The Shadow IT Report

September 2023

dimensional research | KOLIDE

Introduction

Security has an unmanaged device problem

The post-COVID world has seen an enormous and persistent rise in cyber attacks. At the root of many of these attacks are employees, whether through phished credentials or compromised devices; bad actors or honest mistakes.

Organizations that wish to protect themselves from these breaches are dedicating significant resources to security, most recently with the adoption of Zero Trust architecture.

But despite employers' investments in Zero Trust, they have alarmingly low visibility into much of their employees' activity, which takes place on personal and unmanaged devices.

Employees regularly break security policies in ways that are totally invisible to security and IT teams. But employees don't deserve all the blame.

Zero Trust is a security framework based on restricting access to an organization's resources based on a user's identity and security posture.

Lack of transparency is a two-way street.

Organizations often fail to communicate their policies and expectations with their employees, creating an atmosphere of ignorance and mistrust.

In a nutshell: employees disregard policies because they don't know what they are, don't understand why they're important, or prefer to work around tools they feel are invasive.

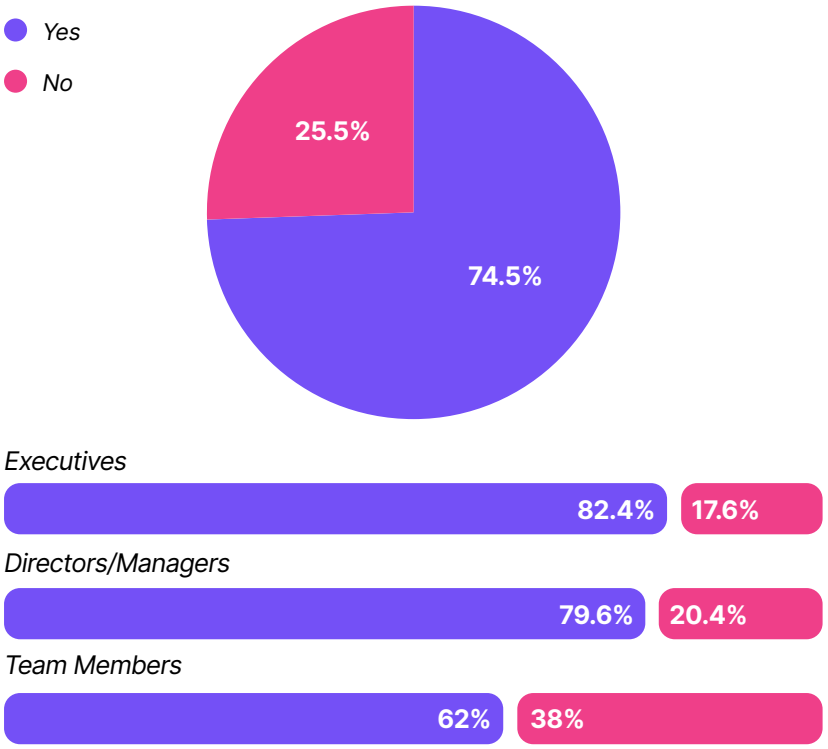
This lack of transparency is particularly dangerous when responding to emerging threats like AI. Executives vastly underestimate AI usage, and have failed to communicate the risks of such tools.

We surveyed over 300 knowledge workers—including executives and security professionals—to study their behaviors and beliefs. This report shows where and how communication is breaking down within organizations and how Shadow IT threatens security.

75% of the workforce does work on non-company owned devices

The overwhelming majority of workers use personal devices to access their company's applications and data. This behavior can be found in every role and at every level, although we do see that executives and managers are more likely to use personal devices than frontline employees.

"Do you ever do company work on personal devices?"



Defining personal devices: Throughout this survey, we asked about personal, rather than unmanaged devices. We chose this wording in order not to confuse non-technical respondents who may not have a clear idea of what device management entails. (That concern seems to have been correct, since in the one question where we did ask about managed devices, non-technical users' answers deviated wildly from those of IT, security, and developers.)

It's safe to assume that some percentage of these personal devices have management software installed. But the rest of our data shows that plenty of companies allow totally unmanaged devices to access their resources.

