ivanti

Government Cybersecurity Status Report

4 Important Ways to Take Action and Drive Change in 2023

Part of Ivanti's Cybersecurity Status Report Series

The Right Time? Now.

Recent attacks on hospital networks, global logistics systems and even democratic elections pose a fundamental threat to public safety and governance.

But we are still in early days.

High-speed advances in generative AI and “deepfakes” mean ransomware delivery is about to become even more believable – and therefore more dangerous.

Governments worldwide have taken notice. New mandates from President Biden, as well as directives from the European Commission, mark a new state of global urgency to protect critical assets and infrastructure from cyberattacks.

Ivanti surveyed over 800 government employees worldwide to understand:

- Employee behavior and attitudes about cybersecurity
- The impact of flexible and hybrid work arrangements on the public sector
- Cybersecurity professionals’ take on emerging threats and security technology

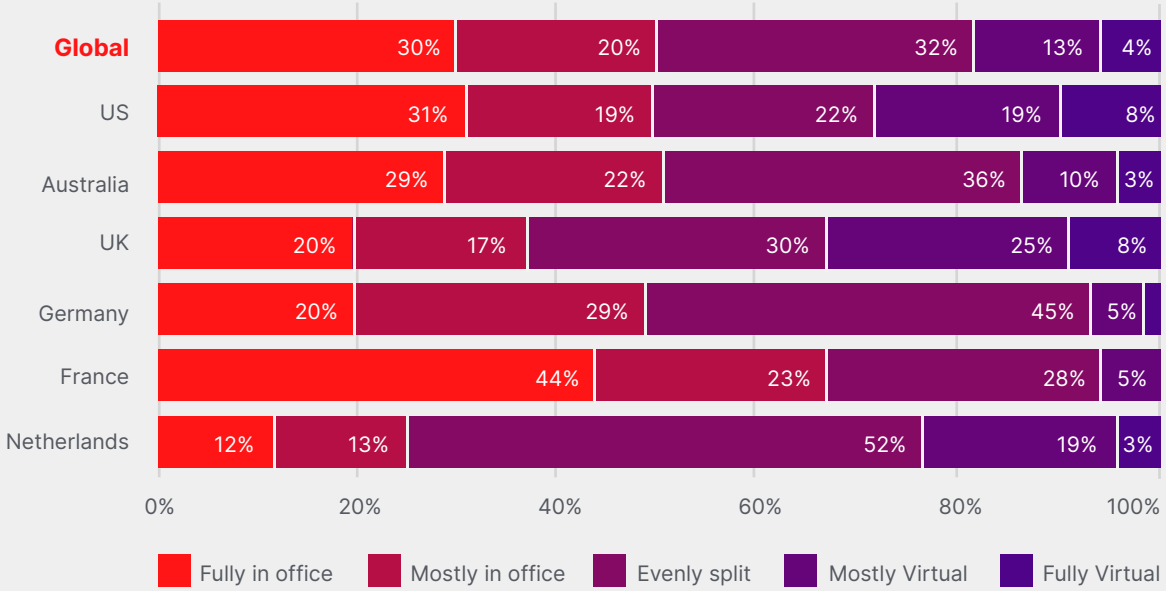
Why the all-out urgency?

It's not only the new modes of attack and high-profile government directives. The very nature of work inside government agencies has changed dramatically in just a few years — without any of the advance planning that would typically precede such a drastic shift. Hybrid working has opened up yet another frontier of vulnerability.

New reality

70% of government employees are working virtually at least some of the time

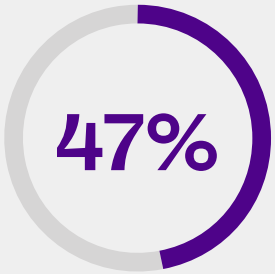
Q: Which of these answers best describes the way people with desk jobs at your organization work?



**Country results may not add to 100% due to rounding errors*

New risks

A proliferation of devices, users and locations adds complexity and new vulnerabilities



of security professionals worldwide say they don't have high visibility into every user, device, application and service on their networks.

of government workers surveyed use the same or similar passwords across multiple devices.

Inside:

