ivanti

Press Reset:

A 2023 Cybersecurity Status Report

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

The chocolate bar wager

We asked 1,356 executive leaders and security professionals about their organizations' ability to stave off a damaging security breach.

Would you wager a chocolate bar on the protections you've put in place?

1 in 5 **professionals surveyed told us "no."**

Is the state of enterprise cybersecurity so dire that 20% aren't willing to stake the value of a chocolate bar — about US$2.00 — on their cybersecurity position?

What's gone wrong when an organization hires the right people, buys the right technology and adopts all the right processes and procedures — but won't take a simple bet on the strength of their IT security? It may be time for an institutional reset of our approach to effective cybersecurity.

For our State of Cybersecurity Preparedness research series, we surveyed over 6,550 professionals to better understand the serious headwinds organizations face — from emerging cybersecurity threats and stretched budgets, to the layers of technologies and processes organizations use for protection.

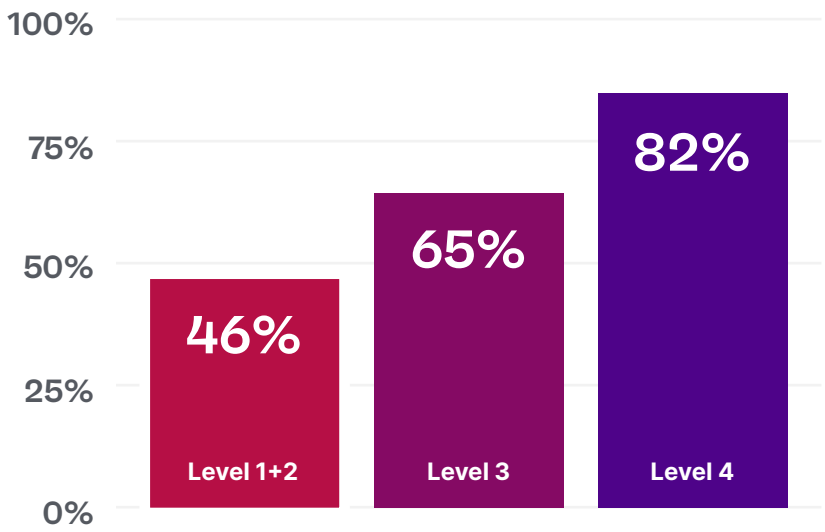
Plus, we look at the problem from three perspectives — company leadership, security professionals and knowledge workers — and spend some time on the shocking vulnerabilities we found in the C-suite.

Our goal: to get to the bottom of why security leaders can be both optimistic about their own preparedness (and they are), but also unwilling to bet a Kit Kat® bar to back it up — and how they can reset their approach for an effective, proactive cybersecurity strategy and practice.

Inside:

Executives are optimistic about preparedness

Q: Do you feel more or less prepared to defend against cybersecurity attacks, compared to one year ago?



"I feel more prepared to defend, compared to one year ago."

Cybersecurity maturity groups are explained on page 24.

01

Security in a hyperconnected world

A recent survey from PwC found “a catastrophic cyber attack is the top scenario in 2023 resilience plans,” and two in three executives consider cybercrime the single-biggest threat in the next year.[1]

What exactly does it mean to be prepared in a world of increasing vulnerability and even unknown threats? Let’s begin by assessing the cybersecurity landscape in 2023.

ivanti

Cybersecurity budgets are growing to match bigger, more damaging threats

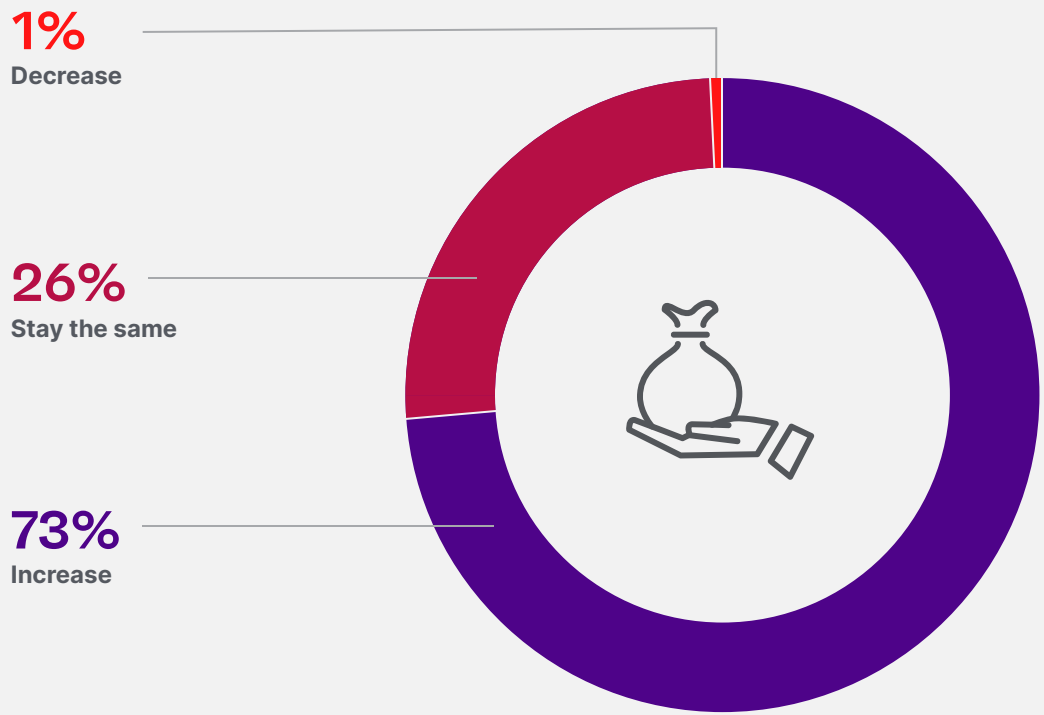
Among security professionals and leaders we surveyed, 71% predict an increase to their cybersecurity budget in 2023 — on average, an 11% bump. That's roughly three times the expected budget growth in compensation for 2023, according to the Society for Human Resource Management.[2]

Lesley Salmon, global chief information officer at Kellogg, told the Wall Street Journal: "If I get a budget challenge, it doesn't come out of cyber[security]."[3]

The average budget increase for 2023 is projected at 11% – well above projected inflation for the same period.

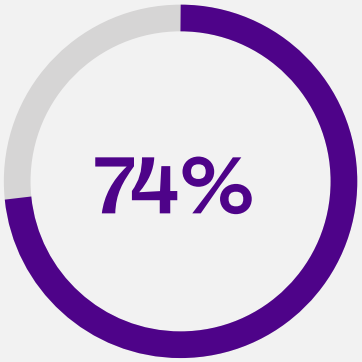
Cybersecurity budgets are growing

Q: Will your cybersecurity budget increase or decrease in 2023 compared to 2022?

