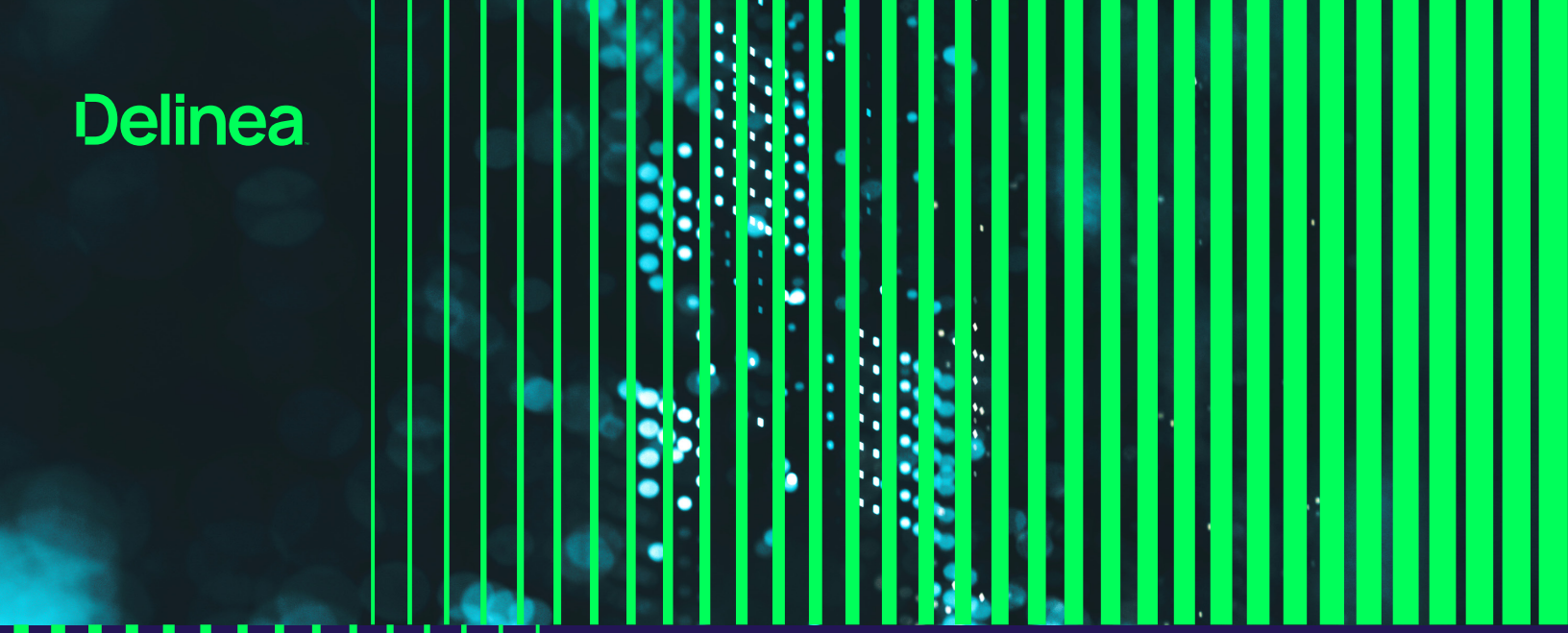
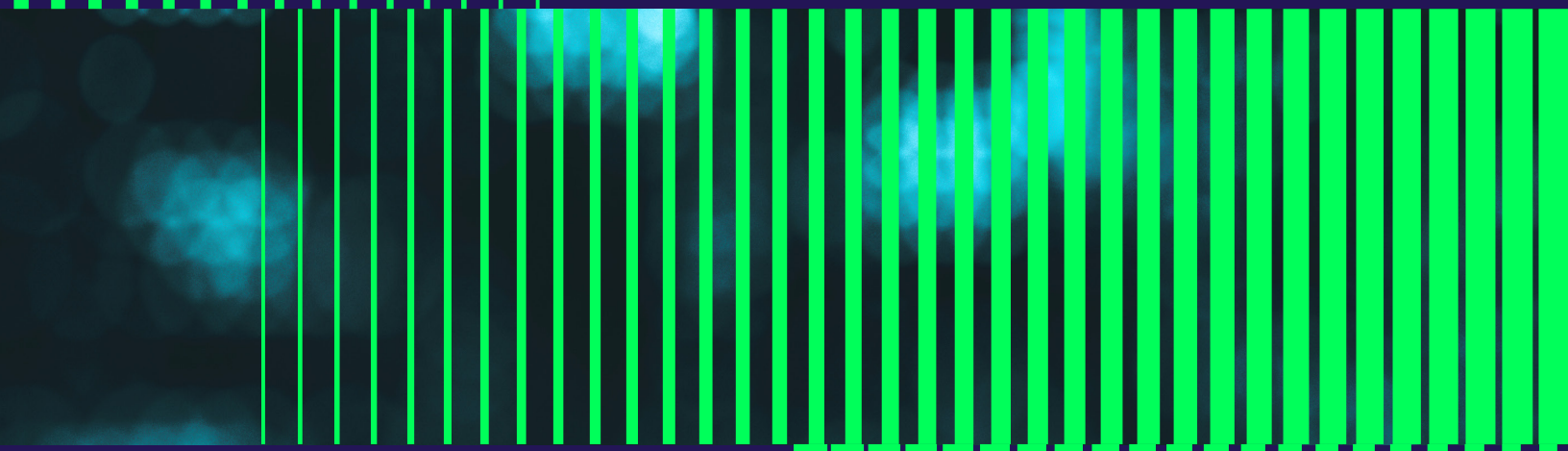
Delinea



