ivanti

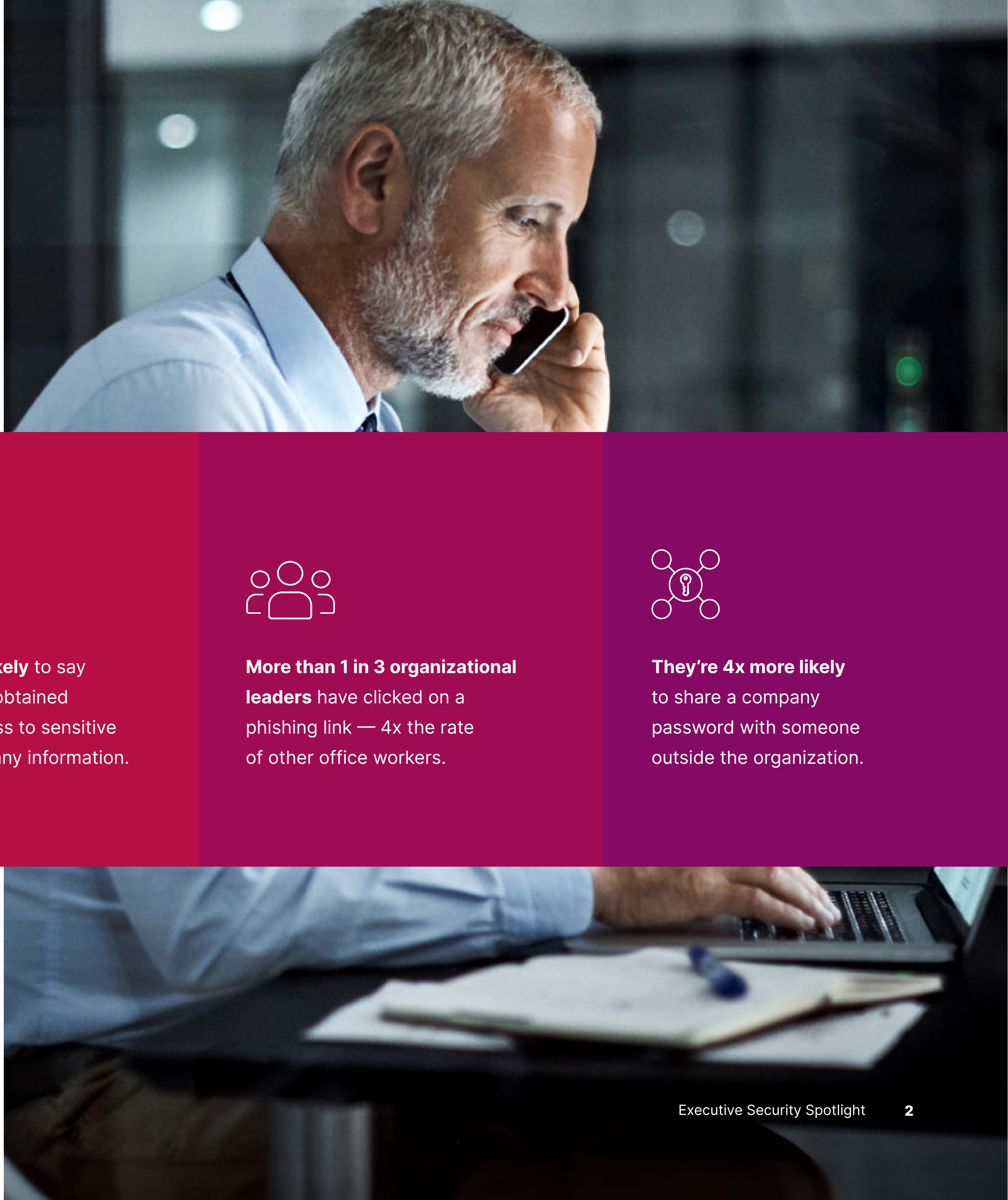
2023 Executive Security Spotlight

New research from Ivanti shows real risks facing the C-suite

Part of Ivanti's Cybersecurity Status Report Series

Shutting down executive cybersecurity threats

As a rule, organizations don't believe executive support blocks cybersecurity excellence. In our inaugural *Press Reset* report, only 21% of leaders and security professionals considered lack of executive buy-in as a security barrier — a full 16 points lower than the most significant blocker, tech stack complexity (37%).



Yet, leadership professionals are more likely to practice unsafe security behaviors than security teams may have previously realized.

They're 5x more likely to say they've purposely obtained unauthorized access to sensitive customer or company information.

More than 1 in 3 organizational leaders have clicked on a phishing link — 4x the rate of other office workers.

They're 4x more likely to share a company password with someone outside the organization.

How do you protect top executives — the most targeted group of employees — when they say they buy in to your organization's mandate, but frequently bypass security protocols?

ivanti

This report highlights:

The sizable gap between executives' stated priorities (e.g., buying into security policies) and their on-the-job actions.

How executives' security habits pose a substantially higher risk for cyberattacks and breaches than those of the general office population.

The current distrust between executives and the teams responsible for securing them — which may drive executives to external IT support, rather than request internal help.

Practical ways to secure your organization with quiet, behind-the-scenes implementations — all while you and your team restore the mutual trust needed to truly secure executive buy-in of your security program.

Security leaders already know that high-powered, high-access individuals present a unique security threat. Rather, Ivanti's newest research underscores the *scale* of the problem, and suggests those executive security exceptions lead to outsized organizational risks.

"It may be tempting to excuse executives from stringent cybersecurity measures due to their limited numbers, underestimating the potential threat they pose.

"However, recent research findings dispel such misconceptions. Executives exhibit distinct behaviors within the workplace, and enjoy unparalleled access and influence.

"This research unequivocally demonstrates the imperative need to address and rectify their habits and behaviors."

