



2023 Hidden Threats

How workforce demographics
impact your security posture

Part of Ivanti's Cybersecurity Status Report Series



Digging into Demographics

Top-down, one-size-fits-all enterprise security ignores the unique risks that accompany geography, age, gender and role, among other factors.

In this latest report from Ivanti, we peel back big-picture averages — investigating everything from risky employee behaviors (the laxest employees aren't who you think they are) to inconsistencies in security culture.

Ivanti surveyed 6,500 executive leaders, cybersecurity professionals and office workers across the globe to understand:

Employees' attitudes toward cybersecurity and their perceived role in defending organizations

Security professionals' diagnoses of key challenges and vulnerabilities

Leaders' tech behaviors, as well as their level of buy-in to cybersecurity strategy



One in three employees believes their actions have no impact on enterprise security.

Inside:

01

Generation Myths:

Are younger users “better” about security?

02

Incident Impacts:

Incident reporting trends by seniority, gender and region

03

Regional Training:

Geographic differences in training and security attitudes

04

Take Action:

How to address end user demographics in your security strategy

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as “Ivanti”) and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document, nor does it make a commitment to update the information contained herein. For the most current product information, please visit [ivanti.com](https://www.ivanti.com)

Methodology

Ivanti surveyed over 6,500 executive leaders, cybersecurity professionals and office workers in Q4-2022 to understand today's risks and discover how organizations are preparing for yet-unknown future threats.

In this report, we focus on how specific demographics of organization end users impact their personal attitudes and behaviors — and how these variations may present advanced risks that threat actors can exploit.

Survey demographics:

5,202

Office workers

Office Workers ages ≤40: 3,609

Office Workers ages >40: 2,769

902

Security professionals

454

Leadership executives

3,414

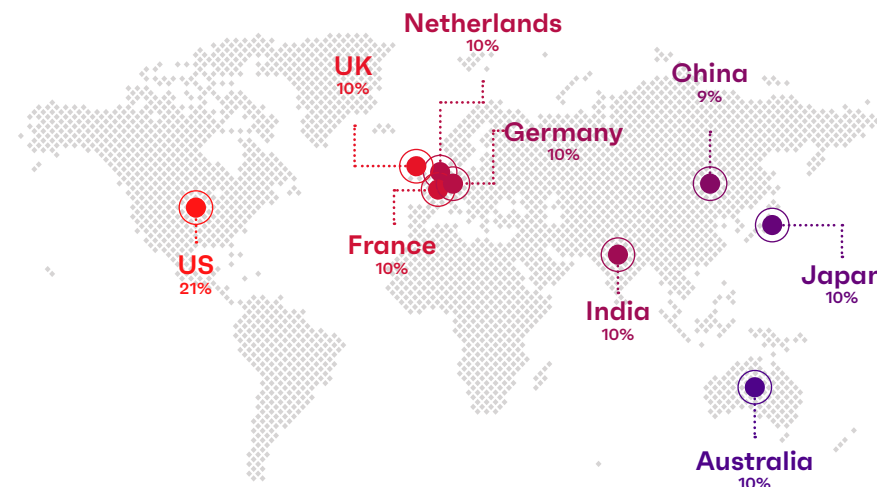
Female

3,119

Male

27

Non-binary / prefer not to answer



Generation Myths:

Are younger users “better” about security?



Problem Today

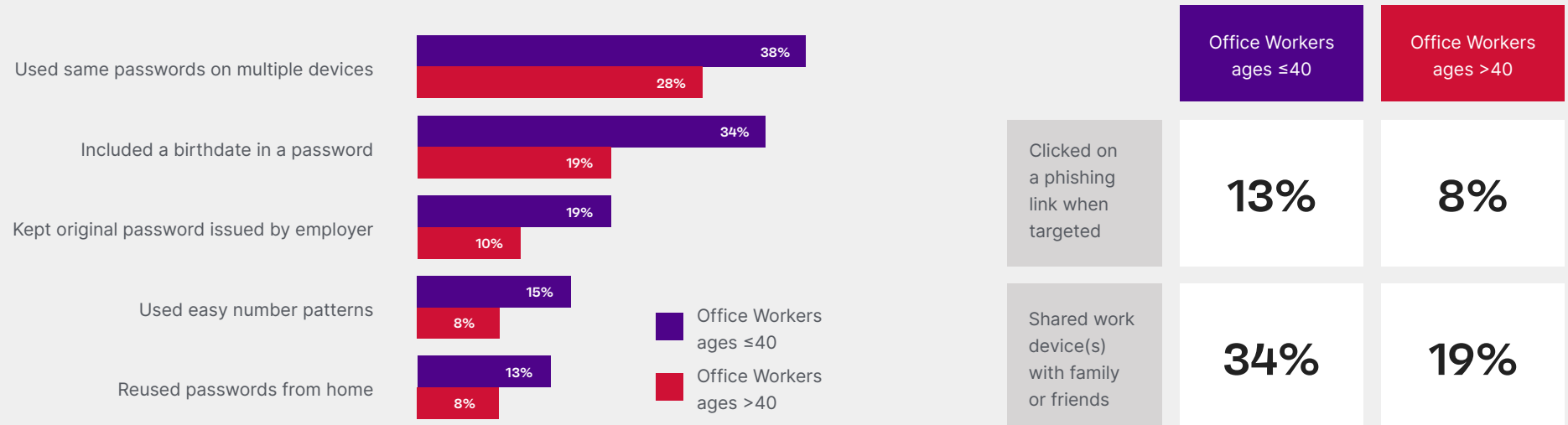
Many assume older employees are less tech savvy — and therefore more likely to engage in risky behaviors. In fact, the opposite is true.

Younger professionals (those under 40) are significantly more likely to disregard important security guidelines, when compared to Gen X and older. This is true about performing password hygiene, clicking on phishing links and sharing devices with family and friends.

Younger office workers are more likely to have unsafe security habits

Q:

When you're asked to create a login password at work, which of these things have you done within the last two years?





Why It Matters

These oversights, lapses and shortcuts add up to significantly higher security vulnerabilities with younger employees.

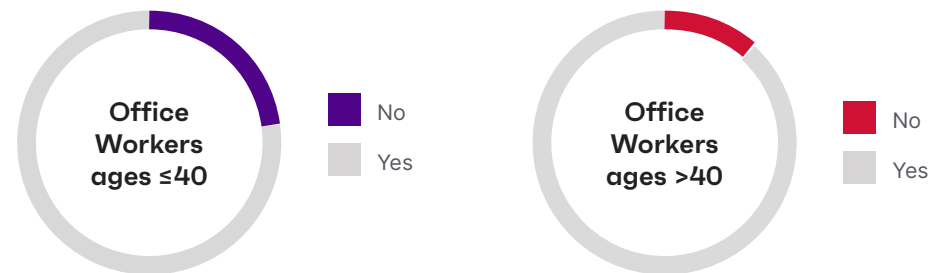
Stereotypes about age-based tech savviness may be leading organizations astray. And the problem is not only related to cyber hygiene (e.g., password habits, sharing devices); the research shows younger professionals are also less likely to report red flags when they encounter them.

Among those workers 40 and under, 23% said they did *not* report the last phishing email or message they received, compared to 12% of those over 40 who also failed to report.

The most common reason for not reporting?

"I didn't think reporting was important."