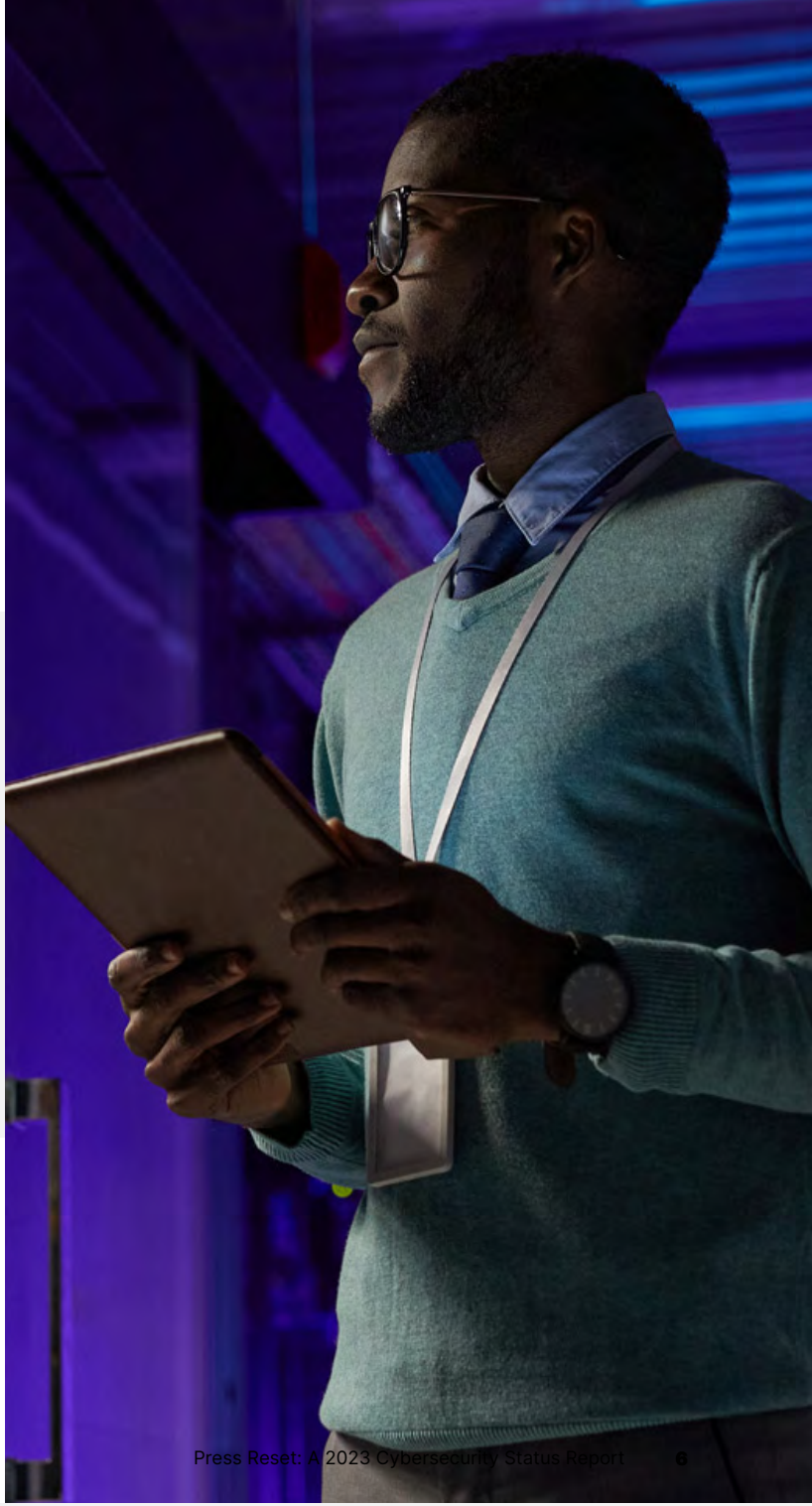


Nearly three in four security professionals Ivanti surveyed set aside funds for security breaches, and the "emergency fund" budget for breaches makes up approximately 16% of the overall cybersecurity budget — a sizable sum.

IBM's *Cost of a Data Breach 2022* report notes that the cost to recover from a data breach can easily reach seven figures; on average, a company will spend $4.35M to recover — and industries like healthcare and banking notch the highest recovery penalties.[4]



say they budget for security breaches — and on average, a breach "emergency fund" makes up 16% of the overall cybersecurity budget



Security hampered by deep security skills gaps and a complex tech stack

"Tech stack complexity" and "security skills gaps" are the biggest barriers to excellence cited by security professionals and leaders — far outranking "insufficient budget."

Tech stack complexity

Security professionals say they use on average six distinct cybersecurity tools and programs.

Charlie Bell, security chief at Microsoft, says the accumulation of too many security platforms leads to what he calls a "kind of a Frankenstein solution." As Bell explains, "The problem is everywhere you glue things together, there are seams[,] and those seams become places that people attack."[5]

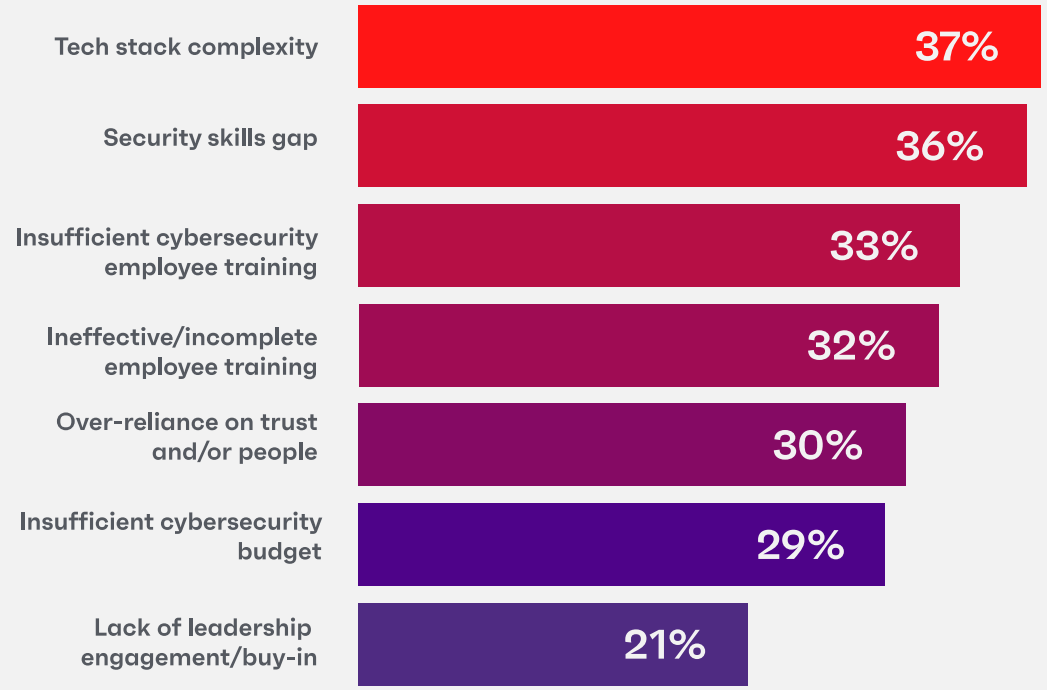
Security skills gap

For security professionals, the "skills gap" is far and away the biggest challenge, cited by 39% of security professionals surveyed.

This gap reinforces findings by many other studies, including a recent report from ISC2 that found the global cybersecurity workforce gap increased by 26.2% in 2022 compared to 2021, and 3.4 million more workers are needed to protect assets effectively.[6]

Complexity and talent pose greatest challenges

Q: Which of these are significant barriers to cybersecurity excellence at your organization?



The race to address supply chain risk

Enterprise digital transformation — and all the efficiencies that come from a highly connected supply chain — brings with it an outsized supply chain risk.