Giuliano Liguori,
CEO of Kenovy

Inside:

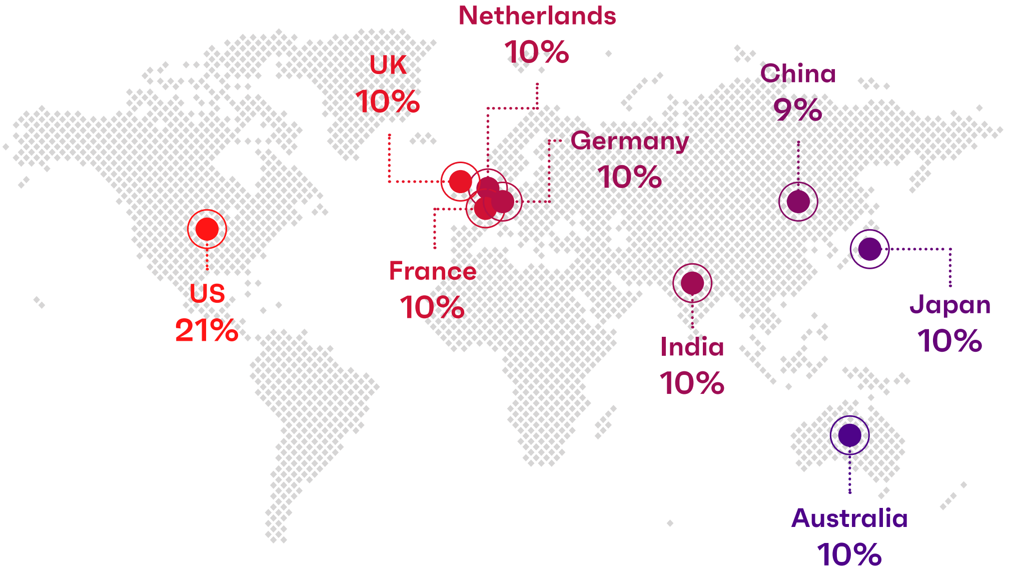
This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti") and may not be disclosed or copied without prior written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

Methodology

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

In this report, we focus on C-level executives — and the attitudes and behaviors that make them security dangers.



Office workers 5,202

Security professionals 902

Leadership executives 454

01

The Executive Conduct Gap:

The difference between what leaders say about security… and what they tend to do

ivanti

Problem Today

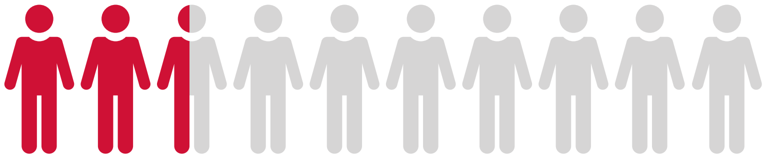
There’s a wide gap between what executives say and what they do.

Executives say they’re bullish about cybersecurity; nearly all claim to be supportive of their organization’s security mandate.
Yet, our research shows a large gap between what leaders say versus what they practice — something we call the Conduct Gap.

The Conduct Gap: executives’ beliefs versus behaviors

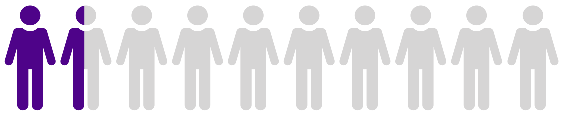
	What leaders SAY:	What leaders DO:
Security Culture	96% of leaders say executives are at least moderately supportive of or invested in their organization’s cybersecurity mandate.	**49% of CXOs have requested to bypass** one or more security measures in the past year.
Training	78% say their organizations provide mandatory cybersecurity training.	**77% use easy-to-remember password hacks,** such as including birthdates or pet names. And, **executives are 3x more likely to share work devices** with unauthorized users, such as friends, families and external freelancers.
Phishing	88% of executives say they’re prepared to recognize and report threats like malware and phishing.	Of those who have been targeted by phishing, **35% admit to clicking on the link** — or even sending money.

Whether due to a lack of time to go through proper channels, a sense of exceptionalism ("the rules can't apply to me"), or some other factor, executives simply tend to behave differently — read: riskier — than any other office workers.



24%

Executives who say they did not change the original password for work applications issued to them during onboarding.



14%

Frontline office workers who also don’t change the original password.

Why It Matters

Far from harmless workarounds, executive behaviors pose a serious threat

Most seasoned security professionals know that risky executive behaviors exist, but they often put off addressing executive cyber hygiene in favor of other strategic priorities.

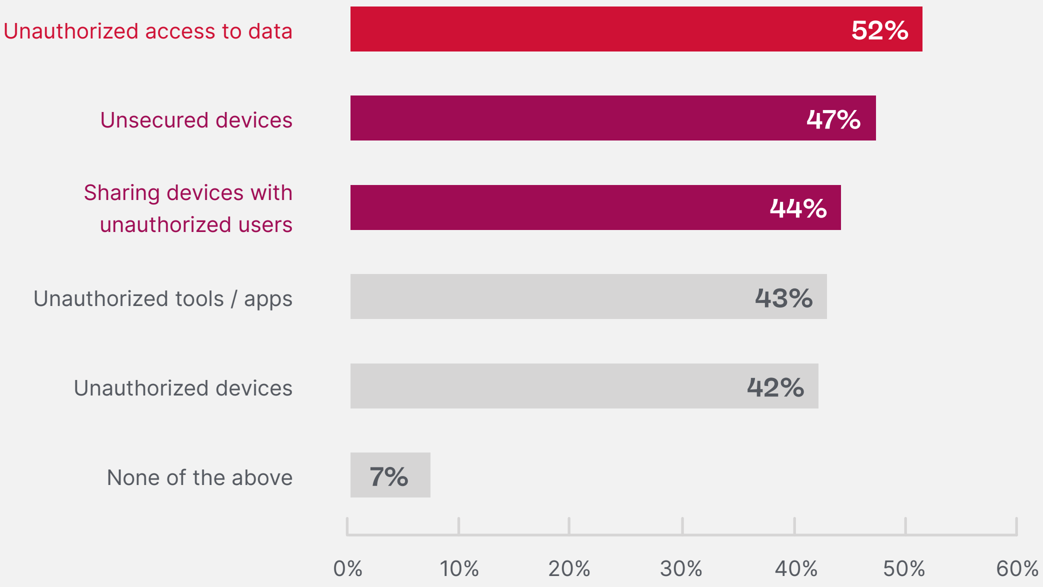
Security leaders must use their limited time and resources in a way that protects the organization from the most likely, dangerous risks. So, the logic goes, why should security teams spend additional time safeguarding leaders who say they've bought into the program — and even secured budget for that program?