Office workers who did NOT report their last phishing message to security



2023 Hidden Threats

6

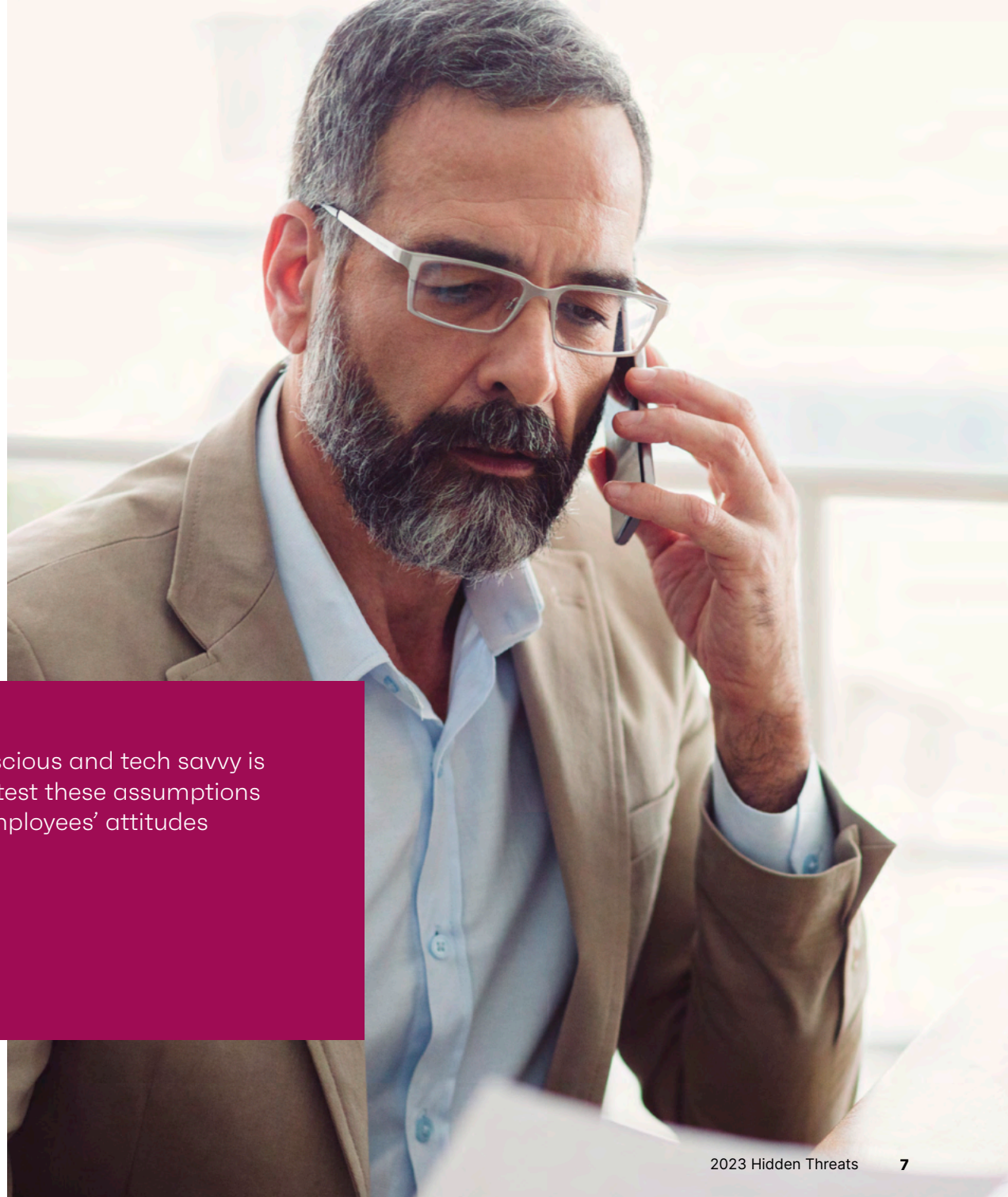
Stereotypes about older workers are particularly insidious because tech workers skew younger — and so may be more likely to believe their older colleagues are uninformed or vulnerable.

For example, a study of 2,250 professionals in the UK found tech workers viewed colleagues as “over the hill” and “too old for their job” when they reached 38 years old.¹

(Keep in mind, this is in relation to their tech industry peers, not average employees, who are less likely to be tech savvy.)

These findings underscore why organizations need to rely less on employees’ individual judgment, and more on tech interventions that make rule-following effortless.

Even better: organizations should consider deploying automations that run behind the scenes entirely, such that your end users aren’t even aware they exist.



“Assuming that younger employees are more security-conscious and tech savvy is outdated and even dangerous. Organizations should road test these assumptions by conducting internal research that captures their own employees’ attitudes about security risk and their part managing it.”

Daniel Spicer
Chief Security Officer at Ivanti

Incident Impacts:

Incident reporting trends by seniority,
gender and region



Problem Today

Keeping an organization safe means getting near-real-time information about security incidents or breaches. Our research shows some employees are less inclined to report red flags.

Will your employees get in touch quickly if they have a security concern? Ivanti's research shows specific segments of your employee base may hesitate to reach out — something organizations should be aware of as they develop outreach and training programs.

Seniority

The biggest swing variable in reporting is seniority. Seventy-two percent of leaders we surveyed say they've contacted a cybersecurity employee with a question or concern, compared to just 28% of office workers.

Gender

Women are less likely than men to do the same. Twenty-eight percent have contacted a cybersecurity employee with a question or concern, compared to 36% of men.



Did you know?