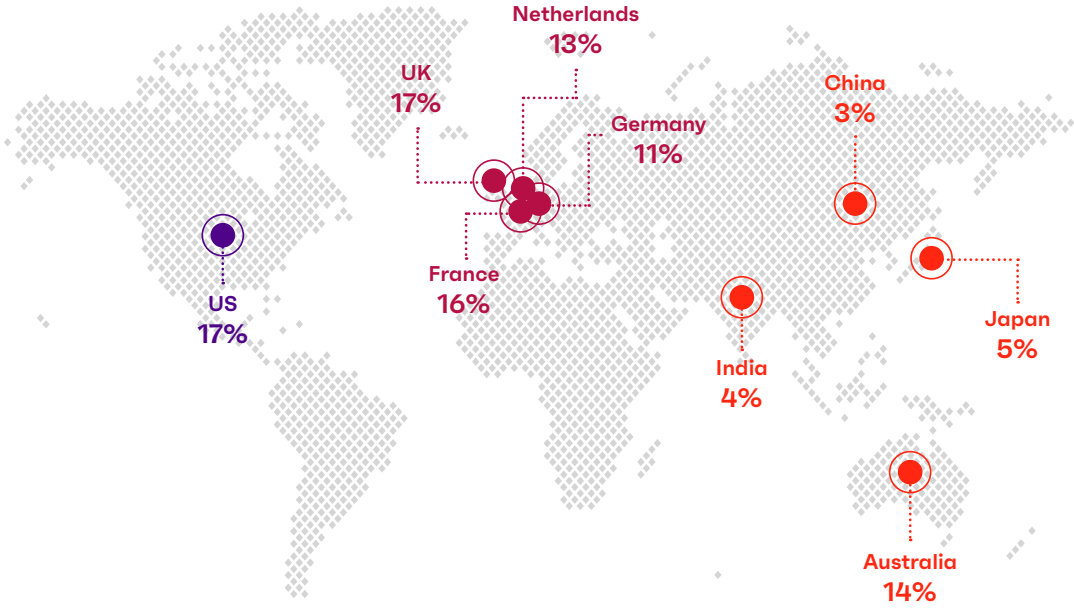
ivanti

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, as originally published in *Press Reset: A 2023 Cybersecurity Status Report.*

Insights collected here are based on responses from a subset of that study: office workers working in government around the globe (803 total), as well as cybersecurity professionals from multiple industries.

Surveyed government employees (n=803)



01

No “Culture of Accountability”

ivanti

Problem Today

A “not my job” attitude compromises government cybersecurity

Employee disengagement is a real security risk for organizations. Engagement and satisfaction scores in the public sector lag behind those of private sector employees by 15 points, according to the Partnership for Public Service.[1]

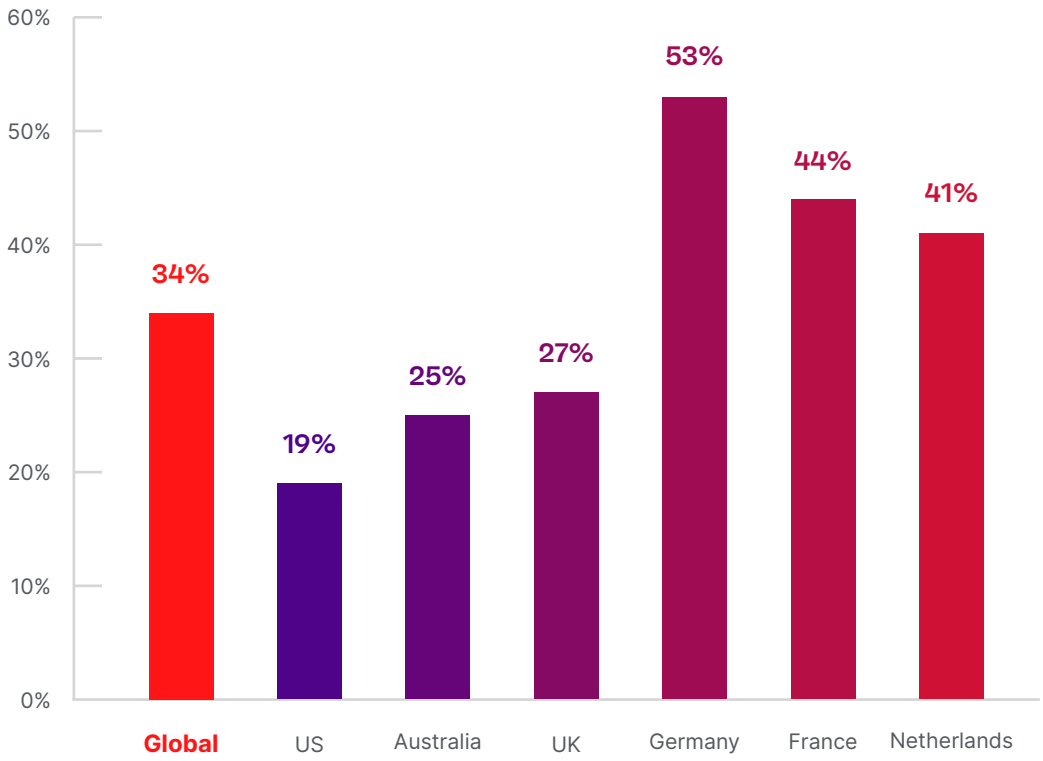
And low engagement means employees don’t feel connected or accountable to the wellbeing of the larger organization.

Ivanti’s research data bears this out: A large share of government employees around the world think their actions don’t matter when it comes to security.

In the UK, 27% of government employees say their actions don’t impact their organization’s ability to stay safe from cyberattacks; in Germany, the ratio rises to 53%.

Do employees think their own actions matter?

Q: Do you believe your actions impact your organization’s ability to stay safe from cyberattacks?



“My actions do not impact my organization’s ability to stay safe from cyberattacks.”

Not all government workers report suspicious activity

17% don't feel safe reporting a security mistake they've made at work to the cybersecurity team.

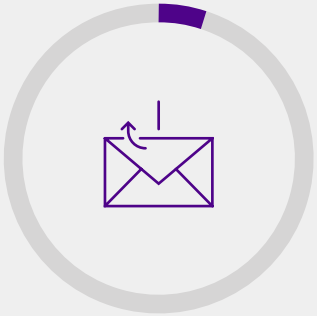
36% did not report a phishing email they received at work.