Ivanti's research confirms that not only is executive security a problem, it’s also a systemic issue that afflicts most organizations.

In fact, the very same factors security pros cited as posing a high security risk to their organizations directly correspond to the self-admitted executive habits.

Q: Which of these pose a high security risk at your organization?

Note: Security professional respondents could select multiple options.



1 in 3 executives

admit to accessing unauthorized work files and data.

Executives are 3x

more likely to share work devices with family and friends than other office workers.

Power dynamics play a role in executive security behaviors

Unfortunately, the unequal power dynamic between security teams and top executives exacerbates the problem.

How often have security professionals tried to implement best-practice security policies, only to face open complaints and shadow IT workarounds from the same frontline users they're trying to protect?

How can security teams be expected to enforce better cyber hygiene and security practices by the same executives who approve their budgets — and their jobs — in an uncertain job market?

Due to limited bandwidth, exhaustion and burnout, security professionals often relent to pressure from executives.

Why security teams struggle to impact executive behavior

Burnout

CISOs are overburdened and burned out. 60% of CISOs say they have experienced burnout in the last 12 months, and 61% say there are excessive expectations for CISOs/CSOs.[1]

Culture

When the boss (or the boss's boss) asks for a favor or workaround against protocol, security employees are understandably uncomfortable pushing back.

Without a strong security-first culture, employees and security pros might simply defer to an authority's unsafe request.

Just-this-once-ism

There is a real appeal to the *“just this once”* or *“just for you”* rationalization.

In the moment, security pros may feel embarrassed to enforce rules with the CEO — especially if exceptions have been granted in the past.

"Just this once" is almost never just once, compounding the risk of executive workarounds and setting a precedent that's hard to walk back.

02

Outsized Executive Risks to Organizations:

The impact of executives' bad security habits on their cybersecurity

Problem Today

Risky executive behaviors have outsized consequences

Though few in number, executives possess an exceptional degree of automatic access as well as some concerning security behaviors; these pose a far greater security risk to their organizations than do office workers.

Unprotected first-degree executive connections

45% of leaders

let family and friends use work devices at least monthly.

❗ That's 3x the rate of all other office workers!

Nearly 1 in 5

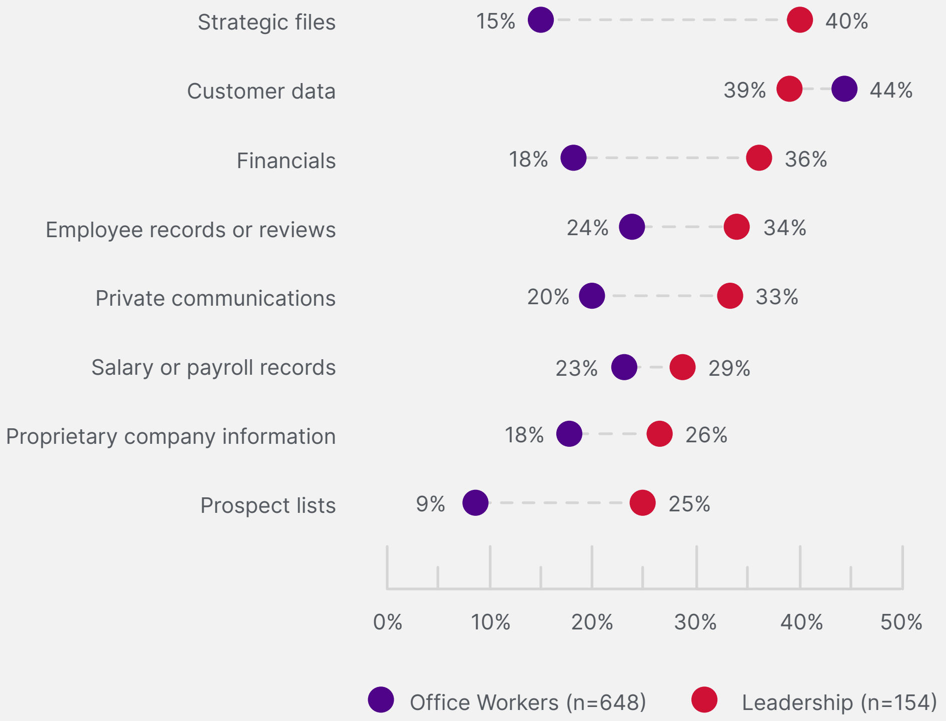
leaders have shared their work password with someone outside the company.

These first-degree associations are not trained in security, nor invested in keeping your organization safe — even as they're using your organization's devices with in-depth file and network access.