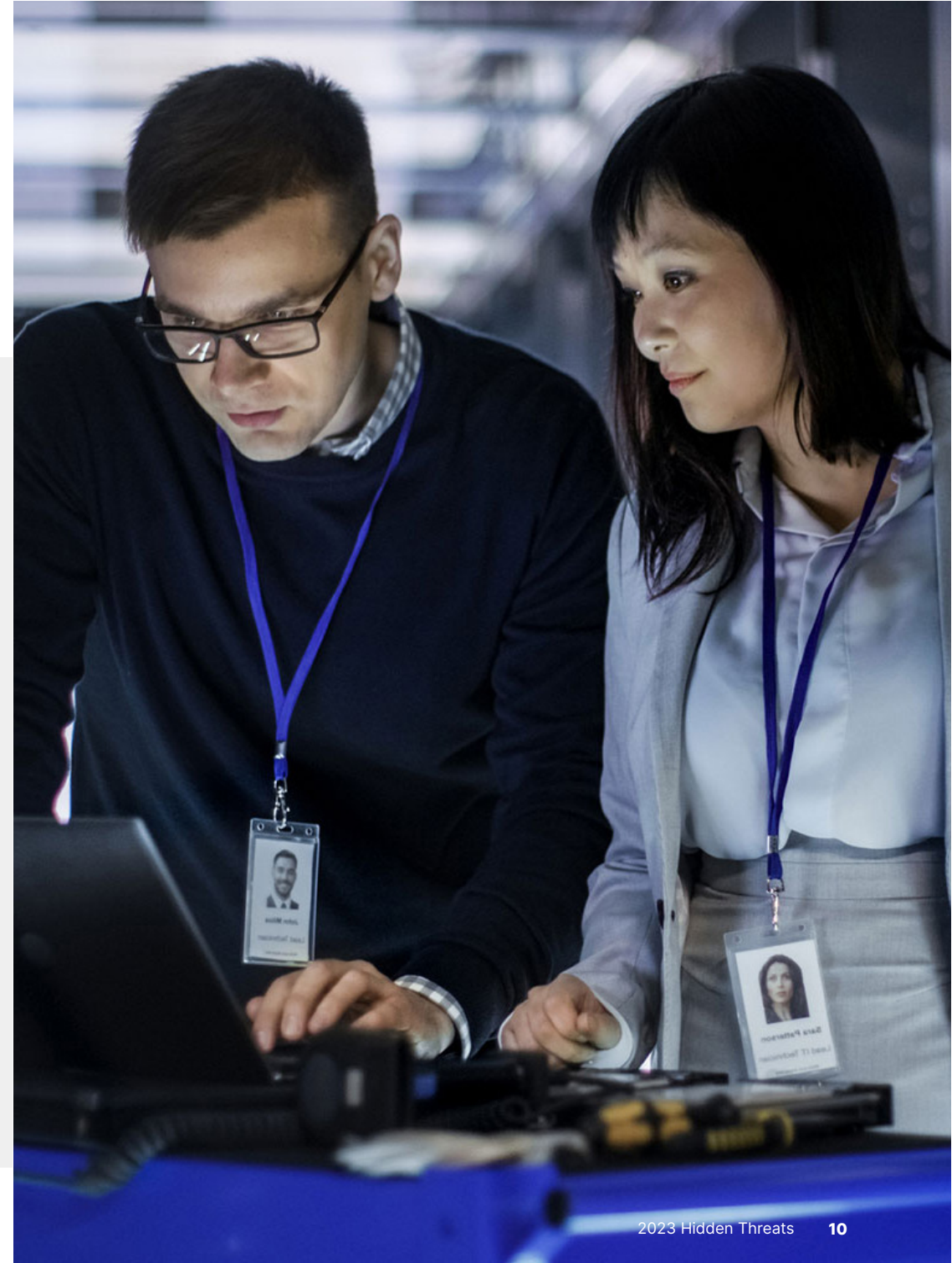
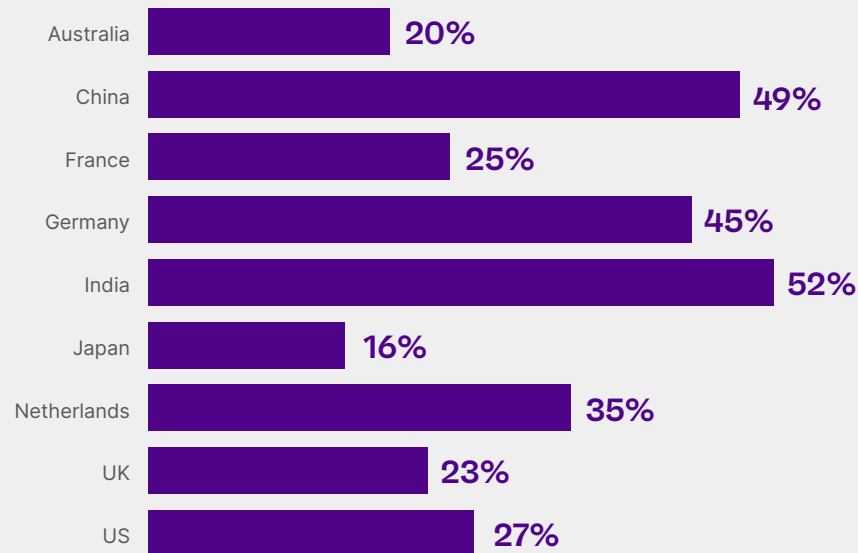
Executives are twice as likely to report security interactions as "awkward" or "embarrassing" than office workers.²

These more frequent, yet negative security interactions may accelerate executives' use of external, non-approved tech support — reportedly at four times the rate of office workers.

User willingness to contact security varies greatly by country.

For example, nearly half of office workers in China have contacted the security team with a question or concern, compared to just 20% in Australia.

Office workers who contacted security with a question or concern, by region





Why It Matters

Your security position depends on thousands of employees playing defense. Do those employees understand that they're valuable members of the extended security team?

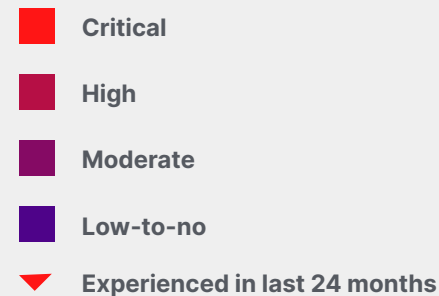
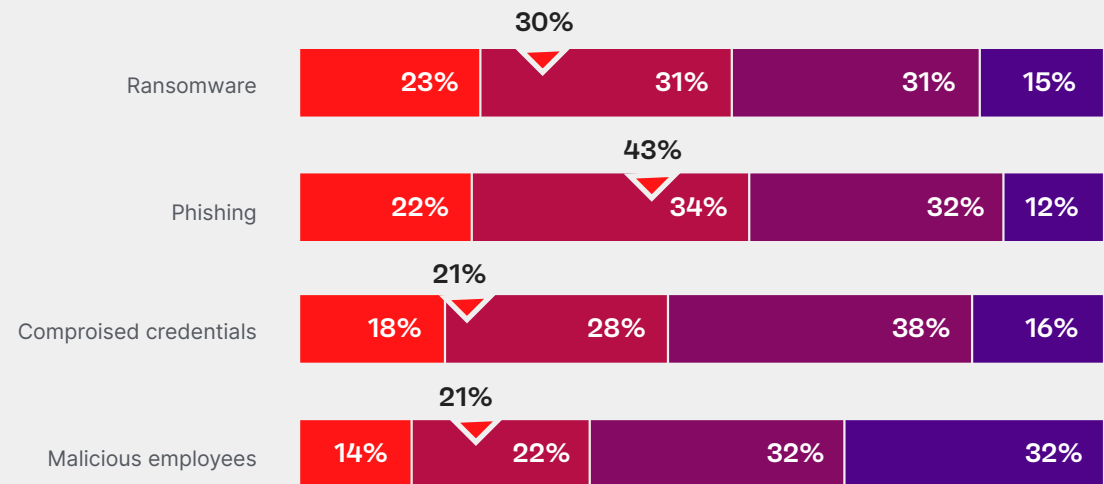
Ivanti's marquee security preparedness study asked security professionals about their biggest industry-wide vulnerabilities. Ransomware and phishing ranked No. 1 and No. 2.

And these threats are becoming more dangerous with each passing year — especially thanks to advances in generative AI, which make phishing harder to spot.

Top rated security threats and weaknesses offer an opportunity for employee defenders

Q:

Please rate the predicted 2023 threat level within your industry for each of the following...



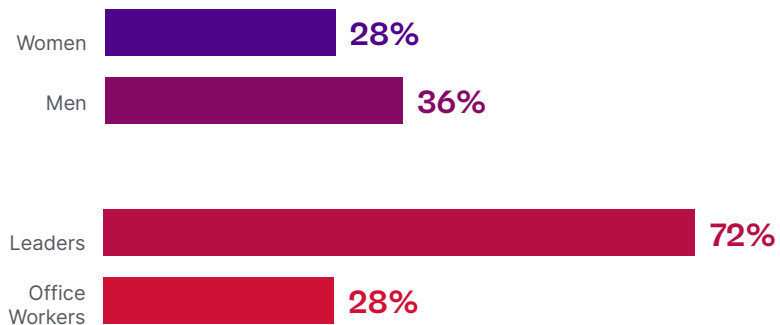
These accelerated threats and increased risks mean your employees need to feel comfortable approaching your security team — even if the only “proof” they have of an incoming attack is a nagging doubt.

