ARCTIC WOLF

2024 REPORT

HUMAN RISK BEHAVIOR SNAPSHOT

An analysis of IT and cybersecurity leaders' attitudes alongside those of end-users in an evolving threat landscape.

TABLE OF CONTENTS

INTRODUCTION

Cybersecurity failures can be traced back to human behavior between 68%[1] -95%[2] of the time, studies suggest. Whatever the precise figure, it's high. High enough to convince anyone interested in building a secure organization to seriously examine how end users and IT and cybersecurity leaders think and behave.

Despite this, disproportionate expectations are placed on tools and technology. More and more solutions explode onto the cybersecurity market every year – without a similarly exponential rise in effectiveness.

The problem cyber insecurity poses is enormous. It's the fourth most severe global risk, ahead of interstate armed conflict, economic downturn, and pollution, according to the World Economic Forum[3].

Technology is chosen, implemented, and managed by people, so to ignore the human element in an organization's cybersecurity posture is a dangerous oversight.

Simply dismissing the issue as "human error" isn't helpful. Nor is a culture of blame, where employees are afraid to raise security concerns and IT and cybersecurity leaders hide breaches from the wider team.

We commissioned the Human Risk Behavior Snapshot to understand what beliefs people hold about their own organization's cybersecurity risk. Whether what people say in this arena matches what they do. And where the greatest opportunities lie to support IT and cybersecurity leaders and end users in protecting against breaches.

The better this topic is understood, the more quickly and easily we can put organizations on the right path to solve cybersecurity's effectiveness problem.

> *Your employees are a critical line of defense against breach attempts – but security isn't solely a staffing problem. Nor is it purely a tools issue.*
>
> *Effective security awareness has to be considered as a root and branch operational undertaking, encompassing culture, communication, technology, and training.*

Adam Marrè
CISO, Arctic Wolf®

KEY FINDINGS

of IT and cybersecurity leaders admit to **reusing system passwords**

of IT and cybersecurity leaders have at least once **disabled security measures** on their system

of IT and cybersecurity leaders are confident in their company's ability to deal with a cyber attack, unfortunately 64% **have experienced more than one breach** in the past 12 months

of IT and cybersecurity leaders have **terminated an employee for falling victim to a scam**

of IT and cybersecurity leaders say **their organization has an AI policy** – but less than a third (29%) of end users are aware of it

of IT and cybersecurity leaders think employees feel comfortable reporting security incidents to the appropriate channels, in reality only 77% of end users do

80% **of IT and cybersecurity leaders are confident their organization won't fall for a phishing attack but 64% have clicked on phishing links themselves**

METHODOLOGY

Two surveys were conducted among 750 IT and cybersecurity leaders from C-level executive, director/VP, and owner roles and 750 end users whose roles include middle and senior management from departments including Finance, Human Resources, Legal, Marketing, Operations, and Procurement. Participants were from organizations with more than 50 employees to large enterprises, and came from 16 countries: United States, Canada, Australia, New Zealand, United Kingdom, Ireland, Germany, Netherlands, Belgium, Luxembourg, Switzerland, Austria, Finland, Denmark, Norway, and Sweden.

Throughout the report we use blue to represent IT and cybersecurity leaders and orange to represent end users. This visual differentiation will help you easily follow the data and see how perspectives vary between these two groups. The interviews were conducted online by Sapio Research in July 2024 using an email invitation and an online survey.

As all percentages are rounded to the nearest whole number, percentages in charts may not add up to 100%.

01

SECTION 01: BASELINE MEASURES

Back to Basics

When it comes to creating a culture of security, we often take for granted basic cyber hygiene practices. Unfortunately, IT and cybersecurity leaders and end users were quick to admit to reusing passwords, having lax multi-factor authentication (MFA) policies, and failing to implement password management best practices.

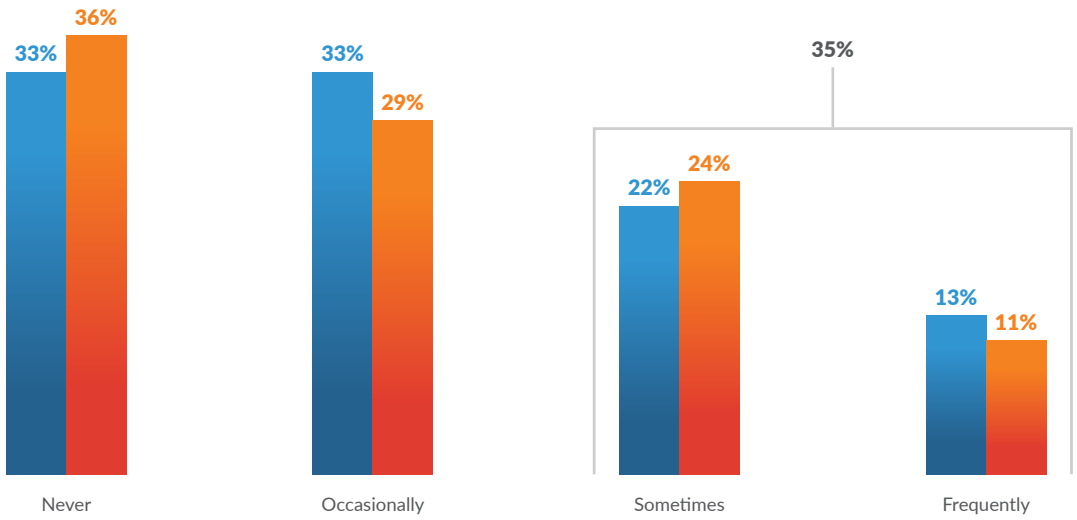
Two-thirds of both IT and cybersecurity leaders and end users reuse passwords

Around two-thirds of IT and cybersecurity leaders and end users reuse passwords at least occasionally.

Any benefit of regular password changes will be canceled out by the same password being recycled.

Indeed, **more of those who ought to be best informed – IT and cybersecurity leaders (68%) – admit to reusing their passwords than end users (64%)**. This is alarming, considering how detrimental an attacker's ability to obtain administrators' credentials can be to an IT environment.