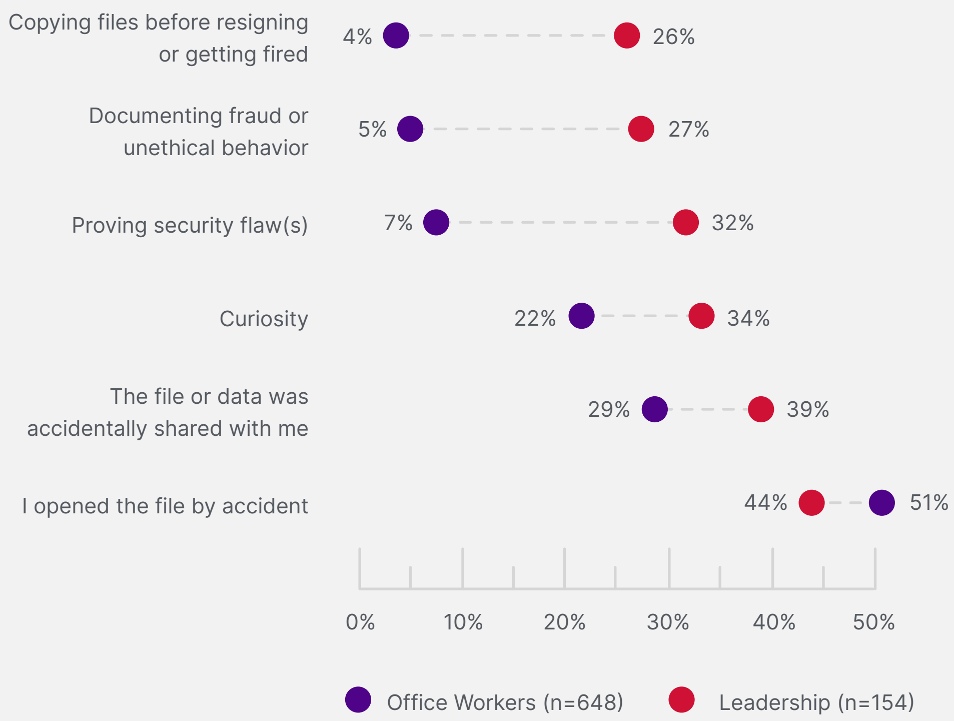
Unauthorized executive access

More than 1 in 3 leaders (34%) admit they've accessed unauthorized information at work. And, nearly 2 in 3 say that they could have edited those files/data when accessing them.

Q: What files did you access?



Q: Why did you access unauthorized information?



Note: For each graph, all respondents previously confirmed they accessed files not needed for their roles.

Why It Matters

Executive security exceptions lead to elevated risks

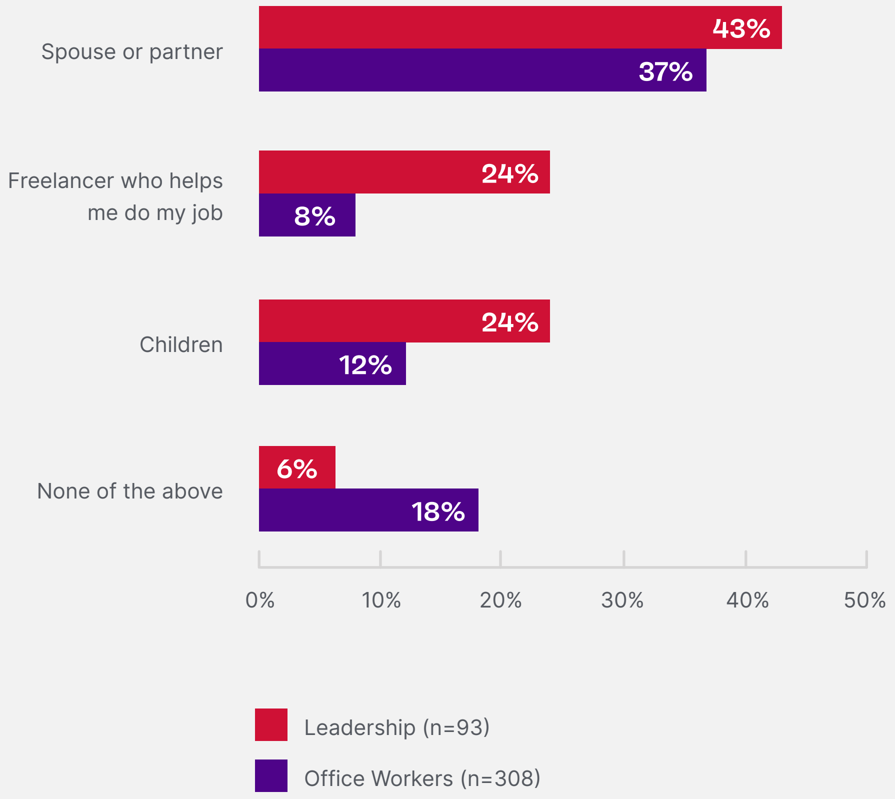
Many executives cut corners to save time or inconvenience. However, Ivanti's research shows the risk is more systemic than previously understood.

Executives reasonably believe their time is precious and limited. Sharing passwords and devices with family, colleagues and third-party tech support, for example, may be viewed as a low-risk time-saver.