21% say they don't care if their organization gets hacked.

Government workers get phished – a prelude to cyberattacks

30%

say they've been a target of phishing.



5%

have fallen victim to a phishing attempt — either by clicking a link or sending money.

Why It Matters

A perfect cybersecurity storm approaches every government organization

Multiple, effective threat vectors

The public sector is particularly vulnerable to attack due to the size and value of the target. In the last year, hackers from state-sponsored persistent threats such as APT29 have all proved formidable, fast-evolving foes.[2]

Fast-evolving “synthetic” digital content

Generative AI has made phishing emails “picture perfect” — personalized to the vulnerabilities of each individual target.[3]

Even more alarming: Deepfakes pose a threat to the credibility of journalism and democratic elections worldwide.[4]

Budget constraints and organizational silos weaken security efforts

The US Government Accountability Office (GAO) says 60% of its cybersecurity recommendations have not been implemented over the last decade.[5]

A significant share of disengaged employees

The average US federal employee engagement stands at 64.5 out of 100 — 14 points behind the private sector.[6]

72%

of government employees have never contacted security to ask a question or voice a concern.

ivanti

Take Action

Make security a shared responsibility with all employees

Security leaders can't compel employees to care about cybersecurity, but they can influence employee attitudes over time by investing in and nurturing a positive security culture.

What makes a positive security culture?

Open

Employees feel comfortable asking the security team questions

Integrated

Security accountability is shared; every last employee has a role to play

Safe

Employees feel safe reporting incidents or errors

Iterative

Training is frequent, iterative and compelling

Strategic

Security is an asset — a key to the organization's success

Next Steps

Audit, involve and optimize your employees' experiences for a positive security culture

1

Audit

Survey employees to define your baseline and document current behaviors and attitudes. The findings will help identify your organization's specific weaknesses and inform a practical roadmap for change.

2

Involve

Engage with organizational leadership to get their support and buy-in. Leaders not only set the tone, but they also represent one of your biggest areas of risk.

Read more about leaders' risk to cybersecurity on page 19 ("Whalephishing 101 in government organizations").

3

Optimize

Culture change is never "one and done." It's an ongoing process that requires monitoring key performance metrics, listening to employees and making course corrections when needed.

ivanti

02

Password (Mis)management: Security's "Ground Zero"

ivanti

Problem Today

Poor cyber hygiene — including bad password habits — haunts government agencies

Security experts have been sounding the alarm on password risk for more than a decade, but most organizations — including government agencies — may still take a lax approach to password management. Ivanti's research uncovered a wide range of bad habits from our government respondents.

ivanti

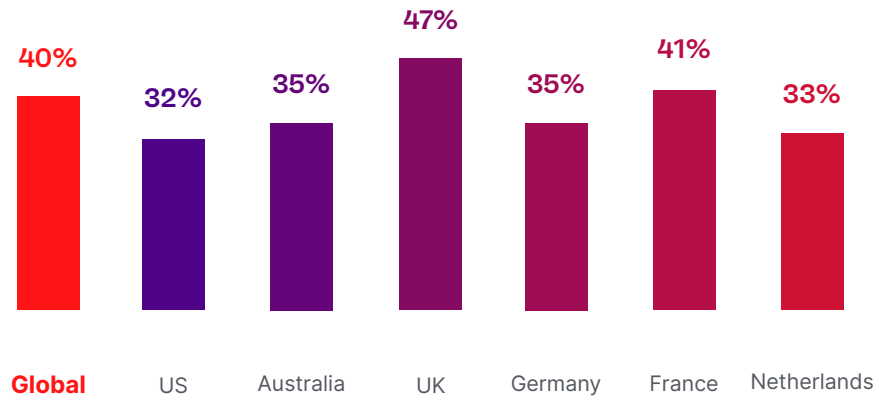
Government password access misdeeds

of government employees admit to accessing sensitive information they didn't require for their job duties.

1 in 3

say they believe their passwords at old jobs still work.

Percentage of government employees who use the same work password for longer than a year



Why It Matters

The push and pull of security versus convenience

So-called “shadow IT” and other workarounds are the enemy of secure organizations. When employees find a security measure inefficient or burdensome, they’ll find a way around it that is decidedly not secure.