IT and cybersecurity leaders and end users were asked how often they reuse their password.



Perhaps less surprising is the fact that while 35% of IT and cybersecurity leaders overall say they reuse passwords either "sometimes" or "frequently," this figure rises to 65% of those who have experienced four breaches.

65%

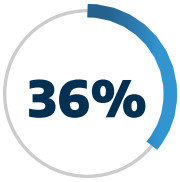
of IT and cybersecurity leaders who reuse passwords "sometimes" or "frequently" have experienced four breaches

Over half rely on memory and spreadsheets for passwords

Despite the availability of purpose-built security password management tools, **over half of IT and cybersecurity leaders rely on either memory (29%), or written notes and spreadsheets (26%) to remember system passwords.**

Considering IT and cybersecurity leaders have access to what attackers consider the "crown jewels" of the organization – administrator accounts, executive machines, and critical business systems – this behavior clearly increases risk.

IT and cybersecurity leaders were asked how they keep track of passwords for their system.



Password locker application

Memory only

Written down or computer spreadsheet

Stored in a physical safe or vault

When it comes to multi-factor authentication (MFA), 93% of IT and cybersecurity leaders enforce it, but only 59% of those enforce it for all users.

Failure to properly and effectively enforce MFA for all users opens organizations up to unnecessary risk, as demonstrated in recent high-profile cases of "prompt bombing" or "MFA fatigue."[4]

IT and cybersecurity leaders were asked to what extent they currently enforce multi-factor authentication for user accounts:

59%
All users

34%
Administrators or High value accounts only

5%
We don't, but we plan to implement MFA within the next 12 months

2%
We don't and we have no plans for MFA

More than a quarter of employees keep passwords over three months

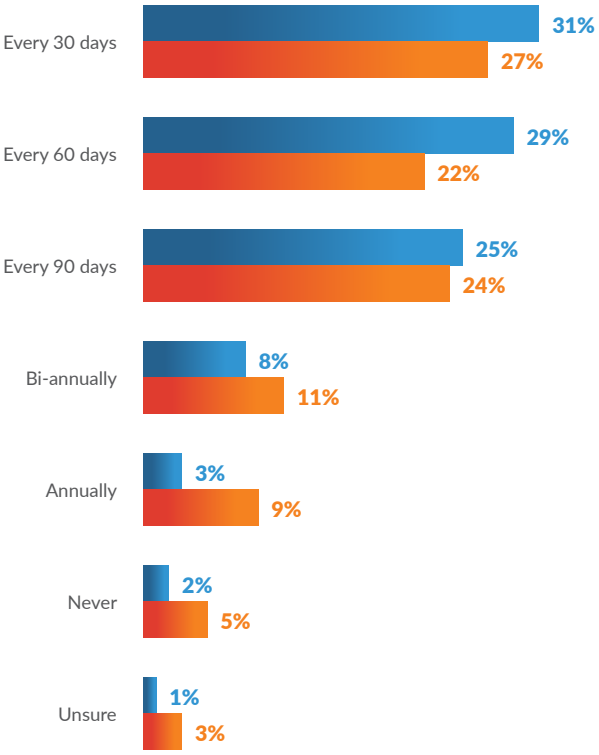
Despite Bill Gates predicting the death of the password twenty years ago[5], it's still the most common authentication method.

Bad actors are able to guess a password in months using brute-force attack technology. One way to mitigate the risk is to use strong passwords – CISA recommends[6]. Regardless of your organization's password policy, Arctic Wolf highly recommends having MFA in your organization and ensuring that end users know they will only accept MFA notifications if they have been initiated.

Most organizations implement policies to minimize the risk of password-related breaches, with **85% of IT and cybersecurity leaders saying they require employees to change their password at least every 90 days.**

And, 73% of end users do so to follow the company policy – one quarter (25%) are accessing company files and systems using passwords which are more than three months old.

IT and cybersecurity leaders were asked how often they require team members to change their password.
End users were asked how often they change their work password.



85%
of IT and cybersecurity leaders require employees to change their password at least every 90 days

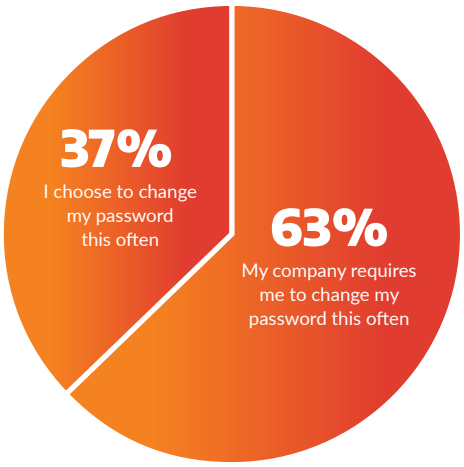
73%
of end users do so to follow the company policies

Password policy communication is inadequate

There's a mismatch between IT and cybersecurity leader messaging and team member understanding in regard to password changes.

This is an area which could be addressed by organizations looking for straightforward ways to minimize human risk in their security strategies

End users were asked why they change their password as often as they do.



Overall, more than a third (37%) of end users say they change their password at the rate they do through personal choice, rather than because this is mandated by their organization.

This suggests a misunderstanding somewhere along the way, particularly when we consider the 12% gap between the IT and cybersecurity leaders who say they mandate changes at least once a quarter, and the end users who actually do so.

Over 3 in 5 end users change their password as often as they do because their company requires it (63%)

Security measures disabled and screen locking disregarded

Given the access to critical systems and valuable information stored on IT and cybersecurity leaders' machines, security measures should never be disabled.

Despite this, **more than a third (36%) of IT and cybersecurity leaders have intentionally disabled their security measures.** This figure drops to 12% of end users, who typically won't have the requisite administrative rights to turn security systems off.