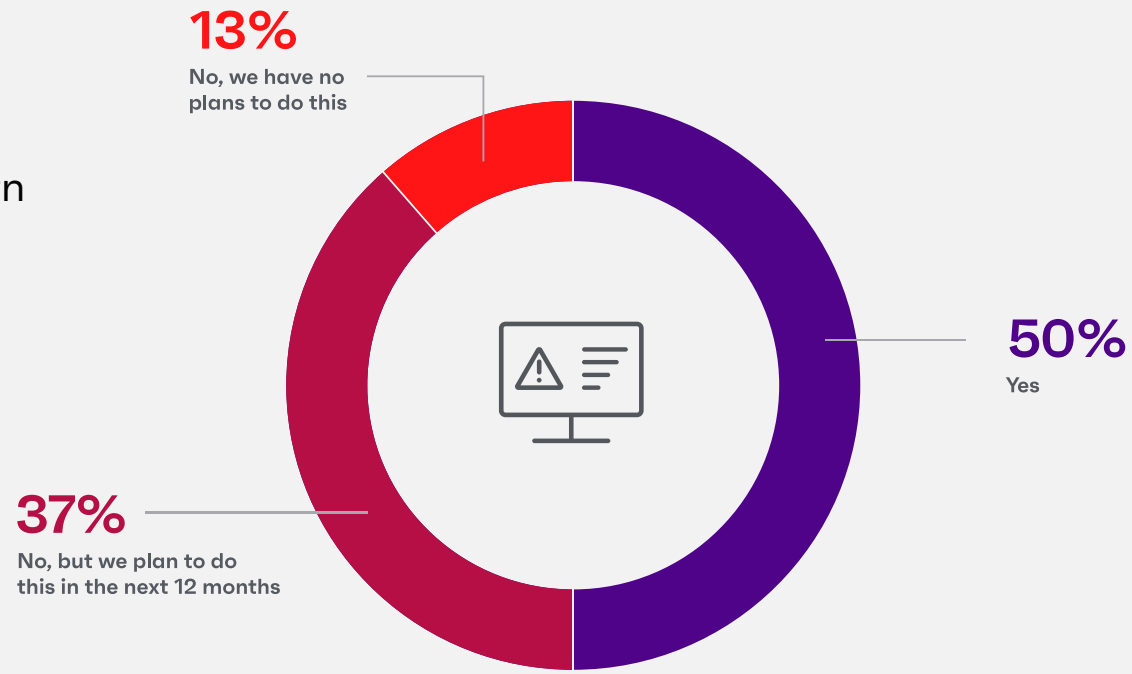
"Because today's supply chains are highly interconnected, a threat to one partner (a third-party vendor, for instance) constitutes a threat to the entire supply chain," says Shaun McAlmont, chief executive officer of Ninjio.[7]

CISOs and their security organizations are rushing to identify and fortify supply chain vulnerabilities, but the majority are still seriously lagging.

In the Ivanti study, fewer than half (47%) say they have already identified the third-party systems and components that are most vulnerable in their software supply chain, but 35% plan to address this risk in the next 12 months. And, 46% rate supply chain threats as "high" or "critical" for 2023.

Supply chain risk a growing area of concern

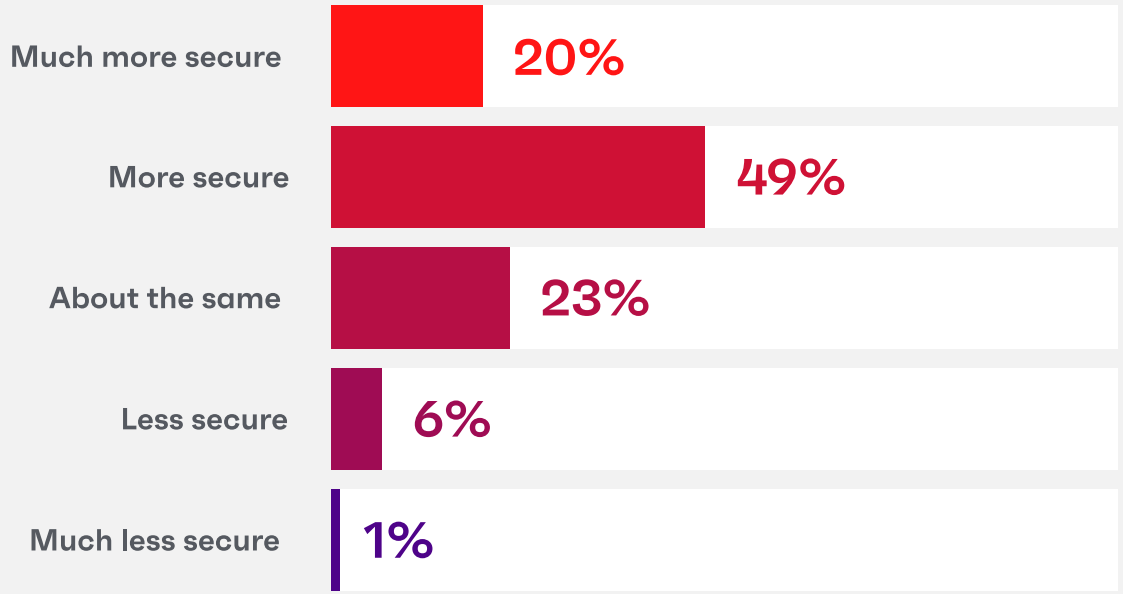
Q: Has your team identified the third-party systems/components that are most vulnerable in your software supply chain and will cause the largest organizational impact if compromised?



Cloud-based risk overblown?

Cloud-based systems a net positive for security

Q: Consider both the security risks and opportunities from a cloud environment. Do you feel your systems will be net more secure or less secure due to adopting cloud-based systems and/or storage?



More than two in three (68%) say their systems are net more secure due to adopting cloud-based systems and/or storage.

In other words, despite a misperception that cloud-based systems expose companies to higher-than-acceptable cybersecurity risks, the executives and security professionals we surveyed feel the cloud-based environment provides greater security after weighing risks and opportunities.

"Ensuring a positive and secure digital employee experience is the new cornerstone for modern IT executives," said Andy Stone, Chief Technology Officer at Pure Storage. "By utilizing the cloud securely and effectively, organizations can enable employees to work wherever they want and on any device. In a digital-first world, failure to achieve a secure shift to cloud will largely stagnate a company's growth."

02

2023 cybersecurity hotspots

What do cybersecurity insiders view as top threats for 2023? And, what are the ways organizations are preparing for attacks — both known and unknown?