(Some examples: an atypical wire transfer request, a suspicious invoice reminder, or an unsolicited password reset link.)

After all, during an active security incident, speed is the single most important factor in defending against an attack.

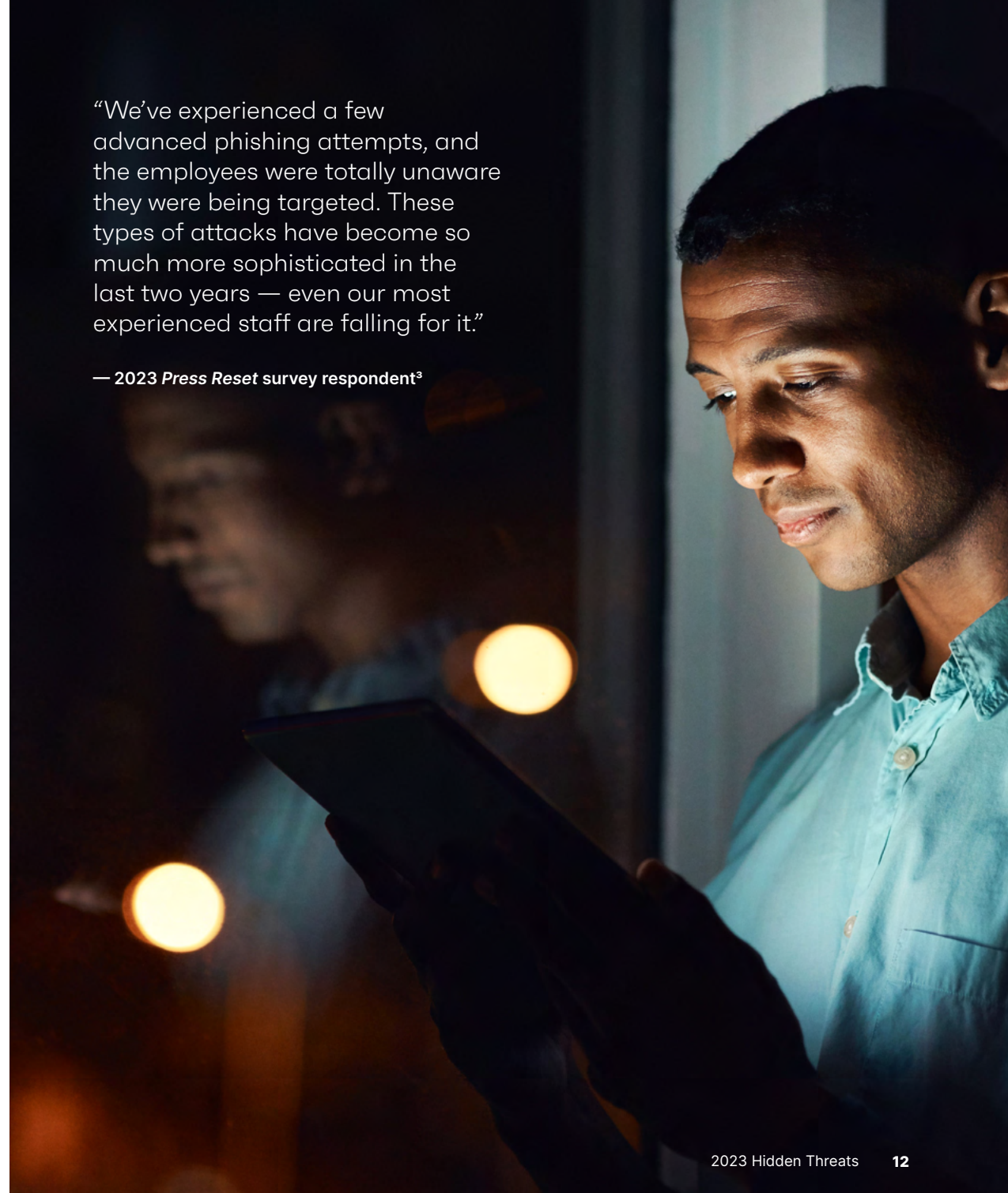
Ultimately, when employers conduct sentiment surveys to understand employee attitudes, they should drill down to investigate demographic patterns and vulnerabilities.

Users who have contacted a security employee with questions or concerns



“We’ve experienced a few advanced phishing attempts, and the employees were totally unaware they were being targeted. These types of attacks have become so much more sophisticated in the last two years — even our most experienced staff are falling for it.”

— 2023 *Press Reset* survey respondent³



Regional Training:

Geographic differences in training and security attitudes



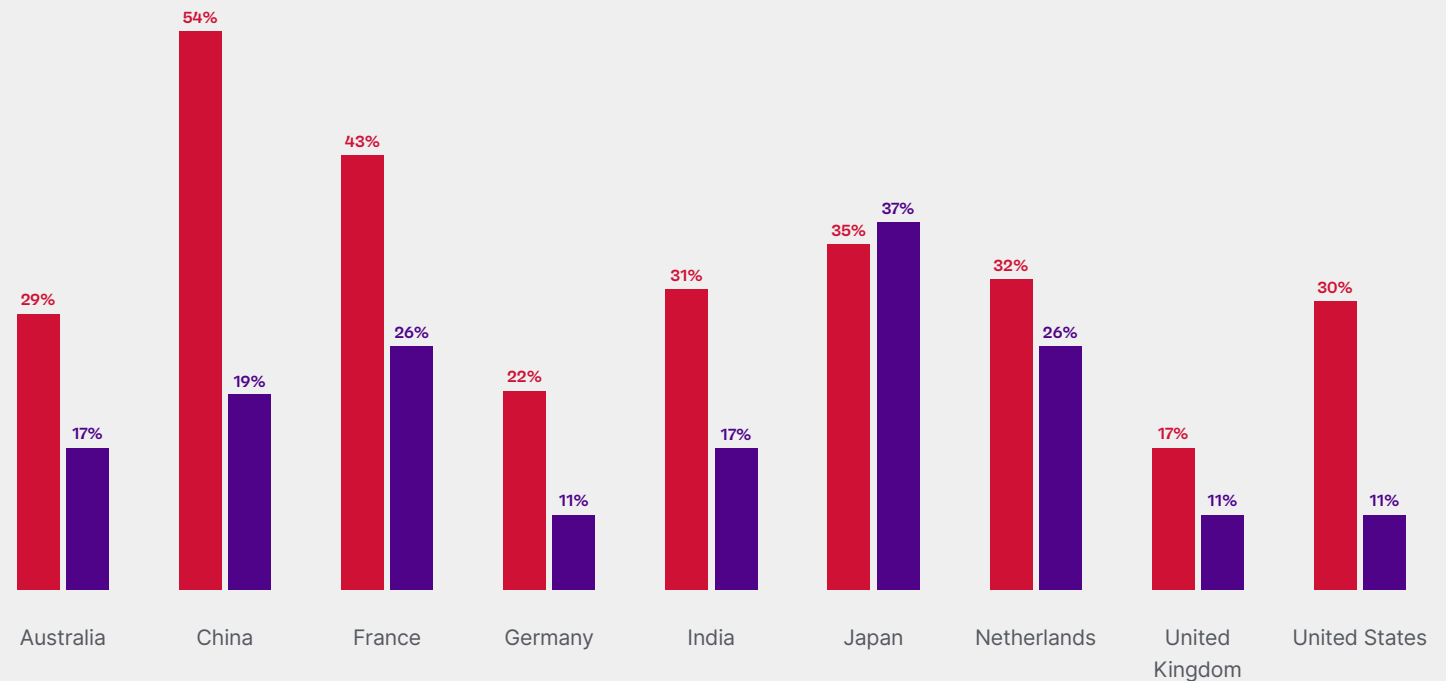
Problem Today

An organization's culture and training programs have a significant influence on security preparedness, but our research shows both are inconsistent at the country level.