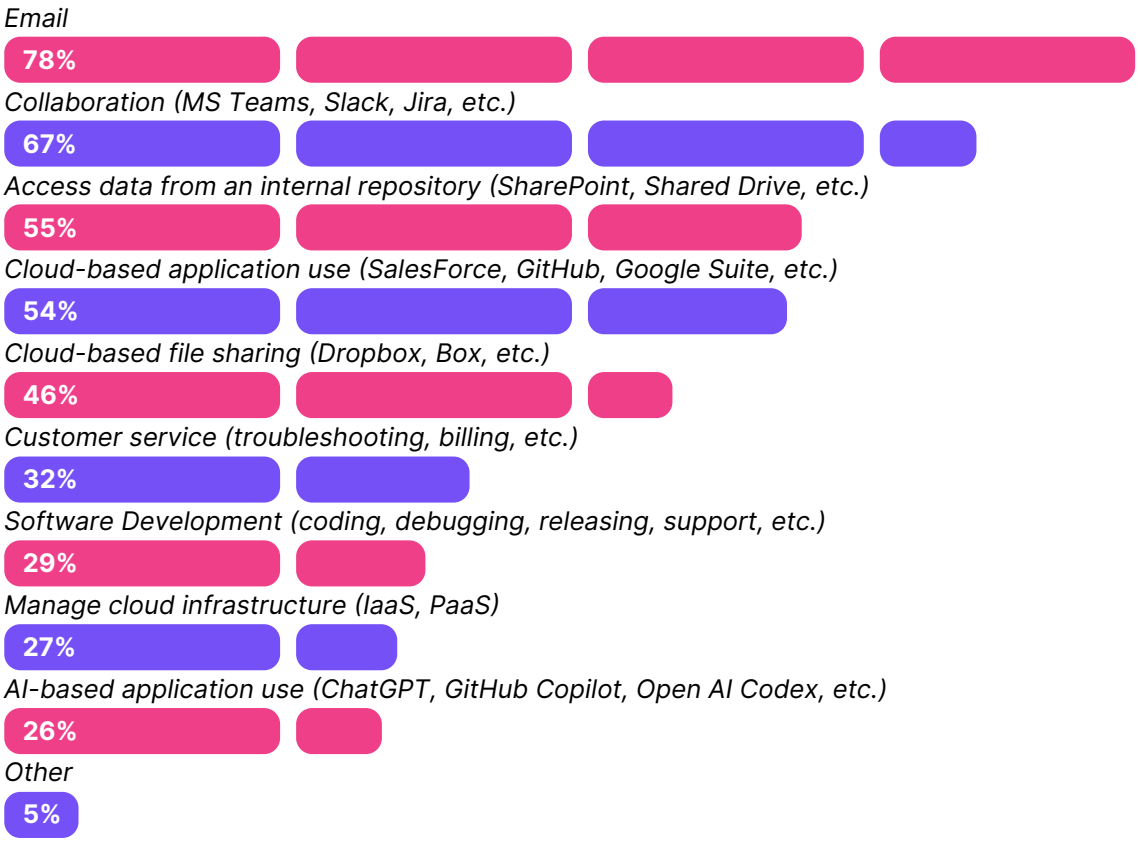
It's not just phones

When most people hear about "personal and unmanaged devices," they think of employees checking email and Slack on their phones. Companies often tolerate unmanaged phones since apps like Slack are considered low-risk (which is incorrect), and employees are reluctant to install management software on the same device where they keep their photos and text messages. So it's not surprising that email and other collaboration tools led the pack when we asked what people were doing on their personal devices.

But the problem goes much further than phones. For every behavior we asked about, a significant number of employees were doing it on a personal device. That data comes into sharper focus when you separate it by role. **For example, 49% of developers reported doing software development on personal devices, and 35% of security professionals use them to manage cloud infrastructure.**

When engineers do production-level work on personal devices, an organization's risk of a breach skyrockets. A bad actor can use a security flaw in an unmanaged device to break into the production environment, as in the LastPass breach. Even a simple smash-and-grab of a laptop can turn into a nightmare if that laptop is full of PII, and IT has no way to remotely wipe it.

"What type of work tasks have you done on your personal device?"



Nearly half of companies let unmanaged devices access protected resources

Personal and unmanaged devices introduce serious security risks. They can be infected with malware, employ unapproved Shadow IT, or, in the worst case scenario, belong to a bad actor using phished credentials.

"Does your company ONLY allow "managed devices" to access company resources?"