ivanti

Preparedness and experience gaps

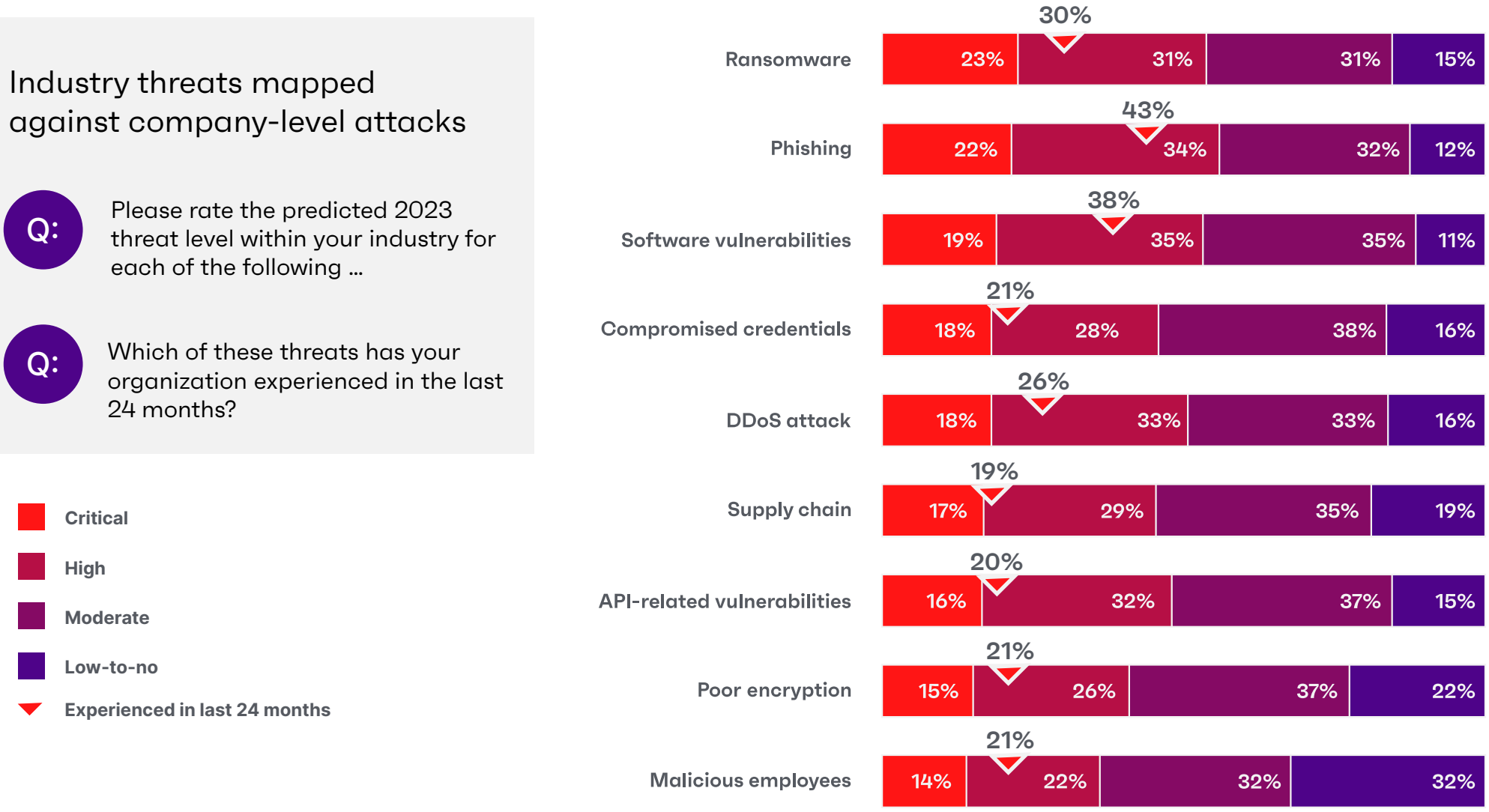
The professionals we surveyed name phishing, ransomware and software vulnerabilities as top industry-level threats.

When comparing actual attacks companies have experienced, phishing and software vulnerabilities outpace other risks by multiples.

Industry threats mapped against company-level attacks

Q: Please rate the predicted 2023 threat level within your industry for each of the following …

Q: Which of these threats has your organization experienced in the last 24 months?



One anonymous survey taker shared,

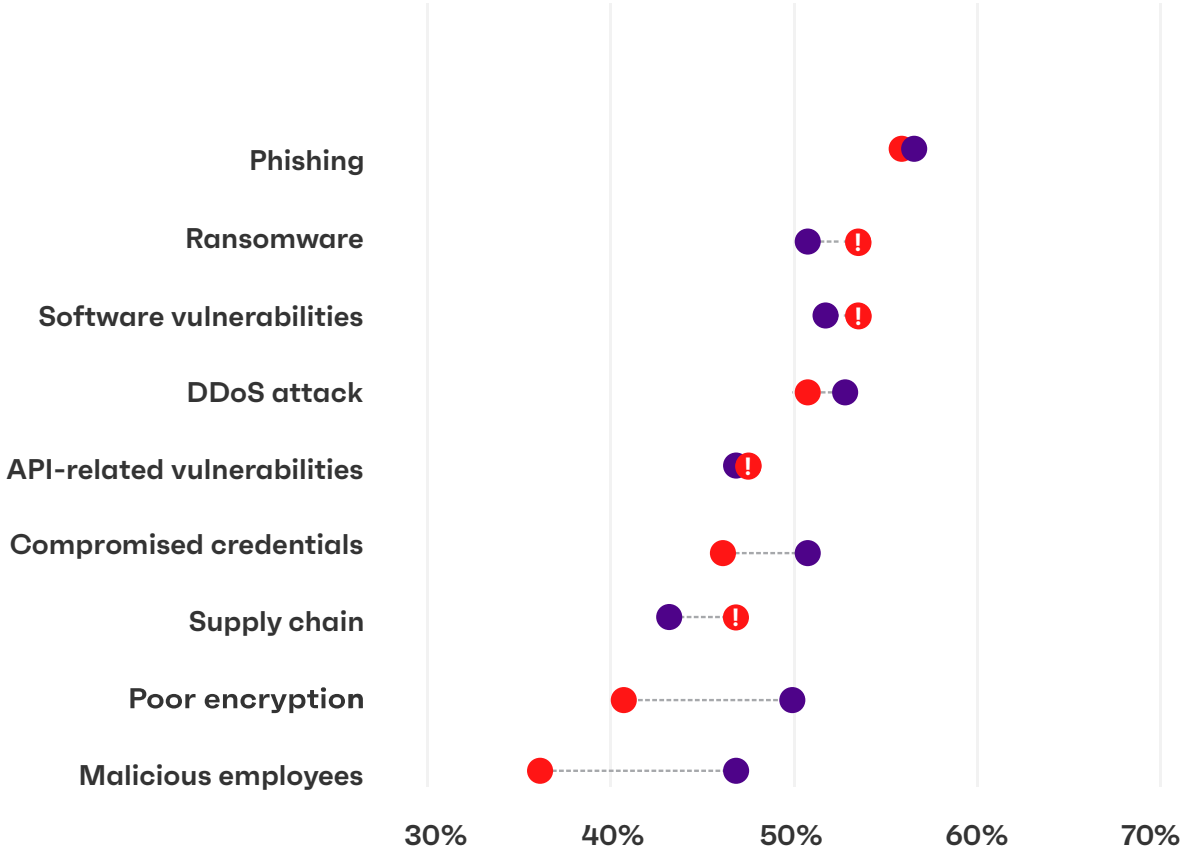
"We've experienced a few advanced phishing attempts and the employees were totally unaware they were being targeted. These types of attacks have become so much more sophisticated in the last two years — even our most experienced staff are falling prey to it."

Despite the diversity of threats, a large share of respondents say they're prepared to meet the growing threat landscape. Approximately half say they are "very prepared" to face myriad threats — including ransomware, poor encryption, malicious employees and software vulnerabilities.

One hotspot: supply chain vulnerabilities. Just 42% say they are very prepared to safeguard against supply chain threats, even though 46% call it a high-level threat.

This risk was just one of several "inverted" threats, where preparedness levels lag estimated threat levels.

Security threats versus security preparedness



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

Q: How prepared is your organization to deal with each type of threat listed here?