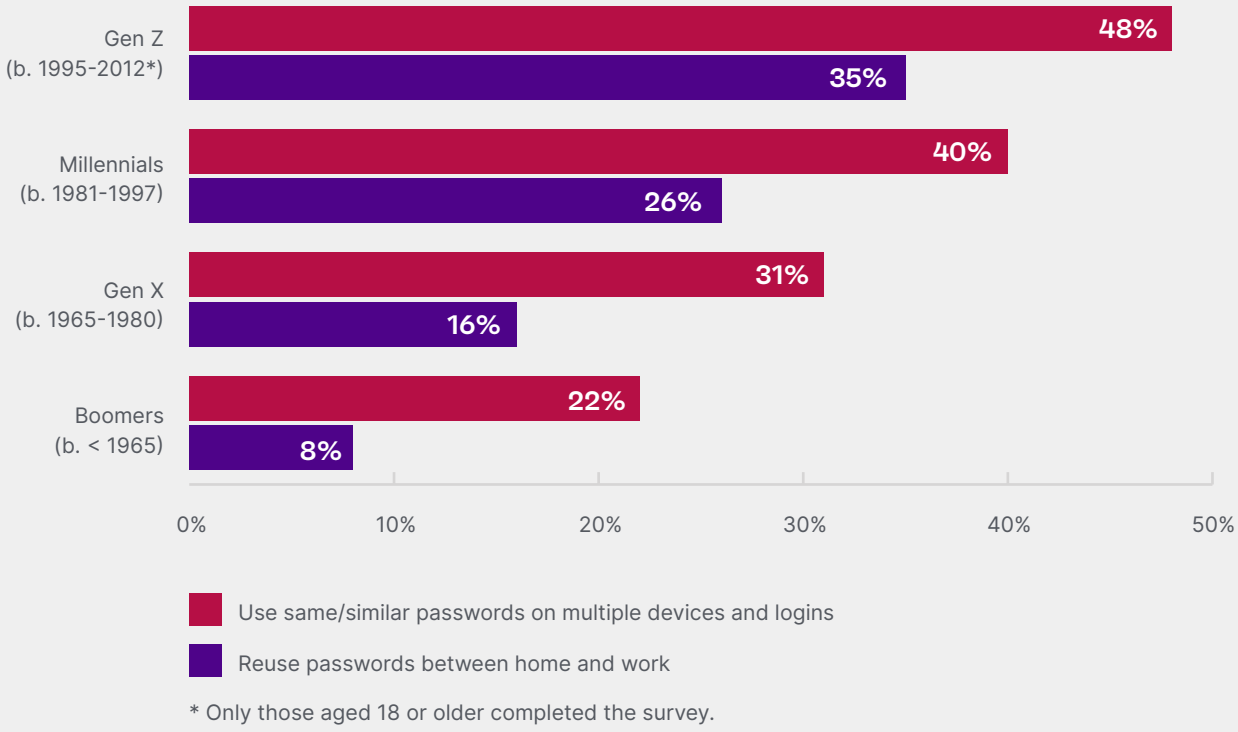
Passwords are ground zero for employee security workarounds. Employees in all industries continue to use sticky notes, pet names, birthdays and the universally favorite unbreakable code: “12345.”

Government organizations need security solutions that are so convenient — so effortless — that employees don’t seek ways around the so-called solution.

The myth of “digital natives”

Think your younger employees are more savvy about password security? The data doesn’t back it up.

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



* Only those aged 18 or older completed the survey.

Take Action

Invest in digital employee experience (DEX) for greater security

Security teams should evaluate new policies or technologies through the lens of digital employee experience, or "DEX," asking themselves, "Will the end-user experience encourage workarounds or other inadvisable behavior for the sake of convenience — and if so, is that risk worth it?"

Next Steps

Implement user-friendly experiences while enforcing security

1 Zero in on the high-hazard workarounds

- Employees sidestep security in the name of convenience
- High-profile leaders request exemptions to security rules

2 Prioritize DEX-focused technology

- Achieve user-centered experiences (less friction = greater compliance)
- Remove human agency when possible
- Lock down exemptions

Real-World Repercussions:

Zero Trust architecture (ZTA) implementations & DEX considerations

Whether using two-factor authentication, tokens or biometric data, organizations and agencies alike should prioritize – and commit to – a least-privileged access model for all employees, following a Zero Trust architecture (ZTA) strategy.

Under ZTA, security and IT solutions work together to continuously verify security posture and compliance by providing only as much access for any given employee as required.

Among other security benefits, this limited access ensures an agency's security while allowing for flexible working arrangements.

After all, if an employee succumbs to a phishing attack, then the threat actor can only access the limited options available to the employee.

However, ZTA can prove excessively cumbersome for day-to-day operations (for employees) and maintenance (for IT staff), encouraging use of shadow IT and erasing any benefit of ZTA.

Therefore, agencies considering ZTA should leverage:

- Strategic automation for unknown device notifications, suspicious behavior alerts and user privilege access timeouts.
- IT playbooks and decision trees for permission requests and common queries.
- Intuitive, easily accessed instructions for end users to "help themselves" before submitting an IT ticket.

Additional Resources for ZTA and DEX

NIST Special Publication 800-207 ("Zero Trust Architecture")

The NIST Cybersecurity Framework (CSF): Mapping Ivanti's Solutions to CSF Controls

The 2022 Digital Employee Experience Report

Getting Started with DEX: Core Areas of Focus to Deliver a Great Digital Employee Experience

Employee Experience in the Age of the Everywhere Workplace: Why IT Needs to Lead the Charge

03

Training for All: Government's Human-Sized Cybersecurity Gaps

ivanti

Problem Today

Uneven cybersecurity training strains government defenses

Security and automation technologies provide powerful frontline protection — but training employees to be your company's security eyes and ears is a critical secondary defense. Ivanti's research shows training in the public sector simply isn't reaching everyone.