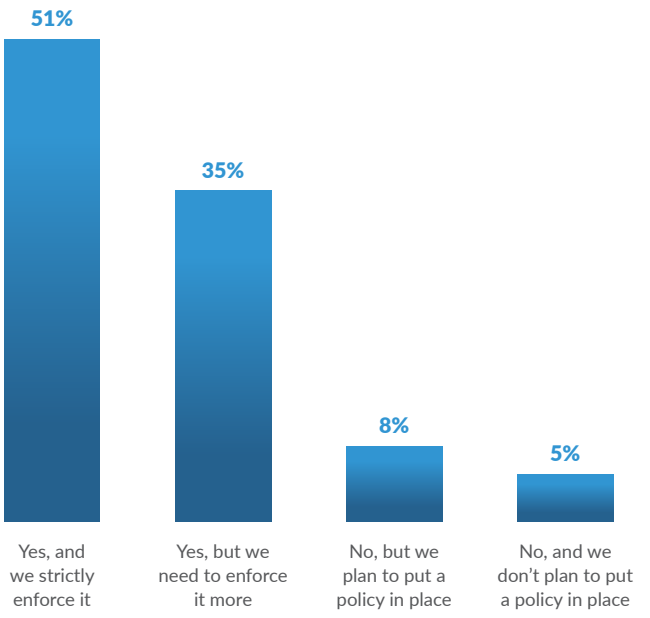
IT and cybersecurity leaders and end users were asked if they have ever disabled security measures on their system.

IT and cybersecurity leaders

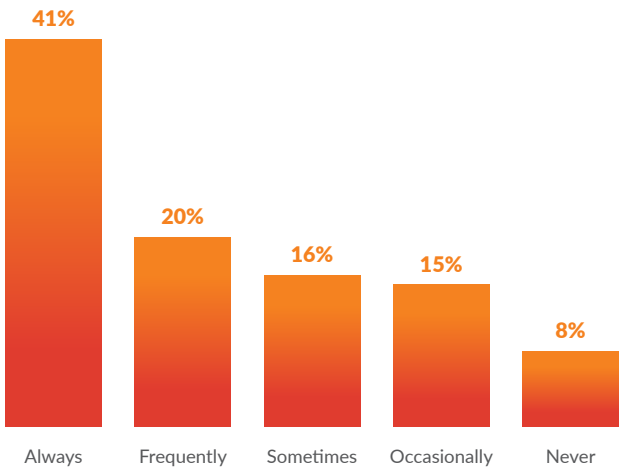
End Users

Another basic cyber hygiene requirement – **locking computer screens when away from desks – is required by 86% of IT and cybersecurity leaders, but fully actioned by less than half (41%) of end users.**

IT and cybersecurity leaders were asked if they have a policy that instructs employees to lock their computers when stepping away from their desks.



End users were asked how often they lock their computer screen when stepping away from their desk.



02

SECTION 02: BEHAVIORS AND BELIEFS

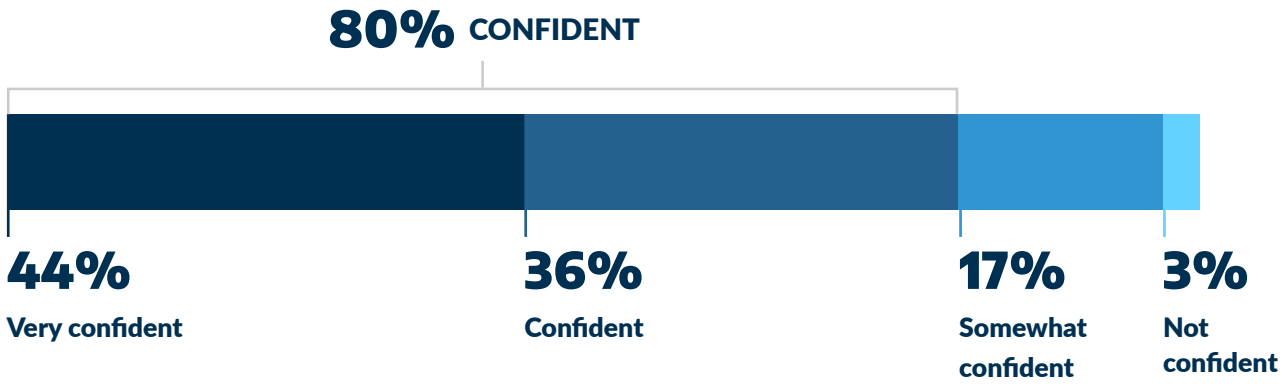
A Chasm Between Perception And Reality

Despite breaches occurring regularly, leaders and users alike appear complacent about their organization's ability to protect against attacks. This unfounded confidence breeds risky behaviors.

Phishing attacks – confidence undermined by reality

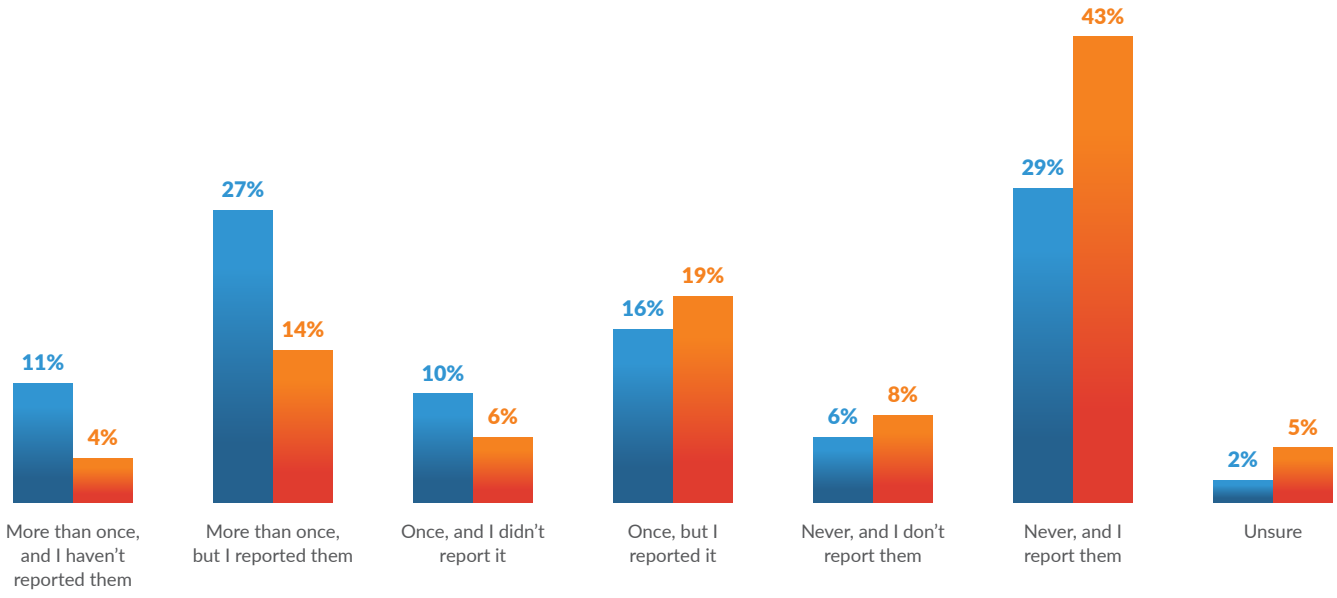
The vast majority of IT and cybersecurity leaders feel well-equipped to deal with phishing, with **80% saying they're confident or very confident their organization won't fall for an attack.**