- High + Critical Threat
- "Very Prepared"
- Inverted Threat

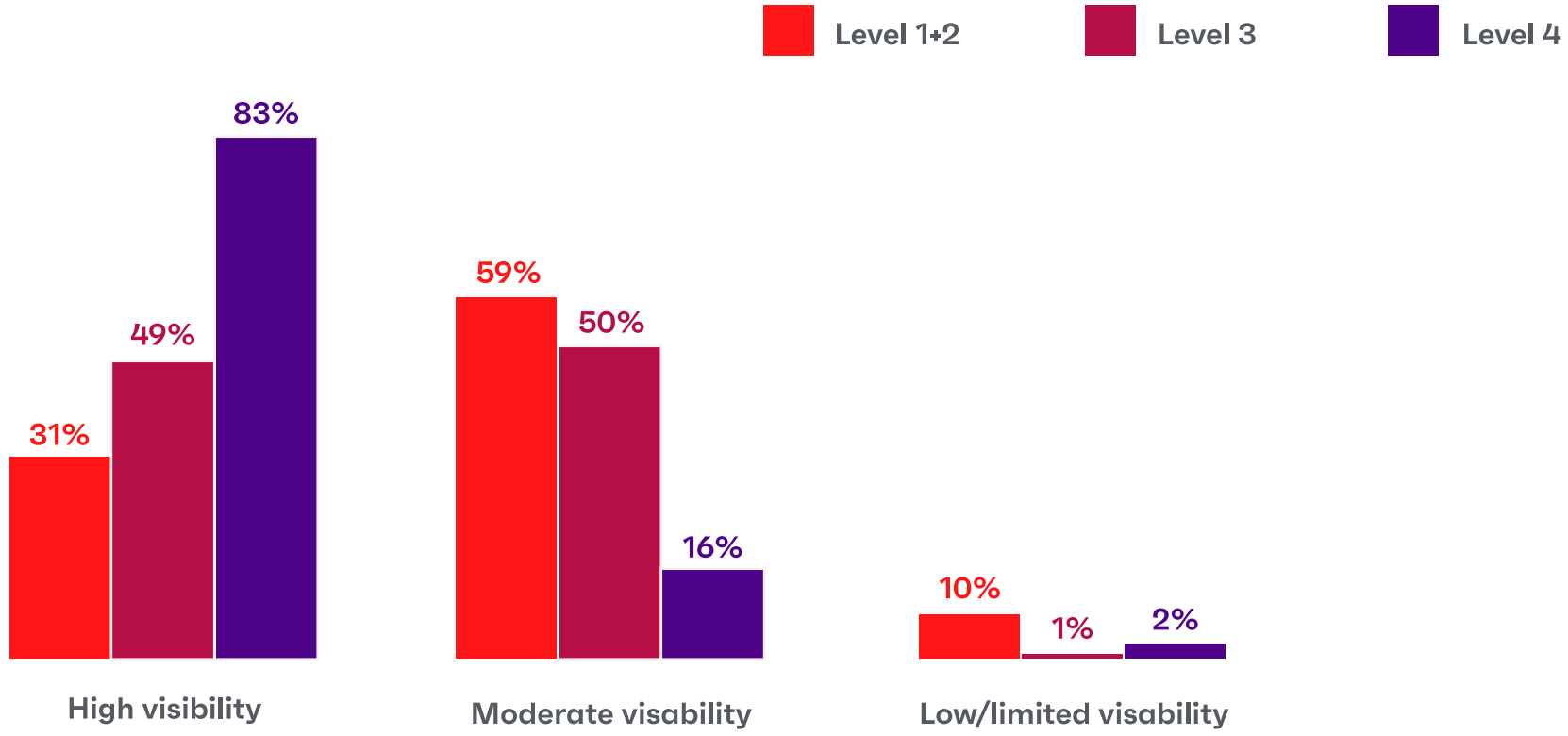
Expected safeguards found seriously lacking

Just over half of leaders and security professionals (52%) say they have “high visibility” into every user, device, application and service on their network.

And, only 48% say they run their asset discovery program at least once per week.

Best-in-class organizations report high asset visibility

Q: What degree of visibility does your organization have into every user, device, application and service on your network? (Shown by cybersecurity maturity level.)

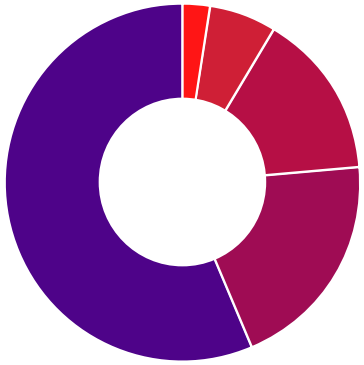


Nearly all say they have a formal process for deprovisioning, and the large majority (68%) say deprovisioning for departing employees occurs within three business days. (For outside vendors, 81% say the process happens within 5 business days.)

Yet, security professionals also tell us that the deprovisioning guidance is ignored a third of the time — a stunning admission, given the exposure involved.

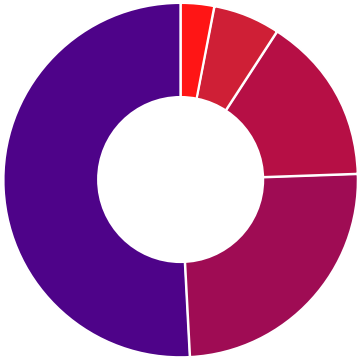
With deprovisioning, good protocols but mixed results

Q: How quickly do you deprovision **an employee's credentials** after they leave the organization?



- 2% — We don't have a formal process to deprovision credentials
- 5% — Unsure
- 12% — Mare than 7 days
- 16% — 4-7 days
- 45% — 2-5 business days

Q: How quickly do you deprovision a **third-party vendor, consultant and/or contractor's credentials** at the end of a contract or service termination?



- 2% — We don't have a formal process to deprovision credentials
- 4% — Unsure
- 10% — Mare than 7 days
- 16% — 4-7 days
- 33% — 2-3 business days

The zombie credential epidemic

Even more glaring: 45% of those surveyed say they suspect that former employees and contractors still have active access to company systems and files — whether because deprovisioning guidance wasn't followed correctly, or because third-party apps offer hidden access even after credentials have been inactivated.

"Large organizations often fail to account for the huge ecosystem of apps, platforms and third-party services that grant access well past an employee's termination," says Dr. Srinivas Mukkamala, Chief Product Officer at Ivanti. "We call these zombie credentials, and a shockingly large number of security professionals — and even leadership-level executives — still have access to former employers' systems and data."

45%

of security professionals say they either suspect or know that former employees and contractors still have active access to systems or files in the form of still-active usernames, passwords and login information.

Deprovisioning guidance is followed just 68% of the time

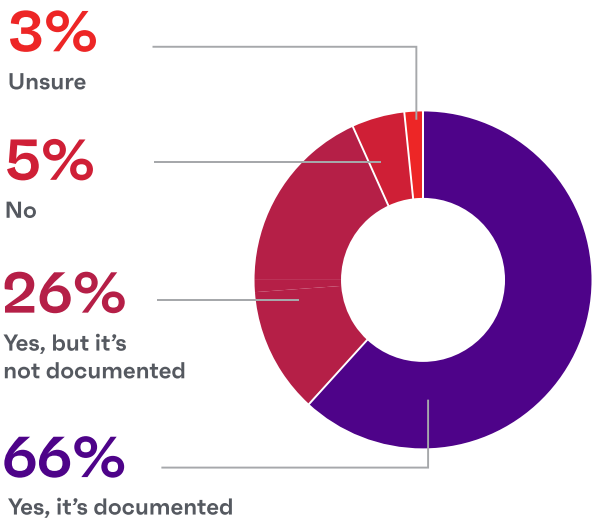
ivanti

When every patch is a priority, no patch is prioritized

92% say they have a method to prioritize which vulnerabilities to patch, though more than one in four of those say these methods are not documented in any way.