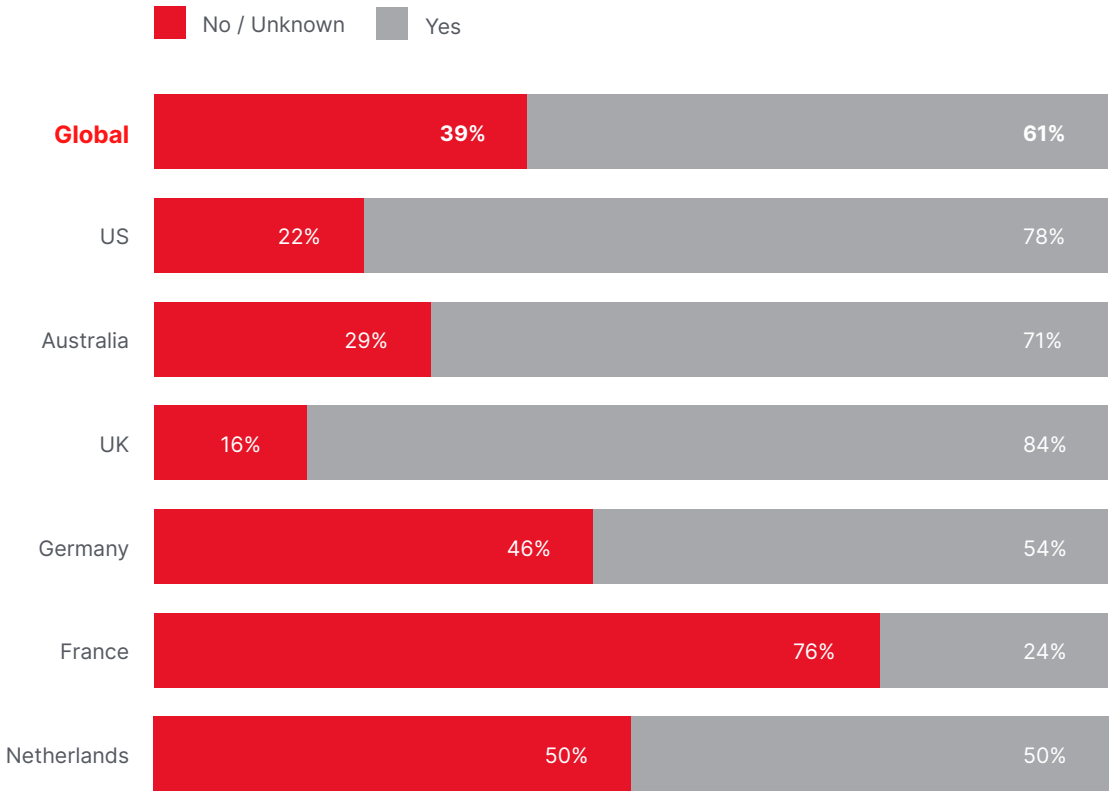
27%

Just 27% of government workers feel "very prepared" to recognize and report threats like malware and phishing at work.

ivanti

Training for all? Not even close.

Q: "Does your organization provide mandatory cybersecurity training?"



Why It Matters

Government workers and contractors report little or ineffective training, despite mandates

The 2023 *Press Reset* global study of security professionals worldwide found that a significant share of organizations fall far short in educating and training employees about cybersecurity risks and reporting processes.

And it only takes a single person making a single misstep to cause unintentional but catastrophic damage — and within government agencies, that damage impacts every supported constituent.

32%

of security professionals say ineffective or incomplete employee training is a significant barrier to cybersecurity excellence at their organization.

29%

of organizations worldwide don't require partners and/or vendors to complete cybersecurity training — an exposed position for government agencies with third-party contractors.

Insights from
Press Reset: A 2023 Cybersecurity Status Report

Real-World Repercussions:

“Whalephishing 101” for government organizations

Whalephishing involves socially engineered communications to high-value, high-risk targets, or “whales.” Common whalephishing targets include division leaders, public figures and finance chiefs – or even their assistants or administrative personnel within a desirable division.

By tricking the target into believing the communication is genuine, threat actors can then gain credentials, sensitive information or even fraudulent wire transfer authorizations.

Such access is often undetected and unreported for extended periods of time, allowing advanced persistent threats (APTs) to lurk within government networks for months… or even years.[7]

And research shows that the very people with the highest levels of access to sensitive information and networks frequently exhibit the poorest security habits.

Leadership-level employees are more likely to practice unsafe security behaviors than other workers

More than 1 in 3 leaders have clicked on a phishing link — four times the rate of the average office employee!

Nearly 1 in 4 leaders use easy-to-remember birthdays as part of their passwords.

Leaders are much more likely to hang on to passwords for years than other workers – in fact, 1 in every 4 surveyed leaders do so.

Leaders are five times more likely to share their passwords with people outside the company.

*These statistics apply to leaders across industries, including the public sector, as drawn from *Press Reset: A 2023 Cybersecurity Status Report.*

Take Action

Enforcing training across all government employees lowers security risks while improving attitudes

One of the best ways to reach sensitive information accessible by “whales” (or any privileged user) can be through the employees who work alongside them:

- An influential administrative assistant.
- The new hire sitting at the front entrance.
- Expert third-party contractors visiting for the day.

Even if these personnel do not officially have direct access to private information or storage, bad security habits born of convenience — and proximity to high-value targets — offer easy access to an agency’s most sensitive information and material.

The best security training delivers both...

What

Specific types of attacks, and how to recognize and repel them.

Why

The critical role each employee plays, no matter their title, role or location.