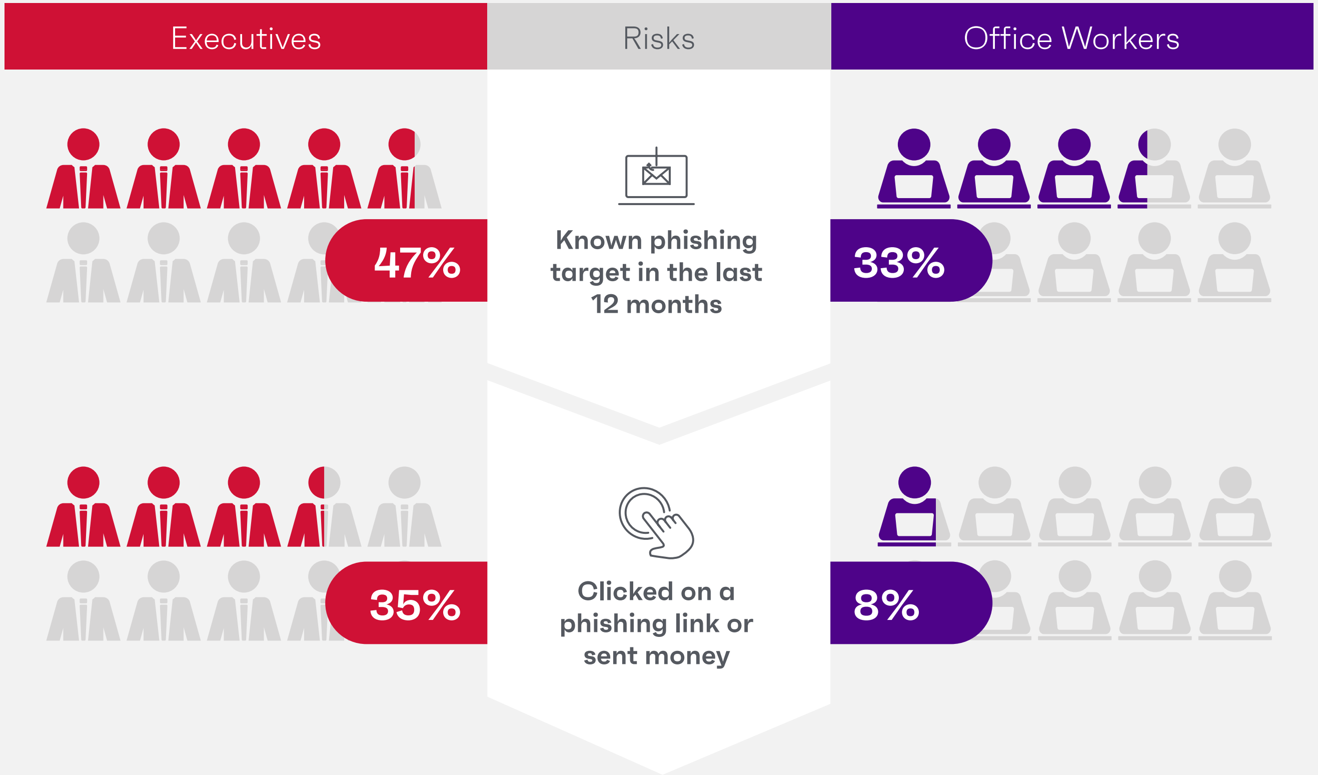
27%

Executive respondents who say they let friends/family use their work devices at least monthly — compared to just 6% of other office workers who say the same.

Q: Who have you shared your password with?



Executives at higher phishing risk than office workers



These higher rates may be due to an uptick in tailored-for-whales spearphishing attacks. It's worth the extra time and effort for attackers to target whales due to their access and privileges.

Threat actors — whether they're financially motivated ransomware gangs or advanced persistent threats (APTs) — explicitly target high-level executives because they are super-connected to valuable data sources and networked assets, while simultaneously less vigilant about their cyber hygiene habits.

After all, why cast a wide net for an average office worker's permissions, when a single "whale" grants exceptional access to more valuable assets?

> "There's a 100% chance your organization has been phished in the last year. It's the #1 way threat actors get that initial foothold in your network.
>
> "We need to make sure that we account for that, and don't just assume people will 'know better' or that a phish will be overly obvious."
>
> **Daniel Spicer**
> Chief Security Officer at Ivanti

Real-World Repercussions

Leadership turnover offers ideal phishing conditions

In 2015, Mattel fell victim to a highly publicized spearphishing event, losing $3 million to cybercriminals based in China.

A subsequent case study by Infosec[2] found that Mattel's decision to hire a new CEO created a scenario ripe for exploitation:

> “They waited for the perfect moment, which came when Mattel decided to appoint a new CEO, Christopher Sinclair, to replace Bryan Stockton in January 2015. The arrival of the new CEO implied changes within higher management which would cause new power struggles in the corporate hierarchy.
>
> **“In other words, the cybercriminals even took into consideration the office politics and human relationships of Mattel to plan their whaling email.”**
>
> **Infosec case study[2]**

03

Security Friction:

Exploring executives' tense relationship with their security teams

ivanti

Problem Today

Executives' security experiences compound bad cyber hygiene

Ivanti's research shows executives are 2.5x more likely to reach out to security than the average employee — a good sign — but they are also significantly more likely to describe their interactions as *negative*.

Leaders are:

2X

more likely to say their past interactions with security were **awkward**

4X

more likely to use **external, unapproved tech support**

33%

more likely to **not feel safe** reporting security mistakes like clicking on a phishing link. (That's over 1 in 10 leaders!)

2X

more likely to say those interactions felt **embarrassing**

5X

more likely to **share a work password** with someone outside the organization

How can organizations lower communication barriers between executives — who may feel awkward reporting errors — and the security teams trying to protect them?

> "It's unequivocal that data breaches rank as top executive concerns. For robust protection, executives must now harness AI's prowess in real-time threat detection to fortify organizational assets."