- *"Yes, only managed devices can access company resources"*
- *"No, with proper credentials (usernames, passwords) any device can access company resources"*
- *"No, any device can access company resources even if it doesn't have proper credentials (usernames, passwords)"*

Zero Trust security requires organizations to restrict access to resources based on:

1. Establishing a user's identity with a high degree of confidence
2. Establishing a device's identity and security policy

This data shows that 47% of companies can't accomplish either of those goals. Allowing users to authenticate on any device means that not only are employees authenticating on their unmanaged personal devices, it means that bad actors can impersonate them with phished credentials.

The typical tech stack can't stop unmanaged devices

The most commonly-used security tools have no solution for unmanaged devices. MFA only checks user identity, not device identity. VPNs can be downloaded onto personal devices, and many SaaS apps fall outside them.

"Which of the following security tools does your company use?"

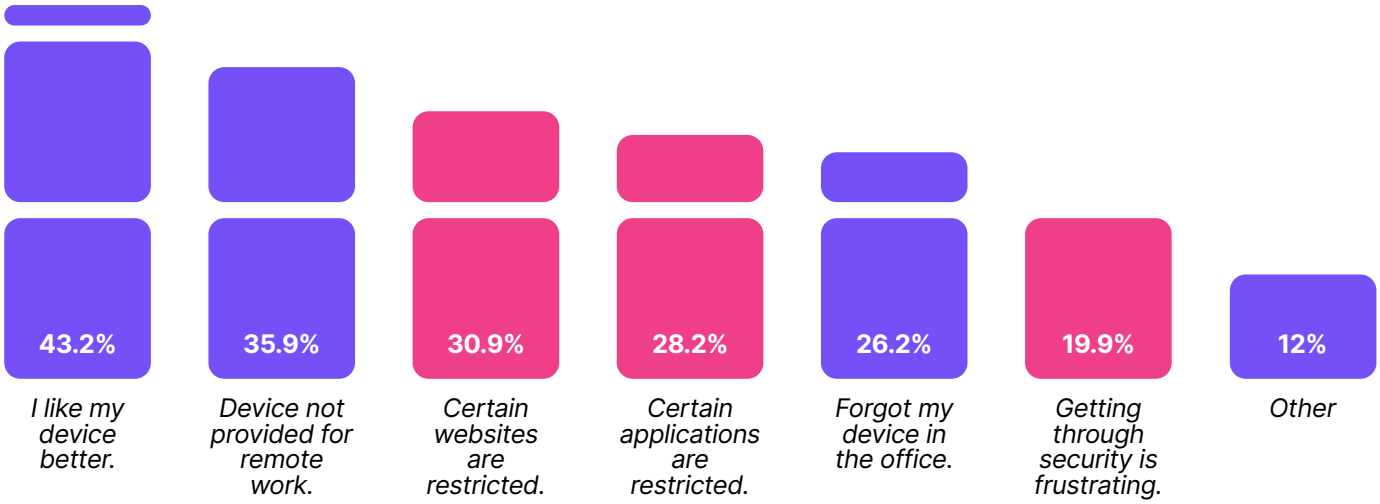
While use of mobile device management (MDM) solutions and biometrics were surprisingly low, many companies have invested in security tools that can feel invasive, such as web browser monitoring. As we're about to see, a desire to escape such tools is why many employees use personal devices in the first place.

Why workers use personal devices

Three of the top six reasons relate to avoiding security requirements.

In other words: employees are consciously using Shadow IT to get around their organization's security policies, which means the policies themselves aren't working.

"Why do you use personal devices to do company work?"



Surprisingly, security professionals were the most likely to report that they used their personal device because getting through security measures was frustrating.

Other common justifications include personal preference, while others report not having a company-issued device, or not having one that lets them work remotely.