Cybersecurity Team's Guide
Balancing Productivity and Security

Security risks employees take to get the job done



WHITEPAPER

Executive Summary

In 2020 our working environment changed dramatically in the wake of a global pandemic. As a result, our cybersecurity landscape and its associated risks have rapidly evolved. To manage large numbers of employees working remotely, organizations worldwide accelerated their digital transformations by moving to the cloud. However, cybersecurity in a cloud-centric environment does not mean traditional strategies to protect users will continue to be as effective.

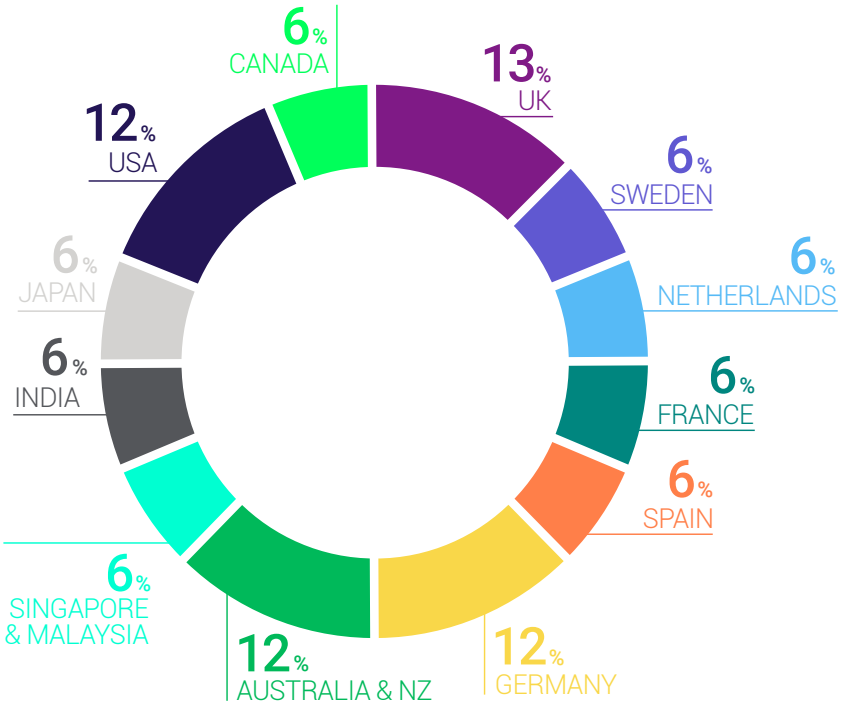
This latest research report from Delinea takes a close look at the perceived cybersecurity risks from an employee's perspective. What security barriers may be keeping them from being productive while working remotely, and the kinds of risks they are taking to get their jobs done.