IT and cybersecurity leaders were asked how confident they were that their organization won't fall for a phishing attack.



However, **64% of IT and cybersecurity leaders admit to clicking on potential phishing links at least once**. This is particularly concerning, given that an individual who has clicked on a phishing link is not paying proper attention and may inadvertently take another dangerous step. Fewer end users (43%) say they've clicked on phishing links – possibly they're less likely to realize they've done so, or more IT and cybersecurity leaders are being targeted.

IT and cybersecurity leaders and end users were asked if they have ever clicked a link in an email they thought could be phishing.



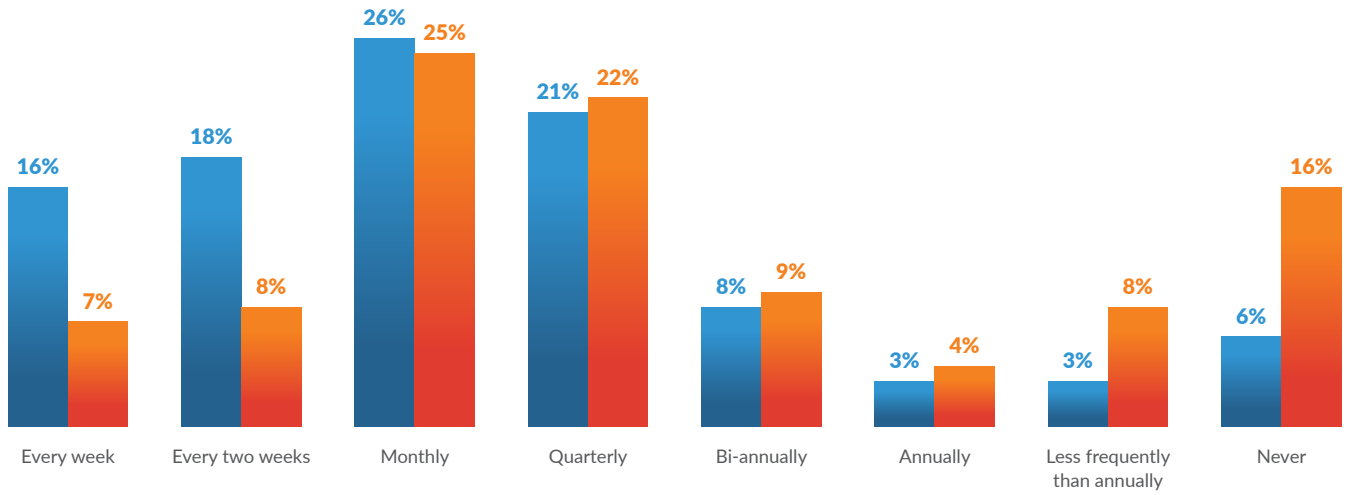
End users likely to be missing phishing events

Business email compromise (BEC) incidents were the most common type of security breach in 2023[7].

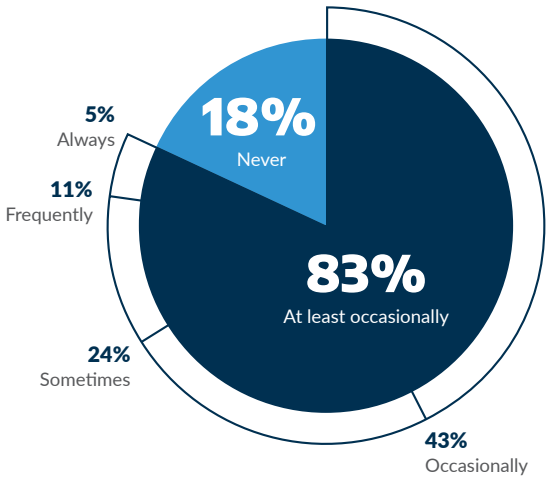
BEC often begins with a phishing attack to gain credentials or access to specific email accounts. Minimizing the success of such phishing attacks is vital, which is why many organizations incorporate phishing simulations to test their cybersecurity preparedness.

More than a third (34%) of IT and cybersecurity leaders send phishing simulations at least every two weeks, but less than half that number (15%) of end users are aware of them.

IT and cybersecurity leaders were asked how often they send phishing simulations to their organization. End users were asked how often their organization sends phishing simulations to help them feel prepared to spot an attempted attack.



IT and cybersecurity leaders were asked how often employees click phishing simulation links.



This finding is concerning, particularly when taken in conjunction with the 80% of IT users who believe their organization is safe from phishing attacks.