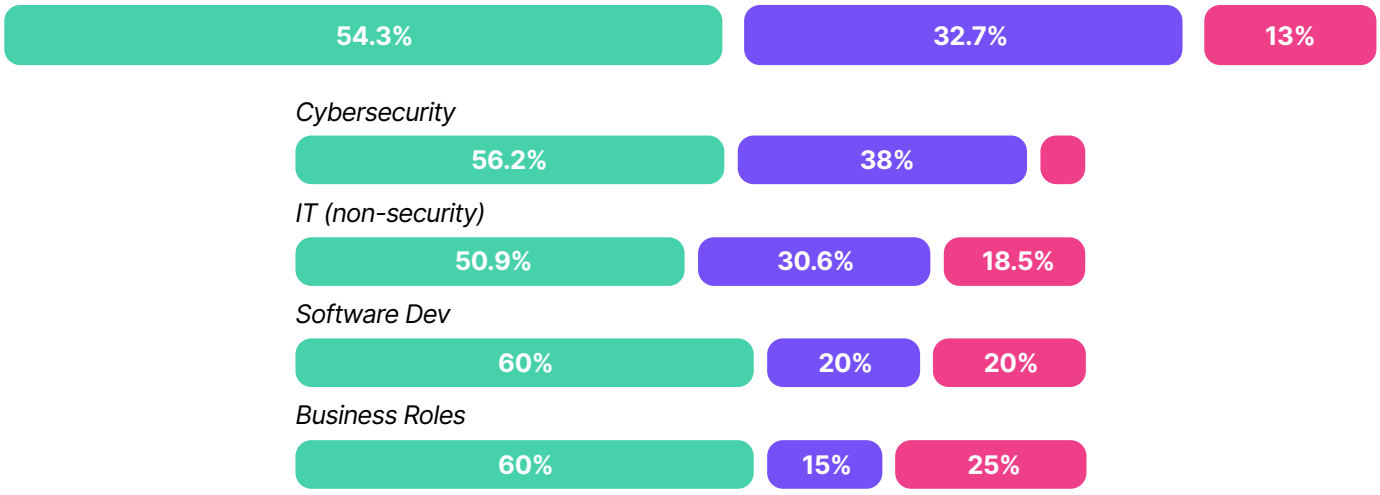
Employees are often kept in the dark about security

Clearly, employees deliberately going around security policies isn't good, but they may be justified in being paranoid, since only 54% of companies fully disclose their use of security tools to their end users.

— *"Are end users informed about all the user-facing security tools your company uses?"* —

- *Yes, we tell users about ALL user-facing security tools*
- *We only tell users about SOME user-facing security tools*
- *No, we don't tell users about user-facing security tools*

All responses



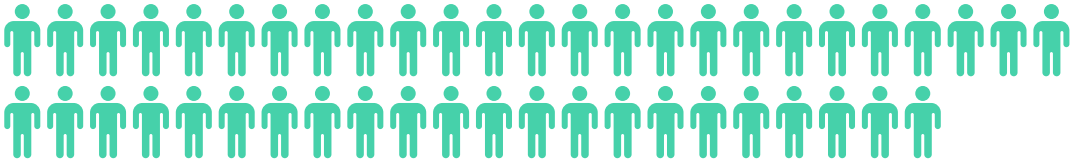
The harm done by this lack of transparency is clearest when we compare the answers of cybersecurity professionals with employees in business roles. Security teams—who know the most about the organization's policies—are the most likely to acknowledge that they only inform their colleagues about some user-facing tools. But very few (5.8%) report not telling employees about security tools at all.

Meanwhile, a full quarter of workers in business roles report that they are not informed whatsoever. It's not clear if these workers are simply poorly informed about security, or if this answer reflects paranoia that their organization is observing them without their knowledge.

Less than half of workers attempt to follow all cybersecurity policies

— *"What is your general approach to adhering to your company's cybersecurity policies?"* —

(47%) *"I always follow all the cybersecurity policies."*



(43%) *"I typically follow our cybersecurity policies but sometimes I have to go around them."*

(7%) *"I know what our cybersecurity policies are but typically ignore them."*

(2%) *"I don't know what our cybersecurity policies are."*

(1%) *Prefer not to say*

These trends hold true across demographics, including executives (52% "always follow") and security professionals (47%). Unfortunately, we don't have data on which specific policies respondents felt justified in going around, but we can make two inferences from this response:

1. Any security policy that workers can ignore at will does not have adequate safeguards around it.

2. If workers who generally try to follow the rules ignore a security policy, either they don't understand the risks associated with a specific behavior, or the policy itself is flawed.