Ivanti's research shows important differences in security culture at the country level — both in terms of training provided by the organization and in terms of attitudes at the leader and office-work levels.

Regional variations in cybersecurity training and attitudes

- "My organization does NOT provide mandatory cybersecurity training."
- "No, I would not feel safe [reporting a mistake to the security team.]"





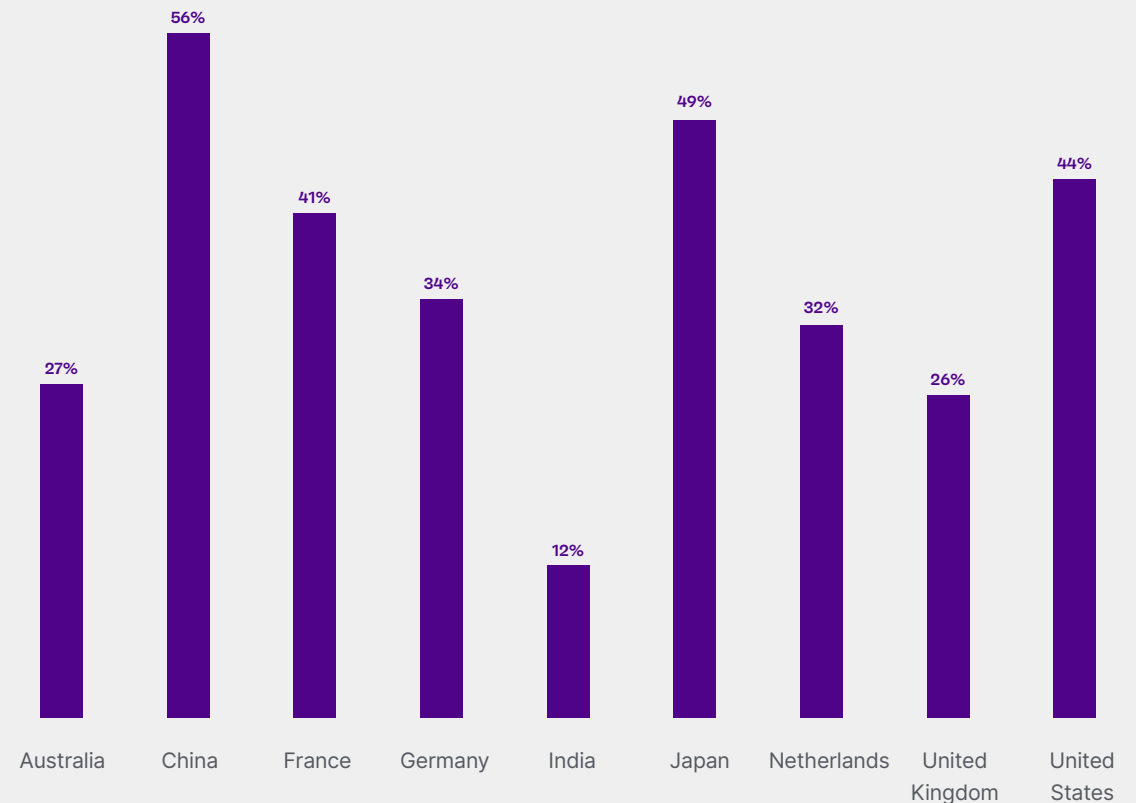
Why It Matters

Many organizations have a top-down approach to training and security culture, but the research shows it's critical to understand local security culture — and even local culture — to put together a coherent plan.

No matter where they're from, every new hire introduces their own unique vulnerabilities to the organization, intentionally or not. Undertrained employees risk diluting the strength of the overall organization's preparedness.

To minimize this risk, organizations must invest in strong onboarding and ongoing security training programs at global and regional levels.

Office Workers: "My actions do NOT impact my organization's ability to stay safe [from cyber threats]."



How local culture interacts with global security programs

Culture can influence how organizations defend their assets and people, as well as how they respond to an attack.


Possible cultural security challenges

Employee discomfort with global-level training (e.g., poor translation of teaching materials into local language and culture).

Employee unease with new standards or rules that have not been “socialized” at the local level.

A top-down local office culture that leaves little room for individuals to report errors or concerns.

Substandard security support for local offices; for example, employees who have questions or concerns must contact a security team member in a different country — and endure language and cultural barriers.



“These country-level differences are an interesting lens through which to study preparedness.

“It’s easy — and common — for a security team to judge security based on what’s taking place in their largest or nearest office.

“This research shows how important it is to explore more granular data and uncover security procedures at every location — whether at headquarters, R&D facilities, supply chain outposts or manufacturing locations.”

Daren Goeson
SVP, Product Management at Ivanti

Take Action:

How to address end user demographics in your security strategy



Take Action

Big-picture excellence can hide pockets of risk.

Let's explore the security risks related to demographics in detail — drilling down to how you can assess the demographic risks at your specific organization, as well as how you can adjust your approach to properly remediate.

5 ways to remediate your hidden risks

1

Survey your employees.

See how your users' security attitudes and behaviors compare against these global benchmarks.

2

Challenge your stereotypes.

Examine the potential assumptions and biases which your security team itself may hold.

3

Localize your materials.

Push past basic translation, so your training and policies don't run into regional misinterpretations.

4

Redesign your backend.

Eliminate employee involvement wherever you can to increase automatic compliance.

5

Rebuild your culture.

Increase employee trust and confidence in your security team's responses, increasing overall organizational security.

Hidden Risk Remediation #1:

Survey your employees to uncover your organization's unique demographic habits.

Use an anonymous survey to surface insights about your employee base, paying close attention to potential demographic differences. (Are there unexpected findings? Answer patterns that counter your initial assumptions?)

Use the findings to step up your training and outreach efforts — matching solutions to the segments of your employee base that need additional support

Sample questions for an anonymous study of employee attitudes

Can you identify a phishing attempt?

Have you been given resources and/or tools to identify a phishing attempt?

Do you feel comfortable asking the security team a question?

Do you feel safe reporting an error to the security team?

Do you think your actions have an impact on the organization's security?