Ronald van Loon
CEO, Principal Analyst at Intelligent World

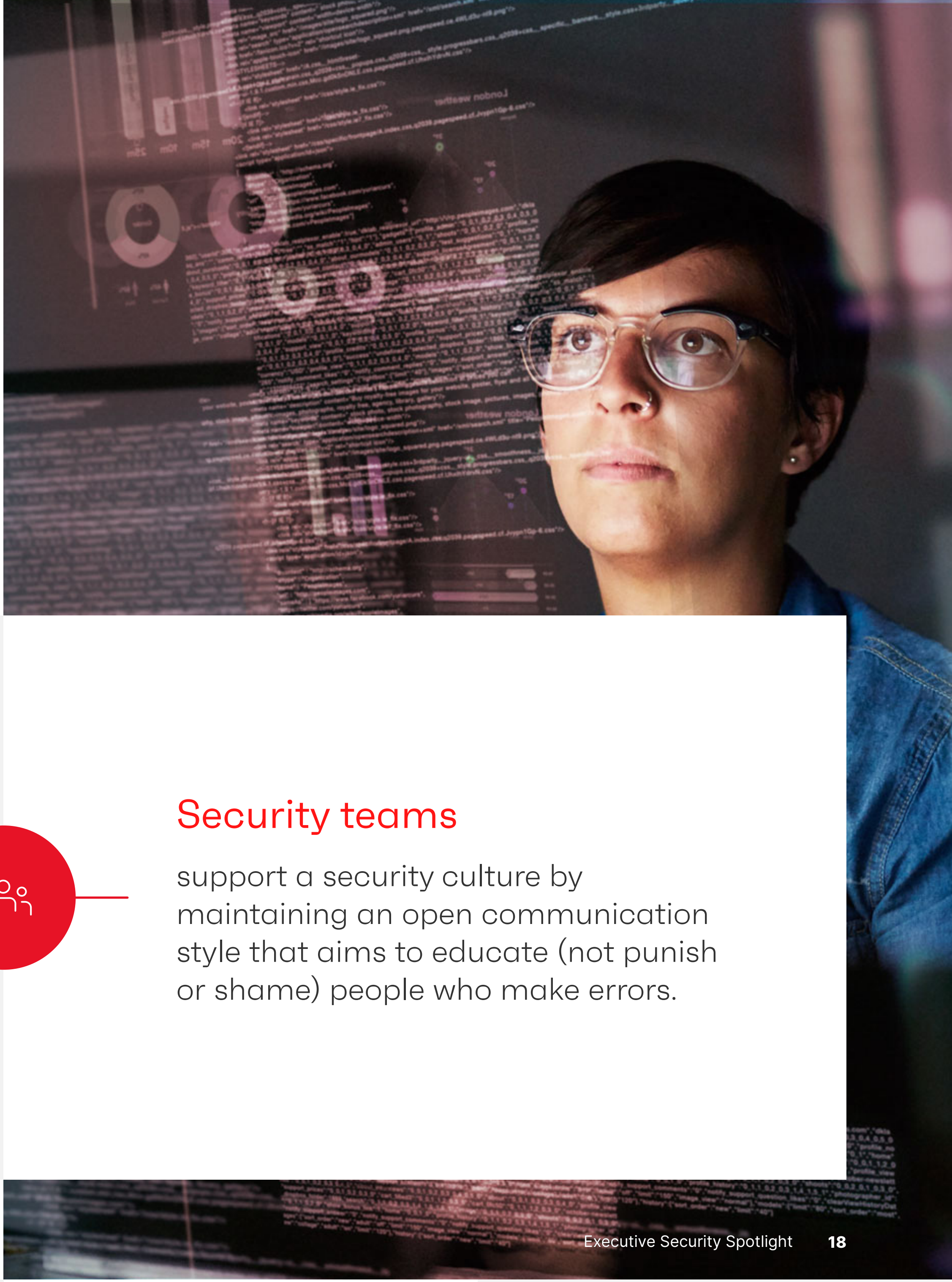
Note: These statistics compare executive-level employees with all other office workers.

Why It Matters

Organizations need a robust *executive* cybersecurity program

Executives' workarounds are driving serious security vulnerabilities, but underlying these is a company culture that tolerates executive exceptionalism and makes reporting mistakes less likely.

Security teams must prioritize rebuilding that trust and buy-in with executives from a place of honesty and friendly support — not condemnation or condescension.



Top executives

support a security culture by understanding cybersecurity's strategic role inside the organization and visibly championing its efforts.

Security teams

support a security culture by maintaining an open communication style that aims to educate (not punish or shame) people who make errors.

Mitigating executive security risks is even more urgent during layoffs

Ivanti's research shows credential deprovisioning is a problem across the board, as security professionals tell us that deprovisioning guidance is ignored a third of the time — a stunning admission, given the exposure involved.

And, 26% of all executives surveyed say they still have usable passwords from a previous job — something we call *zombie credentials*.

The risk posed by zombie credentials is even higher during periods of layoffs — when employees are more likely to take data with them, or hold a grudge against a former employer.

Jeff Pollard, a Forrester analyst, supports this conclusion: "We know that layoffs or job losses are a predictor of insider risks, making it more likely for security events to occur. We have seen over the years that this has happened."[3]

> "It used to be hard [to pull off an inside job]; now it's easy. In the past, you could take what you could carry in your briefcase. Today you can carry out terabytes."

Pete Nicoletti
Field CISO for the Americas
at Check Point Software[3]

26%

of executives surveyed say they still have usable passwords from a previous job

04

Take Action:

Closing the Executive Conduct Gap at your organization

Take Action

Shine an uncompromising light on the problem

Ivanti's research confirms what many of us have known for a long time: executives represent a unique and significant threat to an organization's security position. Now, with data in hand, it's time to address the problem.

> "You have to build a culture — I say that like it's easy, but it's true — where you can challenge leadership and build a process that everyone's accountable to."
>
> **AJ Nash**
> VP and Distinguished Fellow of Intelligence at ZeroFox

1 Conduct audits

to assess your current executive conduct gaps.

2 Fix the easiest and least-obtrusive risks first,

avoiding direct conflicts with leadership when it's unnecessary.

3 Gamify tabletop exercises,

forcing executives to connect the dots between basic cyber hygiene and a future breach's impact on their departments themselves.

4 Implement a "white glove" security program.

Even if you have many more general office workers than leadership-level employees, personal attention to this smaller stakeholder community offers a big return for your limited resource investment.