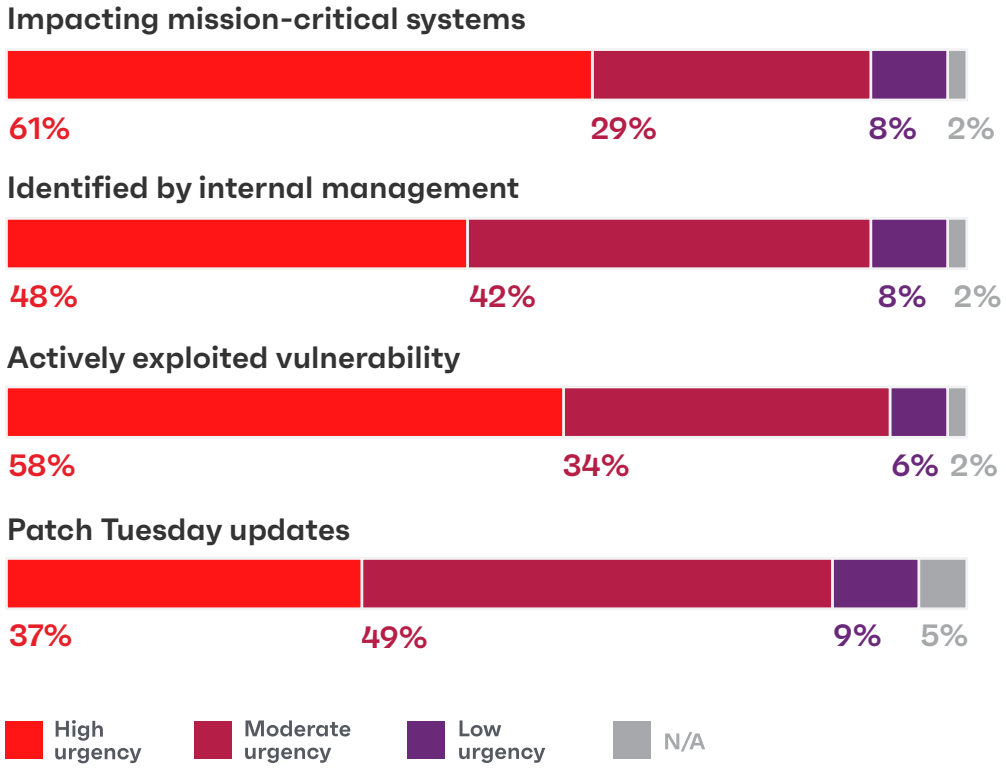
But, when asked which types of patches are prioritized, security professionals tell us all types rank high — meaning none do.

Q: Does the cybersecurity team have a method to prioritize which vulnerabilities to patch?



Patch management plagued by "everything's urgent" mindset

Q: How do you prioritize which vulnerabilities to patch?



This “everything is urgent” mindset not only muddies priorities for the security team, but it can also lead to high levels of stress and burnout.

A global survey of 1,100 incident responders by IBM found that 68% say it’s common to be assigned to two or more incidents at once. As the study explains, “The work appears to be taking its toll: A similar figure, 64%, said they have sought mental-health assistance for insomnia, burnout and anxiety.”[8]

An earlier survey by Ivanti uncovered similar challenges; when asked what drives turnover, IT professionals cited high workload (41%) and unrealistic expectations placed on the team (34%) above all other issues.[9]

The perils of whale phishing

Whale phishing is when cyberthreats use customized spearphishing techniques to chase “whales” — significant, high-value targets like CEOs, politicians or senior government officials.

Once a whale is compromised, attackers can gain access to sensitive information, authorize wire transfers and even compel employees to take certain actions they would normally never agree to — but when the boss says “jump” ...!

Leaders say they're aware of cybersecurity risks but still engage in risky behaviors

Nearly 9 in 10 leaders (e.g., CEOs, vice presidents and directors) say they are prepared to recognize and report threats like malware and phishing at work.

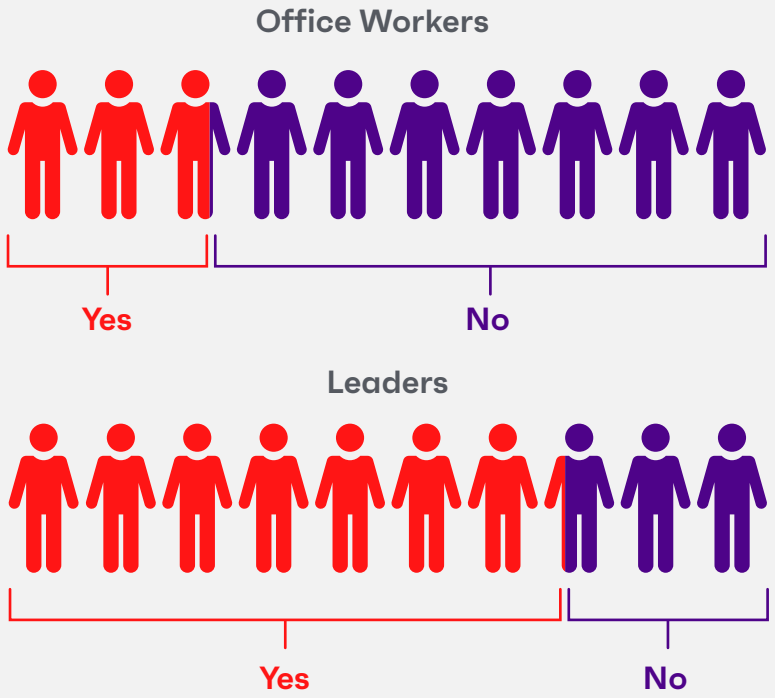
And, they are significantly more likely to say they've contacted the security team with a question or concern, when compared to other employees we surveyed.

These are good signs; however, our research shows leaders are much more likely to report negative interactions with the security team, and they are 1.3 times more likely to say they "don't feel safe" reporting security lapses.

Plus, their actions — the everyday habits that organizational leaders admit to — are even more concerning.

Leaders say they're engaged with security efforts

Q: Have you ever contacted a cybersecurity employee at your work with a security question or concern?



Leaders engage in more dangerous behaviors

Professionals like CEOs, vice presidents and directors — people we labeled as “leaders” in our survey — are more likely than other knowledge workers to practice unsafe security behaviors.

- **More than a third of surveyed leaders** have clicked on a phishing link — four times the rate of other office employees!
- **Nearly one in four leaders** use easy-to-remember birthdays as part of their password.
- **Leaders are much more likely than employees** to hang on to passwords for years rather than update them regularly; one in four do this.
- **Surveyed leaders are five times more likely** to share their password with people outside the company.

A successful whale phishing campaign is a much greater vulnerability than traditional phishing attempts, yet many organizations still don't treat it as a unique, outsized threat.

Consider this: Leaders — people who are targeted with more sophisticated phishing campaigns — are four times more likely to be victims of phishing, compared to all other office workers.

(Let's repeat that in case you're speed-reading: Your most high-value employees are four times more likely to take an action that swings the security doors open to bad actors.)

This risk alone means organizations need to develop customized training curricula and tech interventions for CEOs and other high-level executives — extra layers of protection around these highly vulnerable targets.

More than 1 in 3 leaders—people like CEOs, VPs and directors—have fallen victim to phishing scams, either by clicking a scam link or sending money.

04

How to futureproof organizations for 2023 — and beyond

As part of Ivanti's study, the research team looked at companies that self-report as advanced cybersecurity organizations — a Level 4 on the cybersecurity maturity scale. We want to know: what bellwethers set this group apart? And, how can other organizations learn from them?