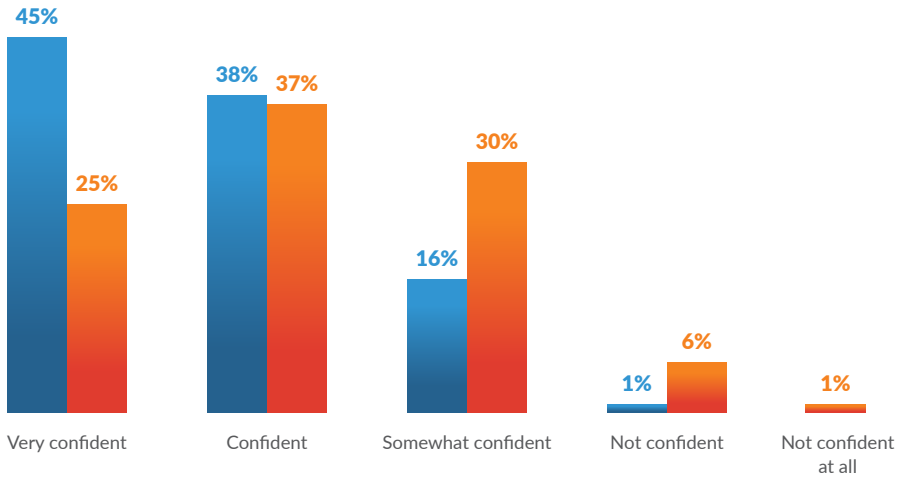
This confidence among IT and cybersecurity leaders is equally at odds with their belief that 83% of employees click phishing simulation links at least occasionally.

Perception and reality mismatch on breaches

Eighty-two percent of IT and cybersecurity leaders are confident or very confident in their company's ability to deal with a cyber attack.

This figure is lower among end users but still relatively high, at 62% – with only 1% saying they're not confident at all.

IT and cybersecurity leaders and end users were asked how confident they were in their company's ability to deal with a cyber attack.

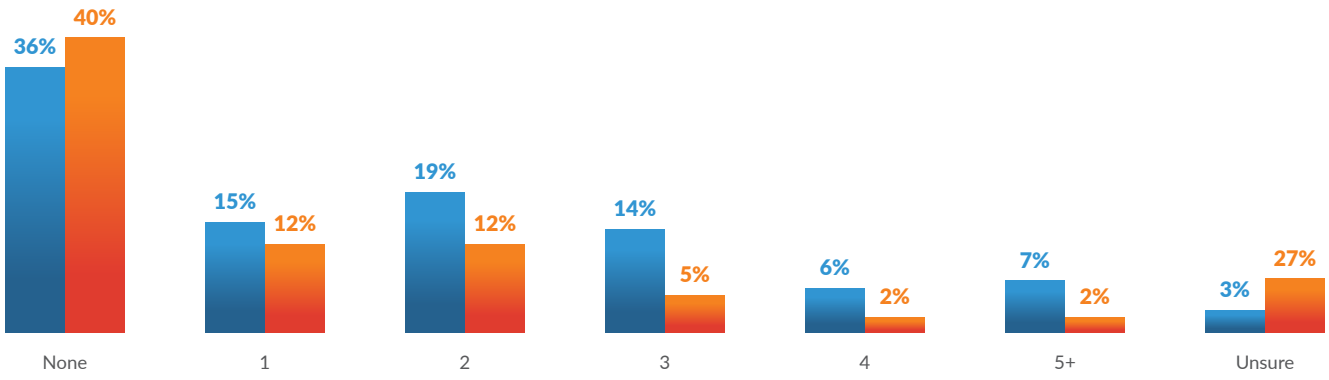


61%

of IT and cybersecurity leaders and 33% of end users say they've had one or more breaches in the last 12 months

Once again, this confidence appears unwarranted when examined in the context of actual breaches. End users are less likely to know about breaches than their IT colleagues. Some organizations hold a misplaced belief that breaches should not be communicated to the wider team, rather than using them as a learning opportunity. Twenty-seven percent of end users were unsure if breaches had occurred, compared to 3% of IT and cybersecurity leaders surveyed.

IT and cybersecurity leaders and end users were asked how many breaches their organization has experienced in the last 12 months:



03

SECTION 03: CRACKS IN CULTURE AND COMMUNICATION

The Key To Creating Positive Security Outcomes

IT and cybersecurity leaders' misunderstanding of end user attitudes may be resulting in missed opportunities to bolster defenses. Poorly communicated policies are missing the mark.

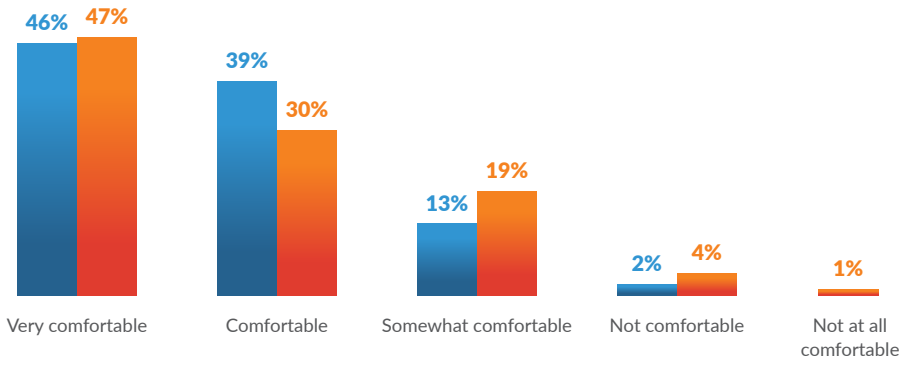
Nearly a quarter are uncomfortable reporting incidents

Robust attitudes to security don't happen by chance, they result from an ingrained culture across an organization.

An important element is making sure employees feel comfortable reporting security incidents so they can be addressed, and the learnings built into future plans.