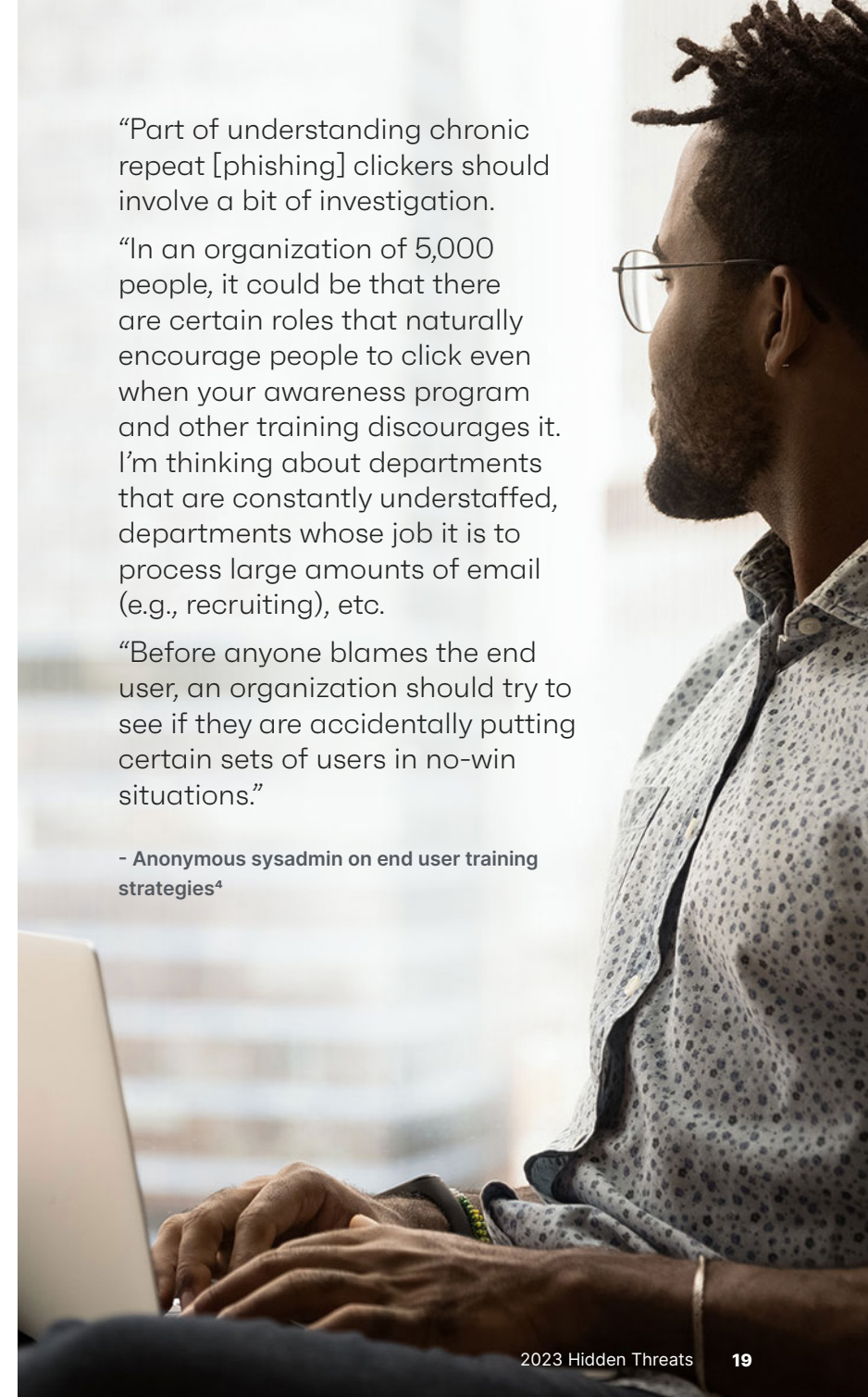


“Part of understanding chronic repeat [phishing] clickers should involve a bit of investigation.

“In an organization of 5,000 people, it could be that there are certain roles that naturally encourage people to click even when your awareness program and other training discourages it. I’m thinking about departments that are constantly understaffed, departments whose job it is to process large amounts of email (e.g., recruiting), etc.

“Before anyone blames the end user, an organization should try to see if they are accidentally putting certain sets of users in no-win situations.”

- Anonymous sysadmin on end user training strategies⁴



Hidden Risk Remediation #2:

Challenge stereotypes about user digital savviness and safety.

Have your security team complete an anonymous survey that examines their assumptions about different employee groups. Then, compare those results to your general employee survey findings to shed light on assumptions that are not only unfair but untrue — and on how those stereotypes might impact your security posture.

3 human-based vulnerabilities impacting security professionals

Satisficing

A specific decision-making process that strives for a minimum viable outcome, rather than dedicating full effort for the best possible outcome.⁵

While focusing through this process can help resource-strapped teams, what a team decides to abandon as “not important enough” for basic implementation can be influenced or shift altogether when other perspectives are considered.

Probability neglect

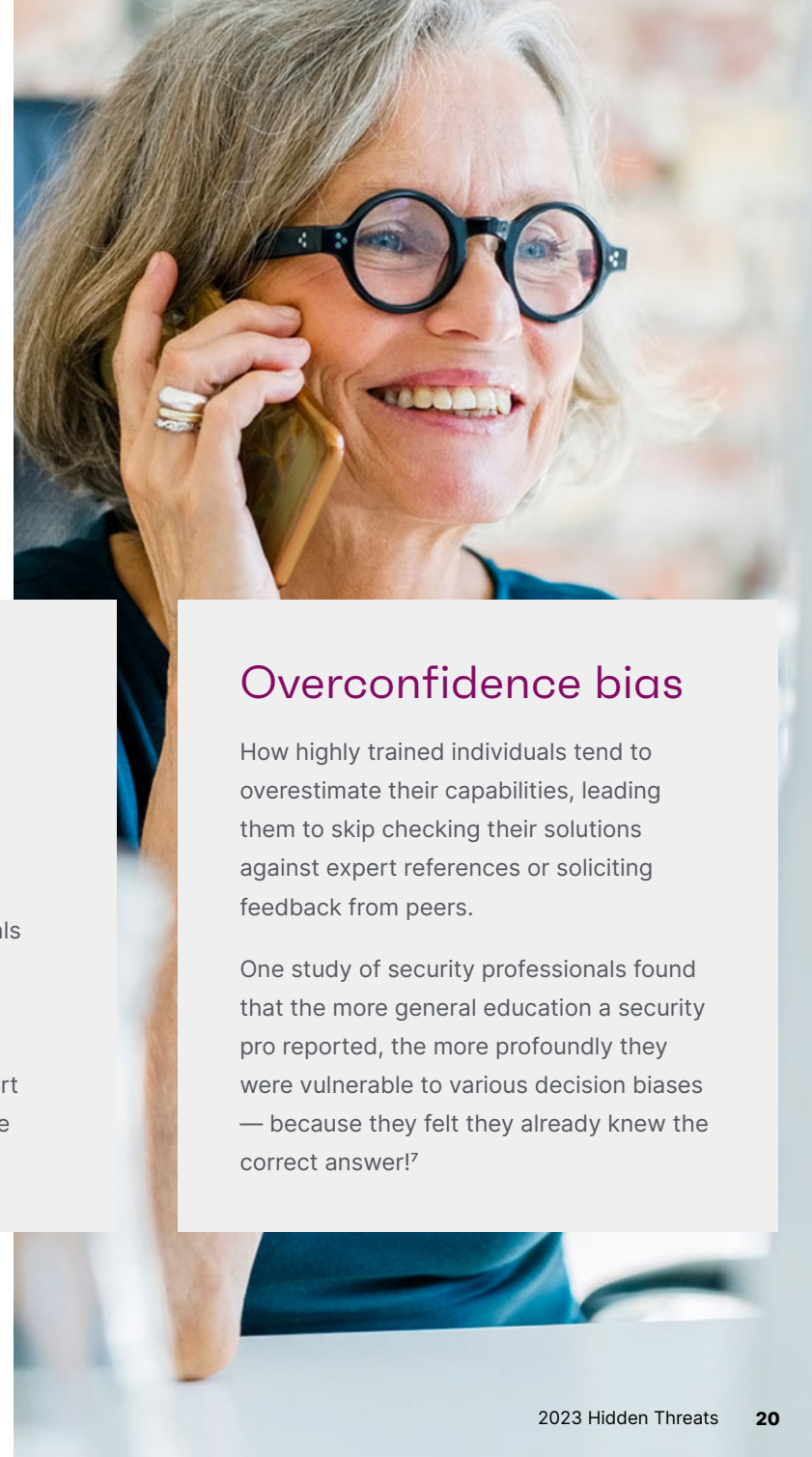
How people often don’t consider the likelihood of an event occurring when its impact is great — especially if high emotions are involved.

