details six pitfalls that threaten security professionals, together with potential solutions:

1. Assuming users are clueless. Though people do make mistakes, belittling users can result in an unhealthy "us vs. them" relationship between users and cybersecurity professionals. Research on nonexperts reveals that users are simply overwhelmed, often suffering from security fatigue. A potential solution involves building positive relationships with users while empowering them to be active, capable partners in cybersecurity.
2. Not tailoring communications to the audience. Security pros often use technical jargon that reduces audience engagement, and they may fail to tailor lessons in ways that appeal to what users care about in their daily lives. Several strategies can help, from focusing on plain-language messages to presenting information in multiple formats to enlisting the help of an organization's public affairs office.
3. Unintentionally creating insider threats due to poor usability. Users who are already pushed to their limit by time pressures or other distractions can unwittingly become threats themselves, as they become prone to poor decision making. (As one example, complex password policies can inspire poor decisions, such as using the same password across multiple accounts.) Offloading the user's security burden can help, such as by exploring whether more mail filtering can be done by the server so that fewer phishing emails get through. Also, when piloting new security

solutions, testing the approach first with a small group of users can reveal potential confusion that can be corrected before a wider rollout.

4. Having too much security. "Too much" implies that a security solution may be too rigid or restrictive for the specific job context. While always using the most secure tools available sounds wise in principle, some users can find the resulting complexity stifling for daily work, leading them to violate security policies more frequently. Instead of a "one size fits all" stance, performing a risk assessment using a risk management framework can help determine what level of cybersecurity best fits a given environment.
5. Depending on punitive measures or negative messaging to get users to comply. Negative reinforcement is common within organizations today: Examples include disabling user accounts if security training is not completed and publicly shaming individuals who cause cybersecurity incidents. Whether or not these measures work in the short term, they breed resentment toward security in the long term. Instead, offering positive incentives for employees who respond to threats appropriately can improve attitudes toward security, as can taking a collaborative approach with struggling users.
6. Not considering user-centered measures of effectiveness. As employees often find security training to be a boring, check-the-box activity, how much of it are they actually retaining? Without direct user feedback and concrete indicators of behavior, organizations can struggle to answer that question. It helps to think of concrete metrics as symptom identifiers—such as help desk calls that reveal users' pain points and incidents like phishing clicks that can show where users need more support. After identifying the symptoms, security teams can use surveys, focus groups or other direct interactions with users to determine the root cause of problems, as well as improve their solutions.

Haney stressed that not all security professionals have these misconceptions; there are certainly security teams and organizations making positive progress in recognizing and addressing the human element of security. However, these misconceptions remain prevalent within the community.

Haney said that though the issue with neglecting the human element has been well known for years—her paper cites evidence from industry surveys, government publications and usable security research publications, as well as her research group's original work—there is a gap between research findings and practice.

"There has been a lot of research into this issue, but the research is not getting into the hands of people who can do something about it. They don't know it exists," she said. "Working at NIST, where we have a connection to all sorts of IT experts, I saw the possibility of bridging that gap. I hope it gets into their hands."

More information: Users are not stupid: Six cyber security pitfalls overturned. csrc.nist.gov/csrc/media/Proje … s_are_not_stupid.pdf

This story is republished courtesy of NIST. Read the original story here.

Provided by National Institute of Standards and Technology

Citation: Is your cybersecurity strategy falling victim to these six common pitfalls? (2023, March 21) retrieved 20 April 2024 from https://techxplore.com/news/2023-03-cybersecurity-strategy-falling-victim-common.html