While 85% of IT and cybersecurity leaders think employees feel comfortable reporting security incidents to the appropriate channels, in reality only 77% of end users do

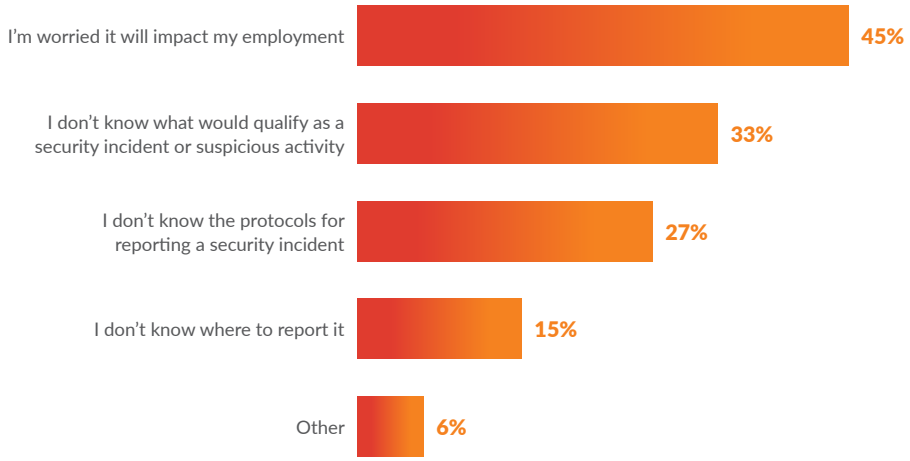
IT and cybersecurity leaders were asked how comfortable they think employees feel reporting security incidents or suspicious activities to the appropriate channels in their organization. End users were asked to what extent they feel comfortable reporting security incidents or suspicious activities to the appropriate channels in their organization.



Fears of termination are justified

Of the 5% of end users who said they were uncomfortable reporting incidents, **45% said they worried it would impact their employment.**

End users who said they weren't comfortable reporting security incidents or suspicious activities were asked why.



End user concerns are justified. **Only around a third (34%) of IT and cybersecurity leaders would rule out termination for an employee who fell victim to a scam such as phishing.**

27%

of IT and cybersecurity leaders have witnessed an employee termination for falling victim to a scam

39%

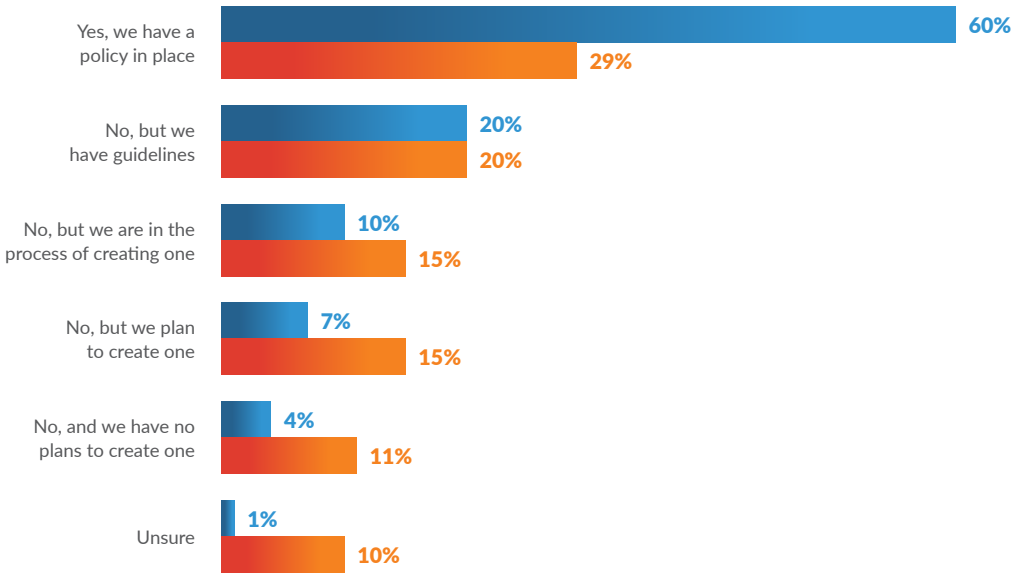
haven't yet terminated someone for that reason, but would be prepared to

Nearly two-thirds unaware of AI policies

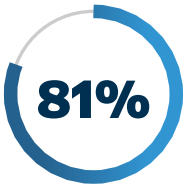
In many organizations policies are not being communicated effectively, meaning end users are potentially unaware of risks and internal guidelines.

While 60% of IT and cybersecurity leaders say their organization has an artificial intelligence (AI) policy in place, less than a third (29%) of end users are aware of one.

IT and cybersecurity leaders and end users were asked whether their organization has an AI policy in place.



IT and cybersecurity leaders and end users were asked if they have ever used ChatGPT results in work material.



IT and cybersecurity leaders

End Users

Given the rate at which generative AI tools are proliferating, the fact that 40% of IT and cybersecurity leaders say they have no AI policy is surprising.

Results from one such tool, ChatGPT, have been incorporated into work materials by 81% of IT and cybersecurity leaders (rising to 86% of millennial IT and cybersecurity leaders).

This, despite the serious concerns these models pose to loss of proprietary company information when used incorrectly. Fewer end users (42%) have used ChatGPT, with the highest take-up among Gen Z (54%).

04

SECTION 04: A ROADMAP FOR HUMAN RISK MITIGATION

Familiarity Breeds Success In Security Awareness

Regular security awareness training increases the likelihood that organizations will perform well against measures such as changing passwords and reporting incidents via the proper channels.

Regular training fosters positive security behaviors

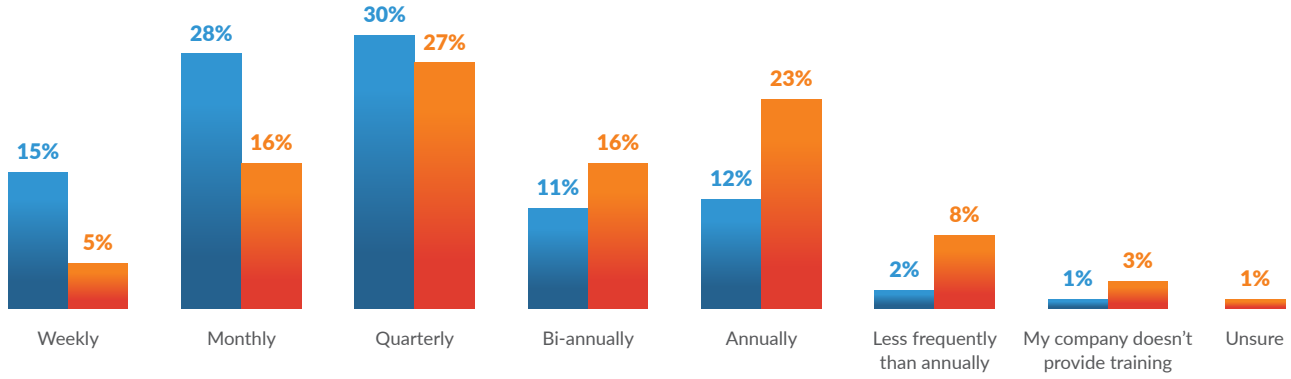
Most organizations provide security awareness training for both IT and cybersecurity leaders and end users, with the former receiving more regular training.