20%

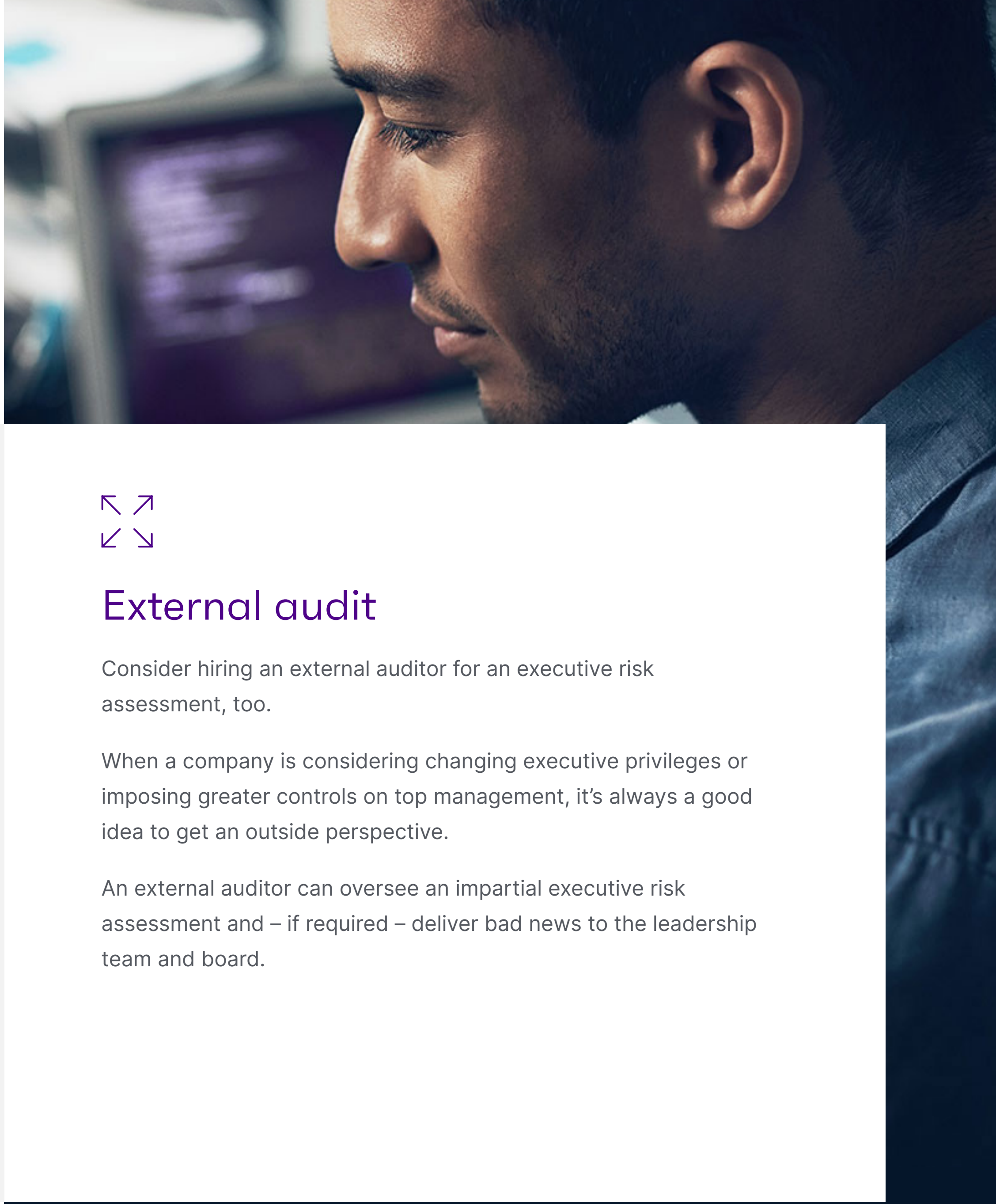
of global data breaches can be linked to insider attacks.[3]

Did you know?

C-level executives are **6.5x more likely to copy files before resigning or getting fired,** compared to other knowledge workers.

1 Conduct an audit.

To get up to date on executive-employee behaviors inside your organization, consider an audit. The goal here is not to punish or shame, but to ensure security governance policies apply to all personnel, regardless of position.



Internal audit

Take inventory of your security team's interactions with executives (director level and above) over the last 12 months, looking for patterns of miscommunication and risky behaviors — both from executives and security team members.

For example, pull a random sample of call recordings and archived ticket messages. Review these looking for cues related to tone and word choice by both parties.

Did the exchange:

- Cause embarrassment over a silly error?
- Inspire fear due to consequences of an oversight?
- Alienate or frustrate either party?

External audit

Consider hiring an external auditor for an executive risk assessment, too.

When a company is considering changing executive privileges or imposing greater controls on top management, it's always a good idea to get an outside perspective.

An external auditor can oversee an impartial executive risk assessment and – if required – deliver bad news to the leadership team and board.

Real-World Repercussions

Internal policy saves school from $100,000 phishing scam[4]

Dr. Jan McGee, the former principal of a Florida charter school, wrote a $100,000 check out of the school's account after corresponding for months with an individual she thought was billionaire Elon Musk or his representative.

Dr. McGee only had authorization to write a check up to $50,000 of school funds without board approval. Luckily, the school's business manager Brent Appy managed to cancel the check before the scammers could clear it.

> "I am a very smart lady. Well-educated. I fell for a scam.
>
> **"Grooming is when you talk to somebody and you believe in them, and they get you to trust them that this is really real, and so I fell for it."**
>
> **Dr. Jan McGee**
> Ex-principal of Florida charter school

2 Fix the easiest and least-obtrusive executive risks first.

With an audit completed and a better sense of your security vulnerabilities, it's time to make an action plan — and do so in a way that is not overly obtrusive.

Identify the most common breach or exposure in your organization based on your executive conduct gap audits, and prioritize that for remediation first.

Some of the easiest items might include:

Establishing and updating your data sensitivity and classification policy: who is allowed to have access to what, in what circumstances and for how long — along with why certain permissions aren't allowed. Make it transparent and obvious to everyone what's allowed and what's not, and why.

Updating internal communication strategies to introduce acceptable use policies (AUPs) and data sensitivity policies at every employee's initial onboarding, as well as regular reminders. You can't count on a single "official" policy document on your organization's intranet to educate your entire internal stakeholder population — especially not busy executives!

Documenting and implementing standard access approval and fulfillment procedures to guarantee that access control policies are applied to all personnel, and that all activities are fully documented and verifiable. (If your audit couldn't confirm access or network activity, then it's time to make sure it can!)

Considering your executives' current digital employee experience (DEX). Punitive or inhibitive security measures that interfere with executives' regular workflow add to feelings of distrust. Instead, choose security tools that run silently behind the scenes, providing security to executives without inviting excessive questions and/or tickets complaining about frequent lockouts.