Studies show that security professionals are often more tempted to prioritize and remediate unlikely but highly damaging events, even if smaller risks — such as an end user’s failure to report a possible security incident — are more statistically likely.⁶

Overconfidence bias

How highly trained individuals tend to overestimate their capabilities, leading them to skip checking their solutions against expert references or soliciting feedback from peers.

One study of security professionals found that the more general education a security pro reported, the more profoundly they were vulnerable to various decision biases — because they felt they already knew the correct answer!⁷



Hidden Risk Remediation #3:

Understand how your global security culture is translated and localized.

For a cross-department program like your security training and policies, just translating materials into the correct language isn't enough. You must "localize" your security materials, so that its core meaning overcomes any potential confusing cultural hurdles.

So, proactively consult with your local and regional teams, soliciting their input and buy-in for the new materials prior to translation.

And remember: local leaders can be powerful evangelists! They can naturally share your security message in a way that other regional employees will naturally understand, trust and follow

Localization checks for security programs and communications

Color

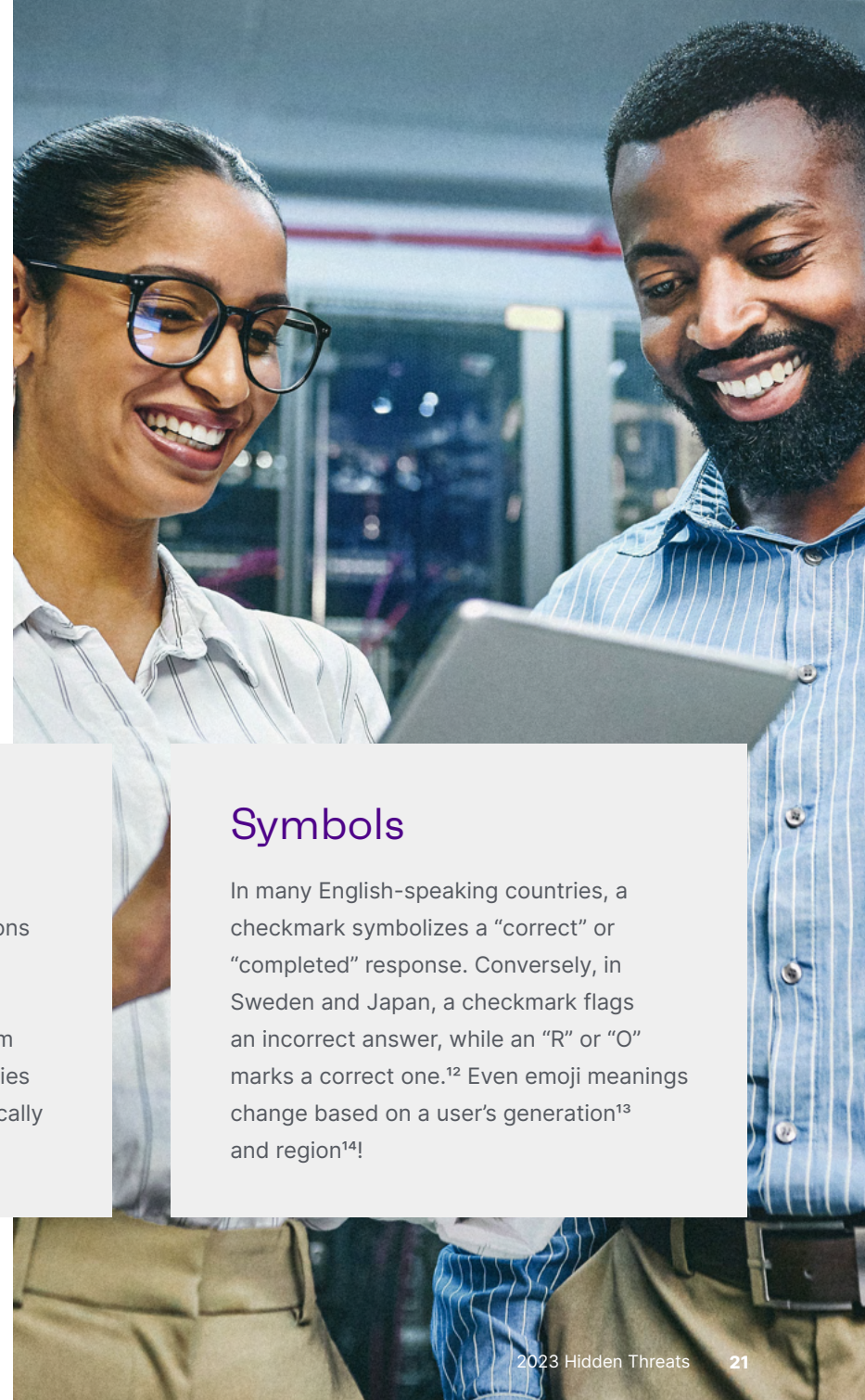
Chinese users may see red-flagged items as lucky and positive — not immediately realizing the Western home office means "stop." Green may trigger negative reactions in Indonesian and South American users, who associate green with infidelity and death, respectively.⁸

Sports

One study of English-Arabic / Arabic-English materials found basic translations had "inappropriate" translation substitutions for sports idioms 37% of the time.⁹ Other studies on sports idiom translations have found similar difficulties for Polish¹⁰, Persian / Farsi¹¹, and practically every other language.

Symbols

In many English-speaking countries, a checkmark symbolizes a "correct" or "completed" response. Conversely, in Sweden and Japan, a checkmark flags an incorrect answer, while an "R" or "O" marks a correct one.¹² Even emoji meanings change based on a user's generation¹³ and region¹⁴!



Hidden Risk Remediation #4:

Design your tech stack to minimize pockets of user nonconformity and inconsistency.

Rather than relying on individual users to conform to security protocols, build stronger back-end automation that is effectively hidden from end users — interventions that make compliance frictionless.

3 common security upgrades that decrease end user friction

Just-in-time security updates

Most employees don't relish shutting down their computers and rebooting for updates. So, they tend to postpone the process indefinitely — or simply forget to restart altogether!

Instead, use a system that automatically forces a restart within a given time frame, but permits a user to schedule that restart outside of their working hours, encouraging timely-yet-convenient updates.

Modern password policies

Recently, many global cybersecurity frameworks have quietly eliminated the older recommendation to rotate passwords if there's no evidence of a user's secret exposure.¹⁵ Rather than increasing security, password expiration policies tend to promote poor password hygiene, as users struggled to come up with — and remember! — net-new passphrases or PINs.¹⁶

Instead, consider deploying password managers, single sign-on policies, or deploying passwordless technologies — no user memory or sticky notes required.

Silent acceptable use policies (AUP) — with built-in enforcement

While your employee onboarding may feature a review of your organization's AUP, policies without enforcement aren't worth the paper they're printed on.

Configure your entire digital infrastructure for specific user profiles and access permissions — with an easy way for users to request advanced access if the basic permissions are insufficient for their unique workload.³

Hidden Risk Remediation #5:

Proactively build an open and welcoming security culture.