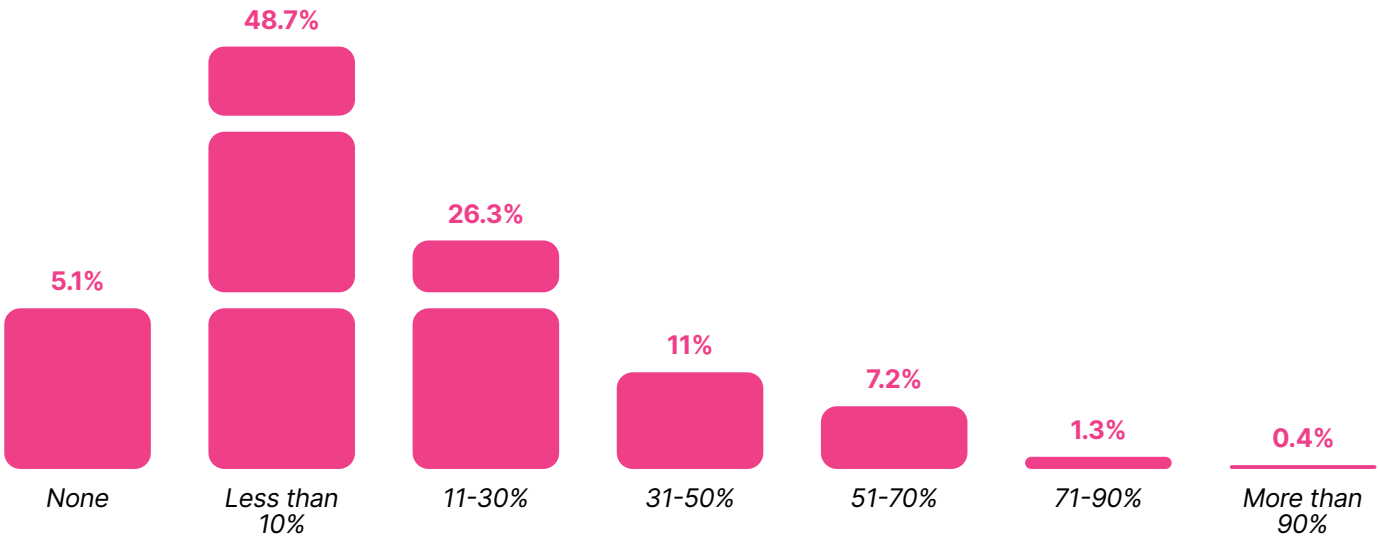
Workers badly underestimate their colleagues' AI use

To show the effects of a siloed, opaque security culture, we wanted to drill down into usage of a specific technology. And there's no better (or more timely) example than AI tools, whose promise and peril are still poorly understood.

What we found is that most workers, including managers and executives, assume that AI use is still relatively rare in their workplace. Roughly half of all respondents believe that less than 10% of their colleagues use AI.

This estimation is staggeringly incorrect.

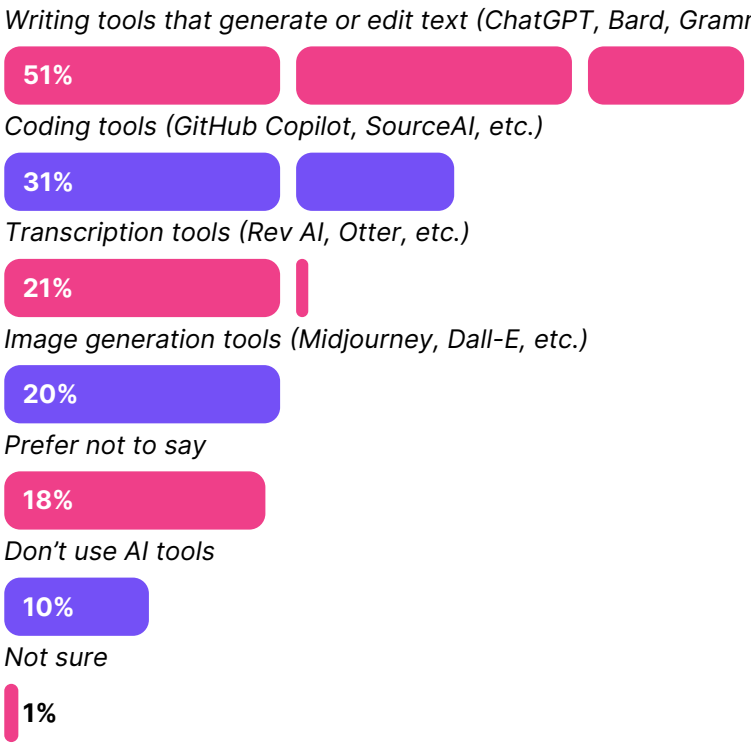
"In your estimation, what percentage of your company's employees use AI-based applications for work-related tasks?"



89% of workers use AI-based applications

Contrary to their colleagues' beliefs, the vast majority of workers reported using some form of AI at least once a month.

"Regardless of your company's AI policies, which of the following types of AI-based applications do you use for work at least once a month?"