ivanti

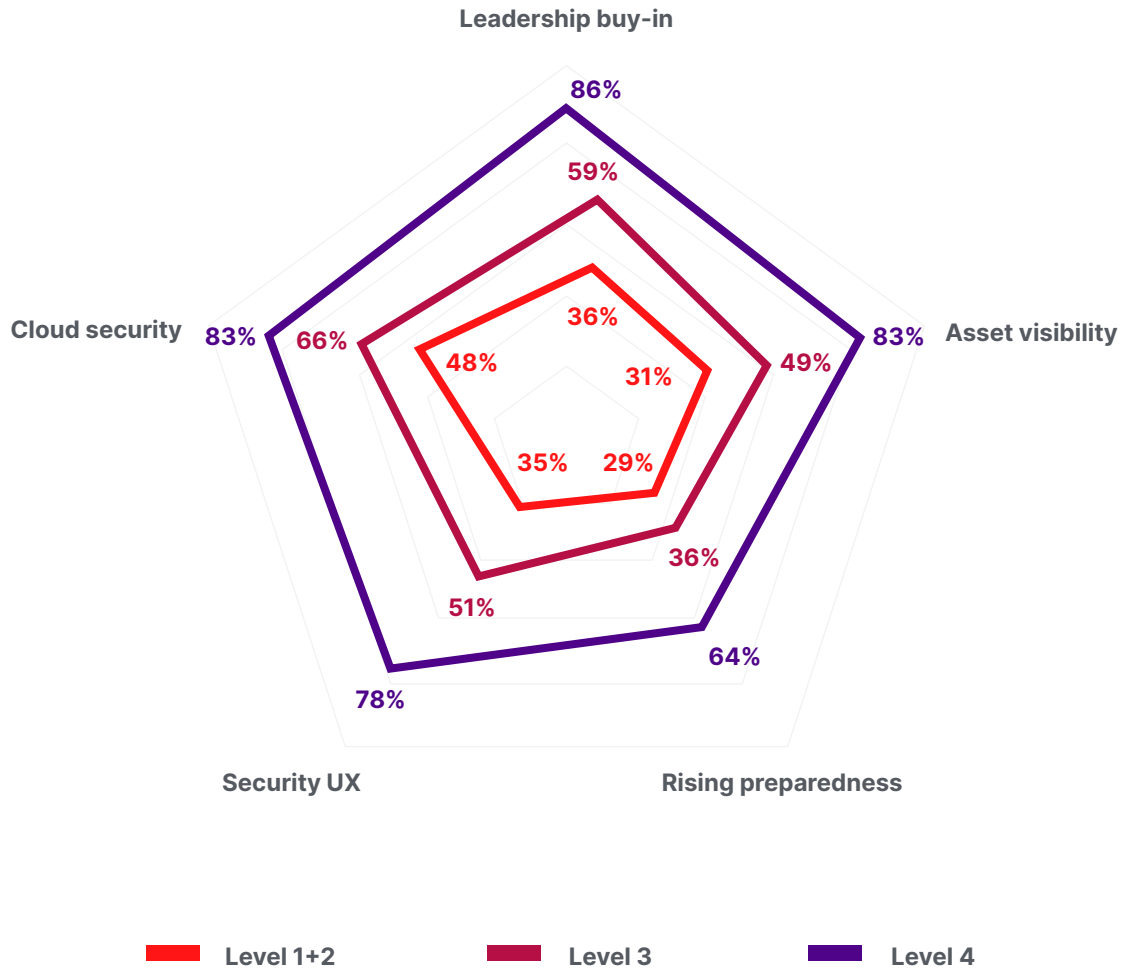
The Cybersecurity Maturity Scale

We asked survey-takers who work in cybersecurity to rate their organization's level of cybersecurity preparedness — from basic (Level 1) to best-in-class (Level 4). We then compared these cohorts to learn more about the practices and behaviors of Level 4 organizations.

More mature cybersecurity organizations report more buy-in, increased attention to visibility and UX

Charts display percent of respondents reporting:

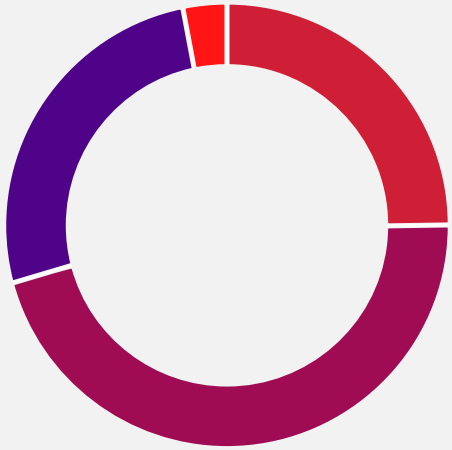
- Very supportive executive leadership ("Leadership buy-in")
- High visibility into users, devices, apps and services on their networks ("Asset visibility")
- Very prepared for supply chain threats within their industry ("Rising preparedness")
- High prioritization of UX for end users for cybersecurity-related tech interventions ("Security UX")
- More security in their cloud-based systems and/or storage adoption ("Cloud security")



Note: collecting information through self-reporting has limitations, as people may be biased when evaluating their own efforts. Self-reporting may be in part responsible for the exceptionally small number of Level 1 responses, which we combined with Level 2 for this report.

We believe the following findings based on this maturity model provide useful signals to the cybersecurity field, but we ask that readers keep research limitations in mind.

Cybersecurity professional responses by level (n=902)



4%

Level 1: Basic cybersecurity hygiene

25%

Level 2: Intermediate cybersecurity hygiene with established procedures and policies

42%

Level 3: Substantial and proactive cybersecurity hygiene

29%

Level 4: Advanced; proven ability to fend off advanced threats

What makes Level 4 cybersecurity organizations different?

Leadership buy-in: The large majority of self-reported Level 4 organizations (86%) say they have buy-in and support from higher ups. Buy-in can surface in a variety of ways, from budget support to build stronger defenses, to autonomy to design proactive strategies instead of chasing the latest executive priority regardless of cost-benefit.

Visibility: Most Level 4s (83%) have high levels of visibility into users, apps and devices across their organizations. In fact, they're 70% more likely to demonstrate this compared to Level 3 organizations. As the number of devices and apps explodes, visibility will be a major area of focus in 2023.

CISA recently underlined this need when it issued a new directive in late 2022 (BOD 23-01). CISA director Jen Easterly explains, "Knowing what's on your network is the first step for any organization to reduce risk."

Supply chain resilience: When it comes to supply chain preparedness, Level 4s report they are more prepared compared to all others we surveyed; 64% say they are "very prepared" to face supply chain threats, compared to just 36% of Level 3s.

"Supply chain preparedness is one area where most organizations are still struggling to adapt — in large part because the problem can be enormously complex," explains Amanda Wittern, Deputy CSO at Ivanti. "We expect supply chain risk reduction will be a big area of investment in 2023 — from implementing Software Bill of Materials (SBOMs), to deploying zero trust solutions and comprehensive access controls."

Security in the cloud: Level 4 organizations are much more likely to say their cloud-based systems are net more secure. In fact, they are three times more likely to say the cloud environment is "much more secure" compared to Level 3s.

UX for risk reduction: Best-in-class organizations know excellent user experience is an integral part of security — effectively an antidote to poor adherence and risky workarounds. Most Level 4s (71%) say UX for end users is a "high priority" or "mission-critical" — 20 points higher than Level 3s.

"Current inflationary pressures and macroeconomic conditions are having a push and pull effect on cloud spending. Cloud computing will continue to be a bastion of safety and innovation, supporting growth during uncertain times due to its agile, elastic and scalable nature." — Sid Nag, vice president analyst at Gartner®[11]

One thing is certain: **wholly defensive tactics will not serve in 2023.** Michael Levin, senior vice president for global cyber risk and defense at UnitedHealth Group, explained this concept to the Wall Street Journal: "A lot of organizations are still focused on those earlier checklists and compliance. *'I did all the things you told me to, so I am safe,'* versus considering *'how can I be safe?'*"[12]

Remember: the overwhelming majority of security professionals and leaders told us their organizations are as prepared or more prepared today than one year ago — a stunning 97% said this! Yet, one in five won't wager a chocolate bar. Optimism, meet reality.

To cope with fast-changing and yet-unknown threats, organizations must move beyond a reactive, rules-based stance (i.e., "I've done all the things I'm supposed to do").

Maturing cybersecurity teams should also consider:

Automation: Deploy automation to boost asset visibility and deploy a risk-based prioritization to patching — both table stakes for secure companies in 2023 — and use smart UX to compel good security behavior from employees (i.e., make exceptions and workarounds more trouble than they're worth).

Resilience: Design react-and-recover plans to shorten outages and limit knock-on effects, knowing that some attacks will inevitably break through.