The findings of this *Hidden Threats* report underscore the need for a collaborative and positive security culture at every organization. Ultimately, employees should not hesitate to contact security professionals — no matter how small the question or potentially foolish the mistake.

Only in non-punitive security cultures can security teams receive enough cooperation from their users to properly protect the entire organization.

4 key tenets of a strong security culture

Open

Employees feel safe reporting an incident, and are rewarded for their honesty and transparency. They feel comfortable approaching the security team no matter how trivial their question is.

Designed

Employee behavior is sharpened by tech-driven behavioral interventions. These technologies should be designed so well that they vastly reduce shadow IT workarounds and general non-compliance.

Iterative

The organization provides frequent, iterative training that's compelling to employees — from formal training workshops and regular organization-wide communications, to gamified security contests featuring real security scenarios.

Integrated

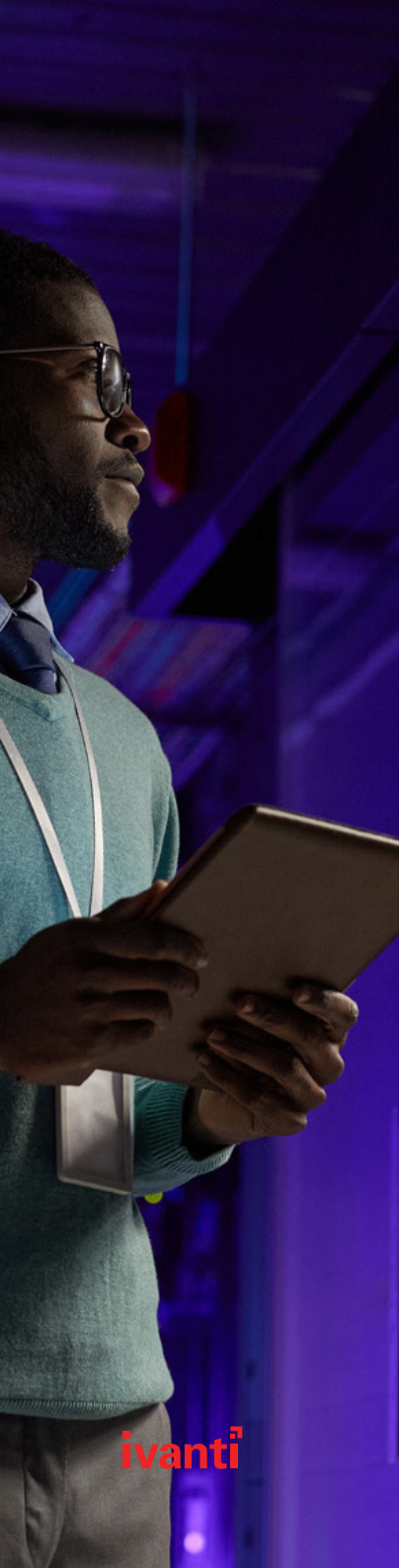
The responsibility for organizational security is shared by all, and your employees are invested in keeping the organization safe.

“Repeat clickers [on security training tests] aren't really the problem. Or, more accurately, they're a relatively predictable problem.

“If you know someone has a hard time detecting deception, they need guardrails — not punitive measures or more ineffective training.”

- Anonymous system administrator on security training solutions¹⁷





References

1. Sevilla, C. (2022, May 23). Everyday ageism in the tech industry. From CWJobs: <https://www.cwjobs.co.uk/advice/ageism-in-tech>
2. Ivanti. (2023, August 29). 2023 Executive Security Spotlight: New research from Ivanti shows real risks facing the C-suite. From Ivanti: <https://www.ivanti.com/resources/v/doc/ivi/2773/17cca519291d>
3. Ivanti. (2023, December 12). Press Reset: A 2023 Cybersecurity Status Report. From Ivanti: <https://www.ivanti.com/resources/v/doc/ivi/2732/7b4205775465>
4. u/CyberAndFolkloreGuy. (2023, January 19). Security Awareness: How to properly address colleagues who repeated fail Phishing tests? From Reddit: <https://www.reddit.com/r/cybersecurity/comments/10g4688/comment/j55k4cn/>
5. Frankenfield, J. (2022, August 23). Satisficing: Definition, How the Strategy Works, and an Example. From Investopedia: <https://www.investopedia.com/terms/s/satisficing.asp>
6. De Wit, J. J., Pieters, W., & Van Gelder, P. H. (2022). Individual Preferences In Security Risk Decision Making: An Exploratory Study Under Security Professionals. WIT Transactions on The Built Environment, 187-199. doi:10.2495/SAFE210161
7. De Wit, J., Pieters, W., Jansen, S., & van Gelder, P. (2021). Biases in Security Risk Management: Do Security Professionals Follow Prospect Theory in Their Decisions? Journal of Integrated Security and Safety Science, 1(1), 34-57. doi:<https://doi.org/10.18757/jisss.2021.1.5700>
8. Eriksen Translations. (2020, February 3). How Translating Colors Across Cultures Can Help You Make a Positive Impact. From Erksen Translations: https://eriksen.com/marketing/color_culture/
9. Nasser, L., & Al-Aazzawi, K. (2022). Context Impact in Translating Sport Idiomatic Expressions from English into Arabic with Regard to Types of Idioms. Adab Al-Rafidayn Journal, 1-26. doi:10.33899/radab.2021.170415
10. Mazurkiewicz, M. (2014). Sports Vocabulary and Idioms – Some Observations About the Specificity of English-Polish and Polish-English Translation. Cultures and Literatures in Translation, 140-153. From https://www.academia.edu/40425597/Sports_Vocabulary_and_Idioms_Some_Observations_about_the_Specificity_of_English_Polish_and_Polish_English_Translation
11. Suzani, S. M. (2007). Sports Idioms and Duality of Meaning in Translation. Iranian Journal of Translation Studies. From <https://journal.translationstudies.ir/ts/article/view/126>



12. Grove, L. (1989). Signs of the times: graphics for international audiences. International Professional Communication Conference 'Communicating to the World', 137-141. doi:10.1109/IPCC.1989.102119
13. Brants, W., Sharif, B., & Serebrenik, A. (2019). Assessing the Meaning of Emojis for Emotional Awareness - A Pilot Study. Companion Proceedings of The 2019 World Wide Web Conference, 419-423. doi:<https://dl.acm.org/doi/abs/10.1145/3308560.3316550>
14. Gao, B., & VanderLaan, D. P. (2020). Cultural Influences on Perceptions of Emotions Depicted in Emojis. Cyberpsychology, Behavior, and Social Networking, 567-570. doi:<https://doi.org/10.1089/cyber.2020.0024>
15. National Institute of Standards and Technology (NIST). (2020, March 03). NIST Special Publication 800-63B. From <https://pages.nist.gov/800-63-3/sp800-63b.html#sec5>
16. Willson, K. R.-H. (2020, March 9). The Debate Around Password Rotation Policies. From SANS Institute: <https://www.sans.org/blog/the-debate-around-password-rotation-policies/>
17. u/securebxdesign. (2023, April). What does your policy/training look like for people who fail phishing campaigns? From Reddit: <https://www.reddit.com/r/cybersecurity/comments/13csxs0/comment/jjk37bo/>

2023 Hidden Threats

How workforce demographics impact your security posture

Ivanti's Cybersecurity Status Report Series



[ivanti.com](https://www.ivanti.com)

1 800 982 2130

sales@ivanti.com