3 Gamify executive table-top exercises.

Gamified security training sessions explicitly for non-technical leadership can win greater executive buy-in. These sessions help participants discover department-level impacts of security breaches for themselves – with security to point them in the right direction.

Consider starting small with "Spot the Phish."

You can start your next executive meeting with a simple round of "Spot the Phish," in which you show your team sample phishing messages and ask the group which was real and which was a phish.

It takes two slides and less than three minutes for this simple, interactive game featuring real cyberattacks!

Gamified security training tips for executives

Keep it short

Try shorter and more frequent people-led sessions – in-person or remotely – instead of half- or day-long workshops. Spend five minutes at the start of recurring executive leadership meetings for a quick security game or session!

Add random chance

Randomize your session threats and scenarios. It could be as simple a rolling a 20-sided die to pick a risk from a numbered list, or as complex as a generator weighted for the most realistic risks to your specific organization, region or industry.

Be creative

Encourage your executives to come up with creative solutions to block an attack or ways to exploit the risks to the presented scenarios; don't bog down a session by explaining why an idea is unrealistic, impractical or inaccurate.

Play on the Same team

Never name current or former employees as risks or threats, even in pretend exercises! Keep both executives and security team members working on the same side, so everyone either succeeds or fails as a group.

Act it out

Set up pre-made security training boxes of various scenarios, materials, props, tools or even toy bricks to speed up training exercises while including unique and creative engagement opportunities.[5]

Retrofit board games

Purchase a used board game like "Shoots and Ladders," "Life," or "Monopoly" for an easily retrofitted security-game-in-a-box.

Offer prizes

Award the best and most creative participants with company swag!

Avoid utilizing complex vernacular

Avoid security jargon and acronyms, as well as even veiled remarks on current executive security habits.

Use real-world case studies during exercises to connect the dots.

Security leaders should also highlight how malicious attacks impact personal lives and careers through incident case studies within a similar industry, executive role or risk profile. Remember to find both good and bad reactions!

Example case study: Levitas Capital[6]

The incident:

In 2020, a founder at Levitas Capital clicked on a spoofed Zoom link that installed malware on the organization's network. The attackers stole $800,000 before the ruse was discovered.

What went wrong:

In short? The normal channels for approving financial transfers broke down; attackers gained control of the company's email system; and they twice impersonated a fund co-founder to a third-party administrator.

What happened after:

Levitas's biggest client lost confidence and walked away, and the hedge fund closed two months after the event — a very public comedown for the fund's two founders, Michael Brookes and Michael Fagan.

> "There were so many red flags which should have been spotted."
>
> **Michael Fagan**
> Co-founder at Levitas Capital

4 Consider implementing a “white glove security service” for executives.

Due to their higher profile and access, high-level executives deserve individual attention from security teams: a “white glove security service,” in a manner of speaking.

Given that leaders are twice as likely to say their interactions with security are awkward — and four times more likely to seek outside tech support — the goal of such a program is to build trust and lower barriers to reporting security errors or questions.

When creating your “white glove” security program, consider:

Assigning a single point of contact – not your top-most security leader! – for high-level executives. This helps build trust while consolidating and standardizing communication.

Enforcing deprovisioning policies through automation, including manual off-boarding checks to avoid zombie credentials.

Rethinking onboarding for leadership-level employees, including custom access permissions and personal password manager set-up. Leaders themselves may not have time to follow step-by-step instructions for proper configurations, but your organization can’t afford for its executives to go without these basic guardrails.

Developing one-on-one personal security training that's not a generic presentation executives can skip through. Use previous tabletop exercises and select case studies which focus on incidents similar to the new executive’s department or role.

No matter the actions taken, your team's focus should be on instilling a positive — not punitive — security culture, and winning greater executive compliance through compelling education and collaborative insights.

As this report's own cited case studies prove: human errors happen. They will happen to your organization. They're inevitable, and impossible to avoid entirely.

However, only organizations with true executive buy-in will be able to restore systems and confidence, navigating forward beyond the breach.

Access Ivanti's cybersecurity research and report series!

ivanti

Press Reset:

A 2023 Cybersecurity Status Report

Organizations race to fortify against cyberattacks—
but the industry struggles with a reactive, checklist mentality.

ivanti

Government Cybersecurity Status Report

4 Important Ways to Take Action
and Drive Change in 2023

Part of Ivanti's Cybersecurity Status Report Series

ivanti

References

1. Proofpoint. (2022, May). 2022 Voice of the CISO: Global Insights Into CISO Challenges, Expectations and Priorities. From Proofpoint: https://go.proofpoint.com/en-voice-of-the-ciso-2022.html

2. Yip, K. N. (2016, May 21). Whaling Case Study: Mattel's $3 Million Phishing Adventure. From Infosec: https://resources.infosecinstitute.com/topic/whaling-case-study/

3. Pratt, M. K. (2023, February 28). Economic pressures are increasing cybersecurity risks; a recession would amp them up more. From CSO Online: https://www.csoonline.com/article/3689008/economic-pressures-are-increasing-cybersecurity-risks-a-recession-would-amp-them-up-more.html

4. Metz, C. (2023, March 29). Florida principal resigns after sending $100K to scammer posing as Elon Musk. From CBS News Miami: https://www.cbsnews.com/miami/news/florida-principal-resigns-after-sending-100k-to-scammer-posing-as-elon-musk/

5. Garzón, G., & Garzón, F. (2020, June 30). Cybersecurity Incident Response: Tabletop Exercises Using the Lego Serious Play Method. From ISACA: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/cybersecurity-incident-response

6. SecureWorld News Team. (2020, November 23). Hedge Fund Closes Down After Cyber Attack. From SecureWorld: https://www.secureworld.io/industry-news/hedge-fund-closes-after-bec-cyber-attac

2023 Executive Security Spotlight

New research from Ivanti shows the real risks facing the C-suite

Part of Ivanti's Cybersecurity Status Report Series

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com