The data suggests that organizations who have suffered a breach are more likely to increase the regularity of training. 40% of IT and cybersecurity leaders whose security awareness training happens quarterly have not experienced a breach in the past year, as opposed to 14% of leaders whose training is weekly.

73% of IT and cybersecurity leaders and

49% of end users receive security awareness training at least quarterly

IT and cybersecurity leaders and end users were asked how frequently they receive security awareness training:



Strong correlation between training and cyber rigor

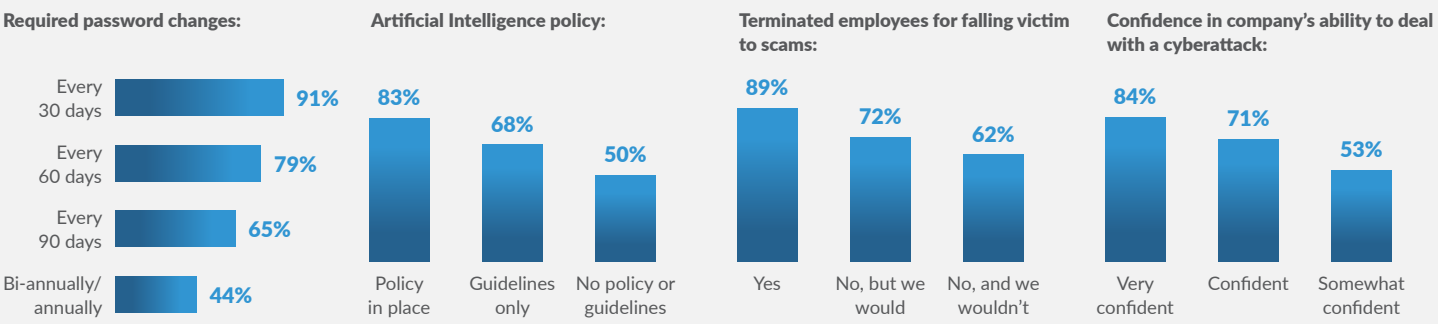
We see a direct correlation between those who receive frequent training, and those displaying the most robust attitudes to security.

Of the IT and cybersecurity leaders who have security awareness training at least quarterly, 91% require password changes every 30 days.

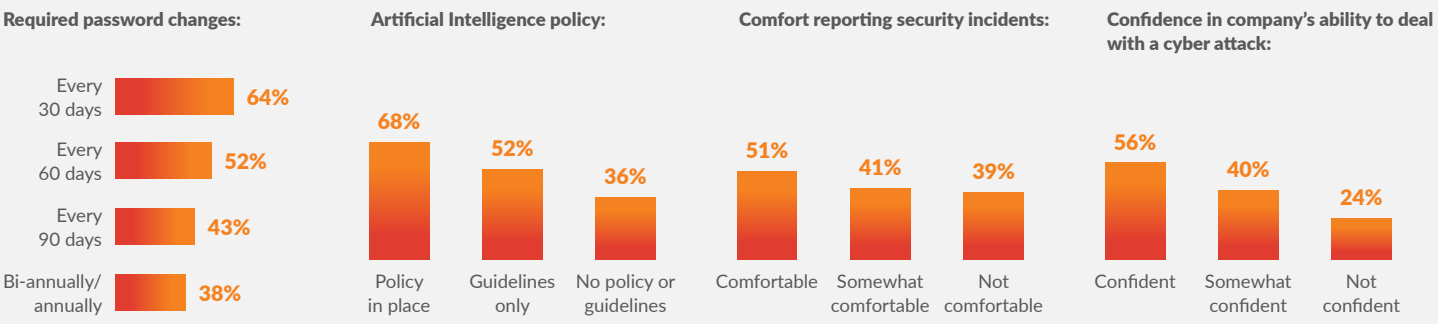
Those leaders who have training at least quarterly account for 83% of those who have an AI policy in place.

84%

of IT and cybersecurity leaders who have training at least quarterly say they are "very confident" dealing with a cyber attack



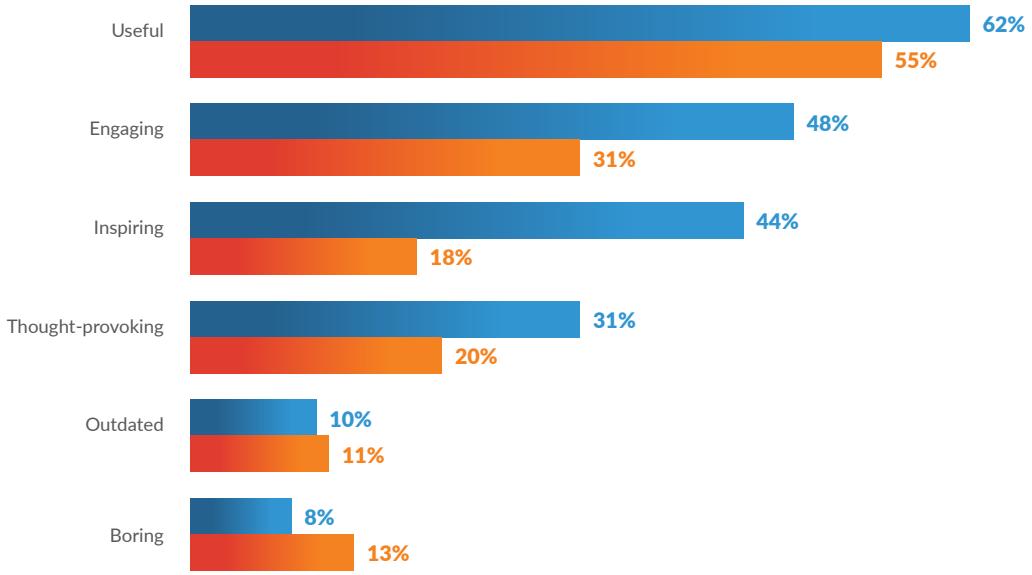
Similar results appear in the end user findings, with 51% of those who receive training at least quarterly being comfortable to report security incidents. **56% of those who receive training at least quarterly are confident in their company's ability to deal with a cyber attack.**



Room for improvement in training engagement

Outside of frequency, another requirement for effective training is that it feels engaging and relevant.