However, AI use is not spread evenly throughout the organization. In all the categories of AI-based tools we asked about, executives and managers reported significantly higher use than frontline workers.

	Executives	***Directors/Managers***	***Team Members***
Writing tools	67.5%	55.8%	34.7%
Coding tools	37.5%	38.4%	18.1%
Transcription tools	30%	26.7%	9.7%
Image generation tools	25%	27.9%	8.3%

Workers use AI without understanding its risks

So why is a security report talking about the disconnect between the assumed vs the actual use of AI in the workplace?

Because it shows that the people designing policies for the workforce don't understand how people are actually working. Without that understanding, organizations can't design security policies and provide education that addresses workers' habits, concerns, and needs.

"Has your company explained the security risks of AI-enabled applications to employees?"

AI tools pose serious risks for an organization on multiple fronts. They present legal issues when it comes to plagiarized text or code. AIs can expose sensitive company information, both by incorporating it into training data and through malware (malicious AI browser extensions and web applications proliferate wildly in this largely unregulated space.)

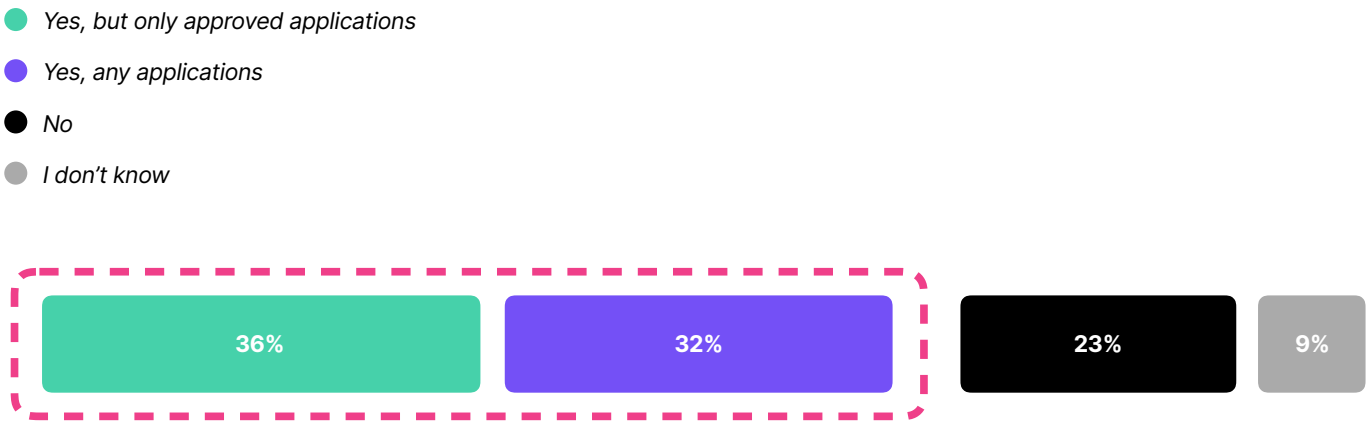
Yet barely half of companies have educated their workforce on these risks.

Most companies allow AI use

Meanwhile, 68% of respondents report that they are allowed to use AI at work. That's significantly less than the 89% of workers who say that they *do* use AI at work, so it's clear some people are using AI tools contrary to company policy.

But the 32% of respondents who are allowed use "any" AI application are also a security risk, given the prevalence of malicious (or at least dangerous) tools. And it's a largely invisible risk since employees can access sensitive data on personal devices. That means that sensitive data is getting out and AI-generated work is getting in without anyone realizing it.

"Are you allowed to use AI-based applications at work?"



68% of companies allow the use of AI-based applications, but only 56% explain their risks.

Security training is falling short, though employees overwhelmingly want it

"Security training is useless and everyone hates it" is a classic corporate truism.