Next Steps

“Training for all” without a “one size fits all” mindset

1

Train ambassadors

Develop highly trained “security ambassadors” — people who don’t work in security but have an interest in it.

2

Pay special attention for high-risk employees

Identify your high-risk segments and develop a custom curriculum for each one — focusing on realistic scenarios for a given government agency based on recent threats.

3

Make it positive

Make training events memorable. Lecture-style training has a place, but also consider competitive activities or “gamified” scenario planning.

ivanti

04

Futureproofing Government Organizations

ivanti

Problem Today

Legacy systems, tech stack complexity, data silos, talent shortages … should we go on?

Many assume that governments — big cities, federal agencies, military agencies or public works — must have cybersecurity all figured out.

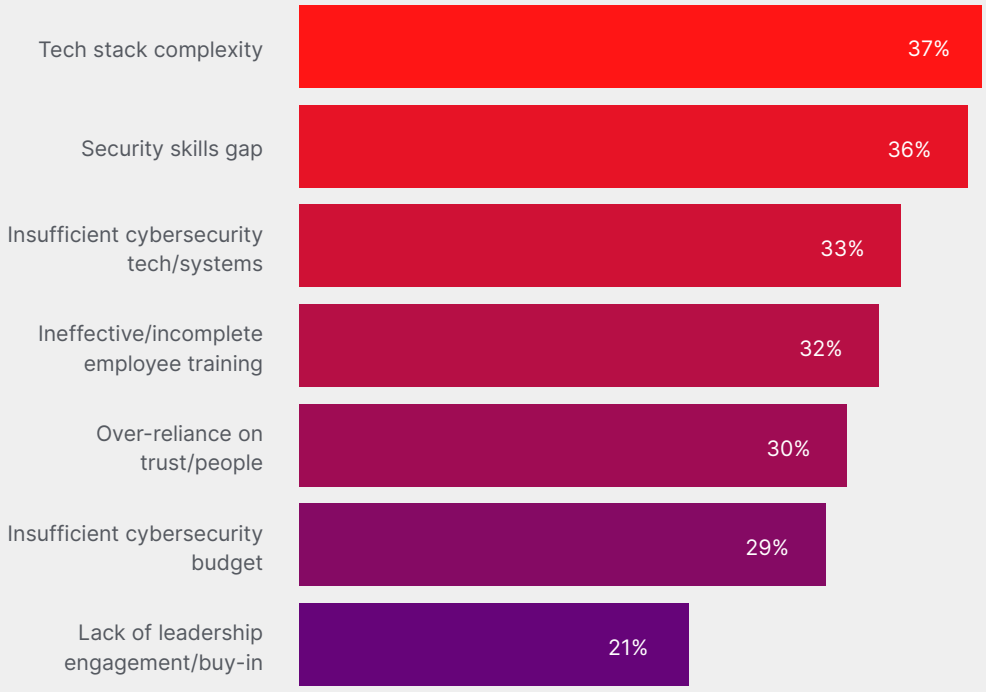
(After all, some of the most advanced cybersecurity talent and technology reside in military departments and applications!)

In reality, most governmental organizations lack sustainable funding to invest in:

- Talent
- New technology
- Training
- Culture

Most commonly reported barriers to global cybersecurity excellence

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



Insights from *Press Reset: A 2023 Cybersecurity Status Report*

Why It Matters

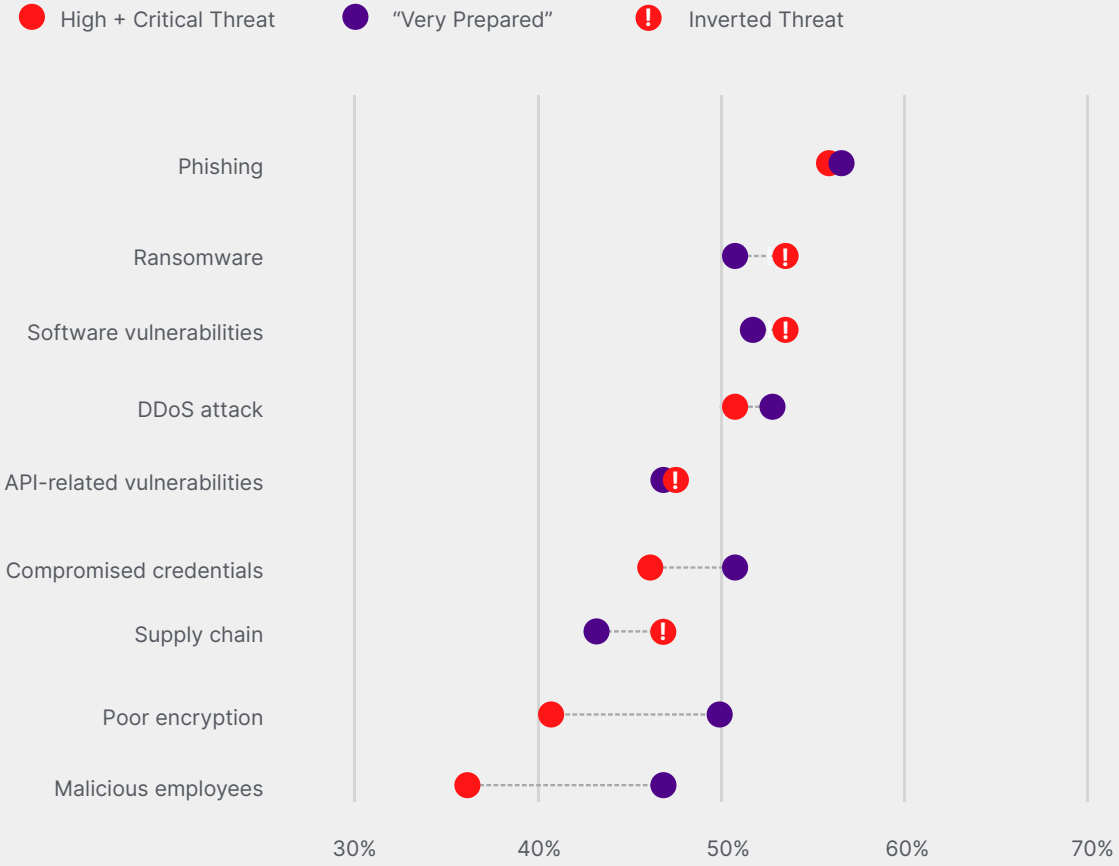
Threat actors continue to advance their weapons against old defenses