IT and cybersecurity leaders and end users were asked to describe their current security awareness training:



31%

or just under a third, of end users describe their current security awareness training as engaging

CONCLUSION AND RECOMMENDATIONS

Human risk is cyber risk and cyber risk is business risk. Wherever humans bring their beliefs, judgments, and individual abilities to bear on your business, you need to understand – and be prepared to mitigate – the inherent risk.

01 Basic security measures need improvement:

Regular password updates, the practice of reusing passwords and relying on memory indicates significant vulnerability within organizations. Password reuse and poor tracking increase the risk of credential theft and compromise, especially for sensitive accounts. Implement a robust password management system and encourage the use of unique, strong passwords for different accounts. Consider adopting multi-factor authentication (MFA) to add an extra layer of security and enable end-users to accept MFA notification if only they initiated.

02 High confidence versus reality:

Eighty percent of IT and security leaders are confident in their ability to avoid phishing attacks, but 64% have clicked on phishing emails. This indicates a disconnect between perceived and actual phishing awareness. Regularly test and assess phishing preparedness with simulated attacks to measure and improve real-world responses. Confidence should be supported by practical skills and ongoing training.

03 Communication and transparency are crucial:

Effective communication about security policies, procedures, and training is often lacking. Many organizations struggle to properly inform employees about policies and procedures, such as those which relate to generative AI, leading to gaps in awareness and confidence.

To foster a culture of trust within organizations, and improve security postures, it's vital that security leaders such as CISOs feel empowered to share information openly with the executive team. Transparent communication about security incidents to the executive team and proactive updates on policies are essential for all employers. By strengthening these communication strategies, organizations can ensure that all employees are well-informed and confident in their understanding of security policies and procedures. Also, executives should have a good knowledge of incident response protocols.

04 A security culture mindset correlates with fewer breaches:

Repetitive phishing clicks are a serious concern. Increase the frequency and engagement of security training programs. Tailor the content to be fresh, relevant and engaging to maintain interest and effectiveness. Select a human risk management solution like **Arctic Wolf Managed Security Awareness®**, that helps you create a security culture instead of a culture of blame.

DEMOGRAPHICS

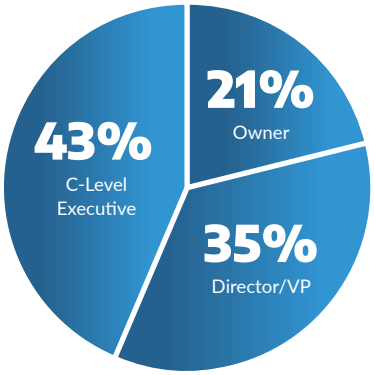
750 IT and cybersecurity leaders

250	100	100	100	75	75	50
US	Australia & New Zealand	United Kingdom & Ireland	DACH	Benelux	Nordics	Canada

750 end users (managers)

250	100	100	100	75	75	50
US	Australia & New Zealand	United Kingdom & Ireland	DACH	Benelux	Nordics	Canada

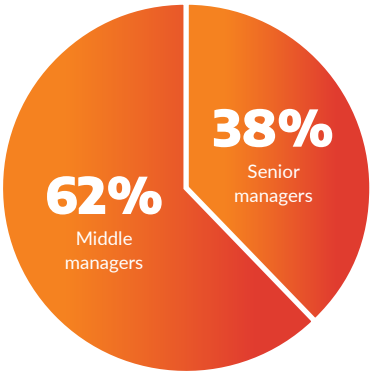
IT and cybersecurity leaders:



Top 3 business sectors:

- Financial services
- Manufacturing
- IT/technology (managers)

End users:



Top 3 business sectors:

- Financial services
- Retail
- Manufacturing

ABOUT ARCTIC WOLF

Arctic Wolf is the global leader in security operations, delivering the first cloud-native security operations platform to end cyber risk.

Powered by threat telemetry spanning, endpoint, network, identity, and cloud sources, the Arctic Wolf® Security Operations Cloud ingests and analyzes trillions of security events each week to enable critical outcomes for most security use cases. The Arctic Wolf® Platform delivers automated threat detection and response at scale and empowers organizations of any size to stand up world-class security operations with the push of a button.

For more information about Arctic Wolf, visit **arcticwolf.com**.

ABOUT SAPIO RESEARCH

Sapio Research is a full-service B2B and tech market research agency that helps businesses grow thanks to high quality, efficient and honest research solutions.

We deliver valuable insights to support our clients understand their audience, build powerful brands, cut through the noise with great content and headlines, and make vital business decisions relevant to their market. We're based in the UK and have access to over 149 million people across 130 countries, working with clients that range from top tech companies to global consultancies, Marketing/PR agencies and household name brands.

Our purpose-driven team of expert market researchers is passionate about providing data confidence for all and performing research that makes a difference. We're here to support our clients every step of the way in all areas of quantitative and qualitative research, so they can save time and thinking space, deliver with confidence, and unlock more value with their research. For more information, visit sapioresearch.com.

RESOURCES

1. https://www.verizon.com/business/en-gb/resources/reports/dbir/
2. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
3. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf
4. https://arcticwolf.com/resources/blog/prompt-bomb-uber-hack/
5. https://www.cnet.com/news/privacy/gates-predicts-death-of-the-password/
6. https://www.cisa.gov/secure-our-world/use-strong-passwords
7. Defending Against Business Email Compromise | Arctic Wolf