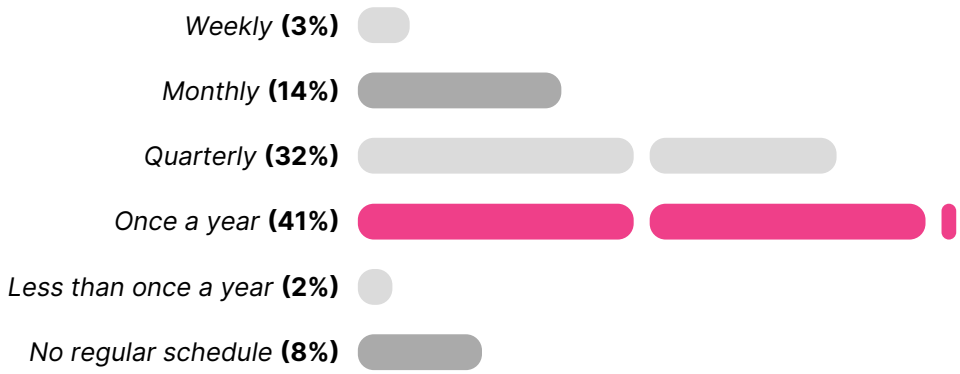
As it turns out, it's also a myth.

In the strongest data point of our survey, 96% of workers (across teams and seniority) reported that training was either helpful, or would be helpful if it were better designed. The message here is that people want to be educated on how to behave safely.

"Do you think the security training is effective?"

Despite the desire for security education, companies fail to make it a priority, often doing a single, annual training. This approach is almost inevitably a "check-the-box" exercise, and it means that education can't keep up with emerging threats.

"How frequently do you typically receive company provided security training?"



Conclusion

This report reveals the scope of the Shadow IT problem. Workers at every level and in every role are using hardware and software that are invisible to their employers. In large part, these behaviors are invisible because workers are allowed to work on unmanaged devices, which open the door to a myriad of security risks.

Some of this data leaves us with further questions, which we hope to answer in future editions of the Shadow IT report.

For now, though, we can make some initial observations. Let's start with the biggest one:

Unmanaged device usage is alarmingly common, and it puts company (and customer) data at risk.

That's not to say that it's feasible or desirable to mandate that employees can only work on company-owned devices. But it doesn't have to be a binary where the only options are "fully managed and locked down" and "totally invisible."

We need lighter touch device management options.

Security teams need to invest in management solutions that ensure that devices meet minimal security standards, but without making employees feel spied on or hugely inconvenienced. Also, the definition of "sensitive" likely needs to expand to include email and messaging apps, instead of excluding them just because so many employees access them on their phones.

Employers and workers need more open, honest dialogue about security.

Several responses to this survey point to a disconnect between how security policies are designed and how people actually do their jobs. When more than half of all workers admit to going around security policies, there's clearly a disconnect. But security and IT professionals can't get at the root of this problem without making an effort to understand why workers feel they have to go around policies. And they can't expect honest answers if they themselves aren't honest about the types of surveillance they're conducting. In trying to eliminate Shadow IT, it's vital not to drive people even further into the shadows.

Bottom Line: Unknown and unmanaged devices are Shadow IT and Shadow IT is incompatible with Zero Trust. To defeat it, you need to ensure that only secure devices can access your apps.

Methodology

The Shadow IT Report was administered by Dimensional Research in June 2023.

We surveyed 334 participants, all of whom had either IT, security, or business responsibilities that required to use of a computer or mobile device for a majority of their work tasks.

Participants by industry

Technology (software)	17%
Education	13%
Financial Services/Insurance	9%
Manufacturing	8%
Healthcare	8%
Government	7%
Services	6%
Technology (other)	5%
Retail	4%
Transportation	4%
Telecommunications	4%
Energy & Utilities	4%
Media & Advertising	3%
Non-profit	3%
Food & Beverage	2%
Other	5%

Participants by job duties

Cybersecurity	30.2%
IT (non-security)	28%
Business roles	25%
Software Development	16.8%

Participants by company size

100-1000 Employees	37.1%
1,000-5,000 Employees	49.4%
5,000-10,000 Employees	12.7%
> 10,000 Employees	0.7%

Participants by seniority

Directors/Managers	49.8%
Team Members	31.9%
Executives	18.3%

Participants by location

US or Canada	63%
Europe	26%
Mexico, Central or South America	3%
Australia or New Zealand	3%
Middle East or Africa	3%
Asia	2%

KOLIDE

About Kolide

Kolide is a device trust solution for companies with Okta. With our product, security and IT teams can conduct wide-ranging device posture checks on Mac, Windows, Linux, Android, and iOS devices. Devices deemed unsecure are stopped from authenticating with Okta. But rather than simply locking users out, Kolide provides them with rich remediation instructions, so they can understand why an issue matters, and how to fix it on their own.

Kolide was founded on the principles of Honest Security, and continues to operate on the belief that security is most effective when it respects end-user agency and privacy.

To learn more visit: kolide.com