According to a report from the US Government Accountability Office (GAO), the US federal government still has not implemented more than half of the recommendations from the GAO since 2010.[8]

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?

Security threats versus security preparedness



Insights from *Press Reset: A 2023 Cybersecurity Status Report*

Real-World Repercussions:

Public sector remains exposed to state-sponsored hackers

The public sector is particularly vulnerable to attacks from state-sponsored cybercriminals, who will move against any related (no matter how distant) agency.

For more context on other active threat actors beyond the three featured to the right – as well as their methodologies, exploited vulnerabilities and publicly known government attacks – please read the complete *2023 Cyberstrategy Tool Kit*.

"Our energy, healthcare and financial systems [...] all face cyber risks from malicious actors. Attacks like these could cause serious harm to people, our environment, national security and most importantly our economy."[8]

Marisol Cruz Cain
Director, GAO Information Technology and Cybersecurity Team

Select advanced persistent threats (APTs) **and cyber gangs** attacking global governments include:

ALPHV

A cybercriminal gang responsible for creating, selling, and deploying a "ransomware as a service" model, or RaaS. Off-the-shelf hacking solutions like these empower a wide range of threat actors.

APT29

State-sponsored hackers connected to Russia's foreign intelligence service dedicated to espionage and intelligence activities.

Conti

A Russian-associated threat actor that dissolved after its playbook was leaked — but Conti-affiliated hackers and code are now rogue threats. Conti-style ransomware tactics were still evident in multiple cybercriminal gangs in the last year.

Take Action

Battle misinformation and accelerated attacks through strategic technology and culture

We live in a world where misinformation is power:

- Bot-powered social media misinformation campaigns at scale
- Highly believable phishing attacks, tuned to individual preferences
- Deepfakes that undermine independent journalism and disrupt elections
- Ransomware that interrupts global logistics and healthcare delivery

All of these can wreak havoc on public safety, global commerce and diplomacy — and even cost lives. Government organizations are particularly vulnerable, because they hold the keys to systems and messages that bad actors want to disrupt and exploit.

Security leaders must protect their positions by operating with precision: developing strategies, systems, tools, training and governance that work in concert to keep out bad actors.

And it's critical to build out these defenses in comparative "peacetime" too many organizations take critical steps after a catastrophic attack.

The time to act is now.

Next Steps

Futureproof your tech stacks

1

Resilience

Design react-and-recover plans to shorten outages and limit knock-on effects.

2

Automation

Deploy automation to boost asset visibility and deploy a risk-based prioritization to patching — both table stakes for secure organizations in 2023.

3

Empowerment

Give the cybersecurity team more independence and budget to set the security agenda — no more thoughtless reactions to the latest threat to hit the news.

4

Holistic risk management

Think about security beyond government walls — from work-from-everywhere (WFE) and hybrid employees, to third-party contractors and vendors.