Empowerment: Give the cybersecurity team greater independence to set the security agenda — no more thoughtless reactions to the latest threat to hit the news, of punishing teams for failing to accomplish endless lists of constantly pivoting priorities!

Holistic risk management: Think about security beyond the walls of the organization — from work from everywhere (WFE) and hybrid employees, to third-party contractors and vendors. Take a risk-reward approach to these players, paying outsized attention to your security "whales" like C-suite executives or highly embedded software suppliers.

In the end, when cybersecurity preparedness resets from reactionary and defensive to future-looking and resilient, we think many more organizations will be willing to take the chocolate bar wager.

05

Methodology

Ivanti surveyed over 6,500 executive leaders, cybersecurity professionals and office workers in October 2022. Our goal: to understand today's threats — from the perspective of security professionals, as well as executive leaders and all other office workers — plus find out how companies are preparing for yet-unknown future threats.

The study was administered by Ravn Research, and panelists were recruited by MSI Advanced Customer Insights. Survey results are unweighted. Further details by country are available by request.

Survey sample

Office Workers
5,202

Security professionals
902

Leadership executives
454

Industry Sectors

6% Education

12% Financial services

12% Government

13% Manufacturing/processing

3% Not-for-profit/charities

18% Other

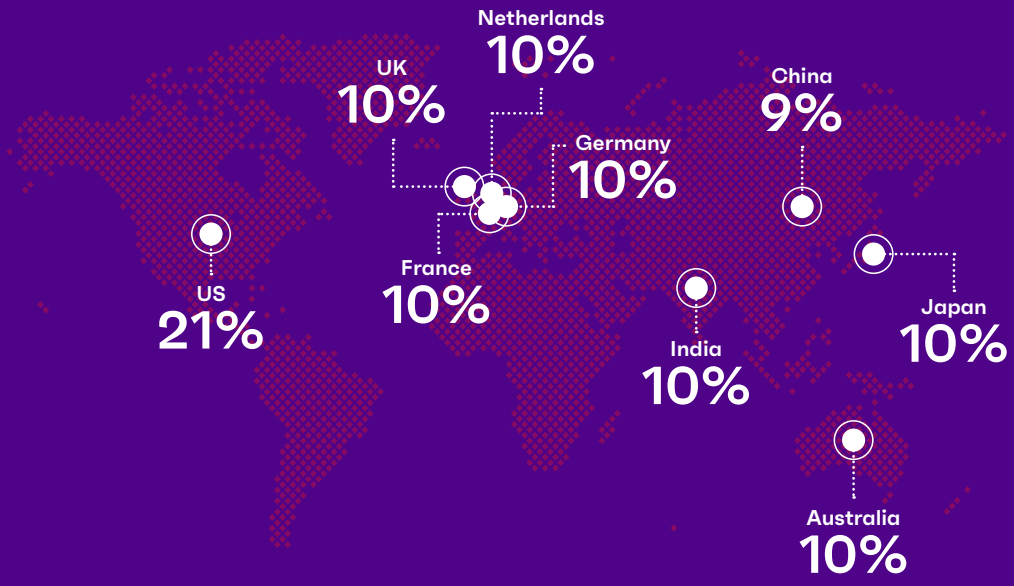
8% Professional services

11% Retail, e-commerce, wholesale

14% Technology

3% Telecom

Countries



References

All charts in this report were generated from survey data collected as part of the Ivanti State of Cybersecurity Preparedness 2023 series, as described in "Methodology."

1. PwC: "A C-suite united on cyber-ready futures: Findings from the 2023 Global Digital Trust Insights," Sept. 2022. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html

2. SHRM: "2023 Salary Budgets Projected to Stay at 20-Year High but Trail Inflation," Sept. 2022. https://www.shrm.org/resourcesandtools/hr-topics/compensation/pages/2023-salary-increase-budgets-stay-trail-inflation.aspx

3. The Wall Street Journal: Cybersecurity Tops the CIO Agenda as Threats Continue to Escalate," Oct. 2022. https://www.wsj.com/articles/cybersecurity-tops-the-cio-agenda-as-threats-continue-to-escalate-11666034102

4. IBM: "Cost of a data breach 2022: A million-dollar race to detect and respond," July 2022. https://www.ibm.com/reports/data-breach

5. The Wall Street Journal: "Microsoft's New Security Chief Says It Is Time to Take Shelter in the Cloud," Feb. 2022. https://www.wsj.com/articles/microsofts-new-security-chief-says-it-is-time-to-take-shelter-in-the-cloud-11645624800

6. InfoSecurity Group: "Cybersecurity Workforce Gap Grows by 26% in 2022," Oct. 2022. https://www.infosecurity-magazine.com/news/cybersecurity-workforce-gap-grows/

7. Supply Chain Brain: "Why Cybersecurity Has Never Been More Important for the Supply Chain Sector," Oct. 2022. https://www.supplychainbrain.com/blogs/1-think-tank/post/35798-why-cybersecurity-has-never-been-more-important-for-the-supply-chain-sector

8. The Wall Street Journal: "Rise in Cyberattacks Stretches and Stresses Defenders," Oct. 2022. https://www.wsj.com/articles/rise-in-cyberattacks-stretches-and-stresses-defenders-11664962202

9. Ivanti: "State of IT in 2021," Dec. 2021. https://www.ivanti.com/company/press-releases/2021/new-ivanti-study-finds-the-biggest-challenge-for-it-departments-is-keeping-up-with-digital-transformation-and-keeping-talent-in-technical-roles

10. CISA: "CISA Directs Federal Agencies to Improve Cybersecurity Asset Visibility and Vulnerability Detection," Oct. 2022. https://www.cisa.gov/news/2022/10/03/cisa-directs-federal-agencies-improve-cybersecurity-asset-visibility-and

11. Gartner Press Release: "Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023," Oct. 2022. https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

12. The Wall Street Journal: Cybersecurity Tops the CIO Agenda as Threats Continue to Escalate," Oct. 2022. https://www.wsj.com/articles/cybersecurity-tops-the-cio-agenda-as-threats-continue-to-escalate-11666034102

Additional Chart Information

Pg. 3 - Security and leader respondents; n=1,356

Pg. 5 - Security and leader respondents; n=1,356

Pg. 7 - Security and leader respondents; n=1,356

Pg. 8 - Security respondents; n=902

Pg. 9 - Security and leader respondents; n=1,341

Pg. 11 - Security respondents; n=902

Pg. 13 - Security respondents; n=902

Pg. 14 - Security and leader respondents; n=1,356

Pg. 15 ("an employee's credentials") - Security respondents; n=902

Pg. 15 ("a third-party vendor's [...] credentials") - Security respondents; n=882

Pg. 17 ("how do you prioritize") - Security respondents; n=902

Pg. 17 ("a method to prioritize") - Security respondents; n=886

Pg. 20 - Leaders and office worker respondents; n=5,656

Pg. 21 ("More than a third") - Leaders and office worker respondents; n=1,949

Pg. 21 ("Nearly one in four") - Leaders and office worker respondents; n=5,656

Pg. 21 ("Leaders are much more") - Leaders and office worker respondents; n=5,373

Pg. 21 ("Surveyed leaders") - Leaders and office worker respondents; n=5,656

Pg. 24 ("Leadership buy-in") - Security and leader respondents; n=1,356

Pg. 24 ("Asset visibility") - Security and leader respondents; n=1,356

Pg. 24 ("Rising preparedness") - Security respondents; n=902

Pg. 24 ("Security UX") - Security respondents; n=902

Pg. 24 ("Cloud security") - Security and leader respondents; n=1,341

Press Reset:

A 2023 Cybersecurity Status Report

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

ivanti

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