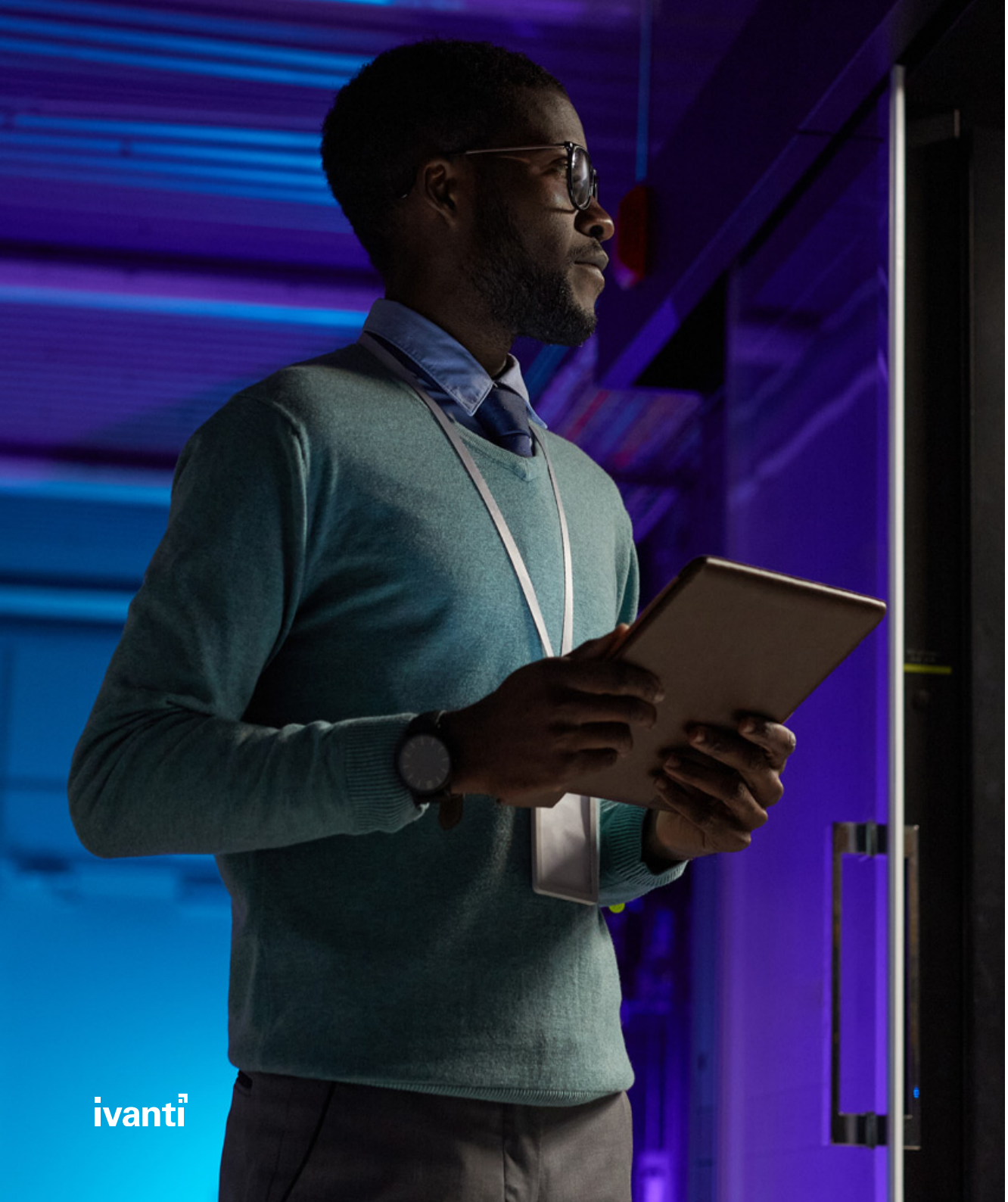
For more information:

Press Reset: A 2023 Cybersecurity Status Report

The scale and urgency of the situation requires government organizations to approach cybersecurity as a team effort – and augment that effort with technology that doesn't place additional burden on workers.

The security posture of governments and agencies will be strengthened when cybersecurity is an issue all employees understand, care about and feel accountable to – coupled with proactive security measures that enable a better employee experience.

ivanti



References

1. Partnership for Public Service: “Engaging employees at federal agencies,” July 14, 2022. https://ourpublicservice.org/blog/engaging-employees-at-federal-agencies/

2. Ivanti: “2023 Cyberstrategy Tool Kit for Internal Buy-in.” October 2022. https://www.ivanti.com/resources/v/doc/ebooks/ivi-2702-cybersecurity-tool-kit-internal-buy-in-budget-influence-non-infosec

3. Sharon Ben-Moshe, Gil Gekker, Golan Cohen / Check Point Research: “OPWNAI: AI That Can Save the Day or Hack It Away.” Dec. 19, 2022. https://research.checkpoint.com/2022/opwnai-ai-that-can-save-the-day-or-hack-it-away/

4. VOA: “Research: Deepfake ‘News Anchors’ in Pro-China Footage.” Feb. 8, 2023. https://www.voanews.com/a/research-deepfake-news-anchors-in-pro-china-footage/6953588.html

5. U.S. Government Accountability Office: “Cybersecurity High-Risk Series: Challenges in Protecting Privacy and Sensitive Data,” Feb. 14, 2023. https://www.gao.gov/products/gao-23-106443

6. Partnership for Public Service: “Employee Engagement,” July 13, 2022. https://ourpublicservice.org/our-solutions/employee-engagement/
Federal News Network: “Return-to-office plans a major cause for decline in 2021 Best Places to Work results,” July 13, 2022. https://federalnewsnetwork.com/workforce/2022/07/return-to-office-plans-a-major-cause-for-decline-in-2021-best-places-to-work-results/

7. Ivanti: “2023 Cyberstrategy Tool Kit for Internal Buy-in.” October 2022. https://www.ivanti.com/resources/v/doc/ebooks/ivi-2702-cybersecurity-tool-kit-internal-buy-in-budget-influence-non-infosec

8. U.S. Government Accountability Office: “Cybersecurity High-Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight,” Jan. 19, 2023. https://www.gao.gov/assets/gao-23-106415.pdf

Government Cybersecurity Status Report

4 Important Ways to Take Action and Drive Change in 2023

ivanti

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