By reading this global research report, you will gain a better understanding of the risky habits of employees and how their behaviors compare with your industry peers around the world. Consider this report a cybersecurity "reality check" that will help you answer several questions, including:

- Do employees understand their cybersecurity risks?
- Where are employees sacrificing security for productivity (what risks do they take in order to do their job)?
- How well do employees understand the impact of risks they are taking?
- What cybersecurity solutions have been deployed to help manage remote workers?
- Has security awareness training been effective?

To answer these questions and better grasp how organizations and their employees have responded to remote working, Delinea conducted a global survey in partnership with SAPIO Research among 8,041 knowledge workers in 15 countries.

Results from the survey reveal a disconnect between an understanding of cyber risks and the activities employees engage in every day to accomplish their tasks. Here are the key takeaways from this global survey.

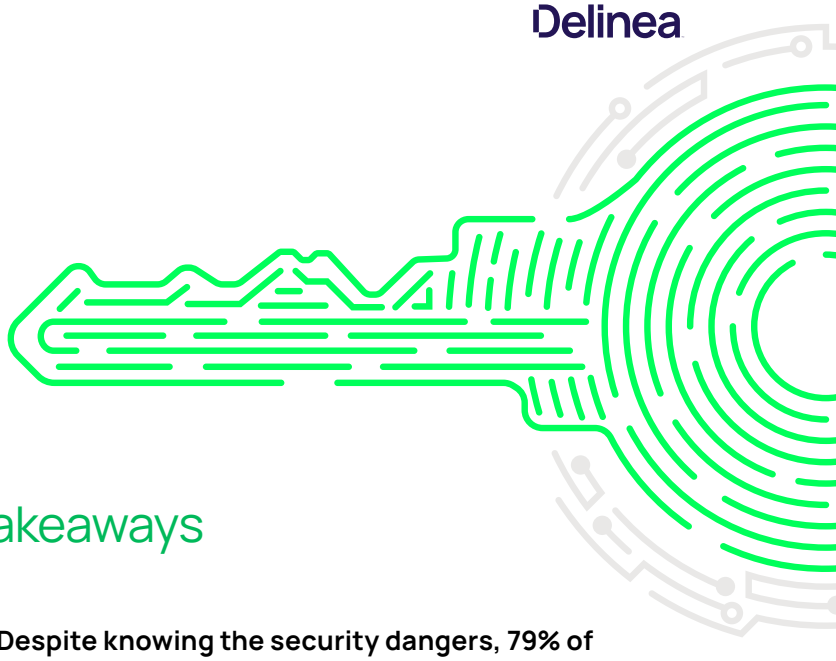


21% of respondents held C-level, owner, or MD positions

21% of respondents held director, manager, vice, or senior vice president positions

59% of respondents held individual contributor or administrative positions

Delinea



79%

Despite being aware of the risks, 79% of employees indicated they had engaged in risky activities in the past year

37%

Only 37% of respondents from SMBs of under ten employees thought their companies are at risk from cyber threats, while more than 50% acknowledged cyber threats as major risks in companies of 100+ employees.

44%

Cybersecurity awareness training falls short, with less than half of respondents receiving any kind of training.

Key Takeaways

1 **Despite knowing the security dangers, 79% of employees still engage in risky behaviors**

The cybersecurity reality check is that many employees believe they are not important enough to worry about security risks and, therefore, not a target. This makes them more likely to engage in risky behaviors to get the job done.

2 **SMB's are at higher risk than other organizations as they sacrifice security for productivity**

Smaller organizations are least likely to have implemented protection such as multi-factor authentication (MFA), virtual private networks (VPNs), and least likely to have received training in the last year compared to larger organizations. Lack of budget and staff may be a major barrier to improved security.

3 **Cybersecurity awareness among employees falls short, with only 44% receiving training in the past year.**

Due to a major focus on phishing attacks as the main priority of cybersecurity awareness training, other threats are perceived as lower risk, contributing to riskier behaviors. At the same time, less than half of respondents received security awareness training in the past year.

Delinea

KEY TAKEAWAY #1:
Despite knowing the security dangers, 79% of employees still engage in risky behaviors

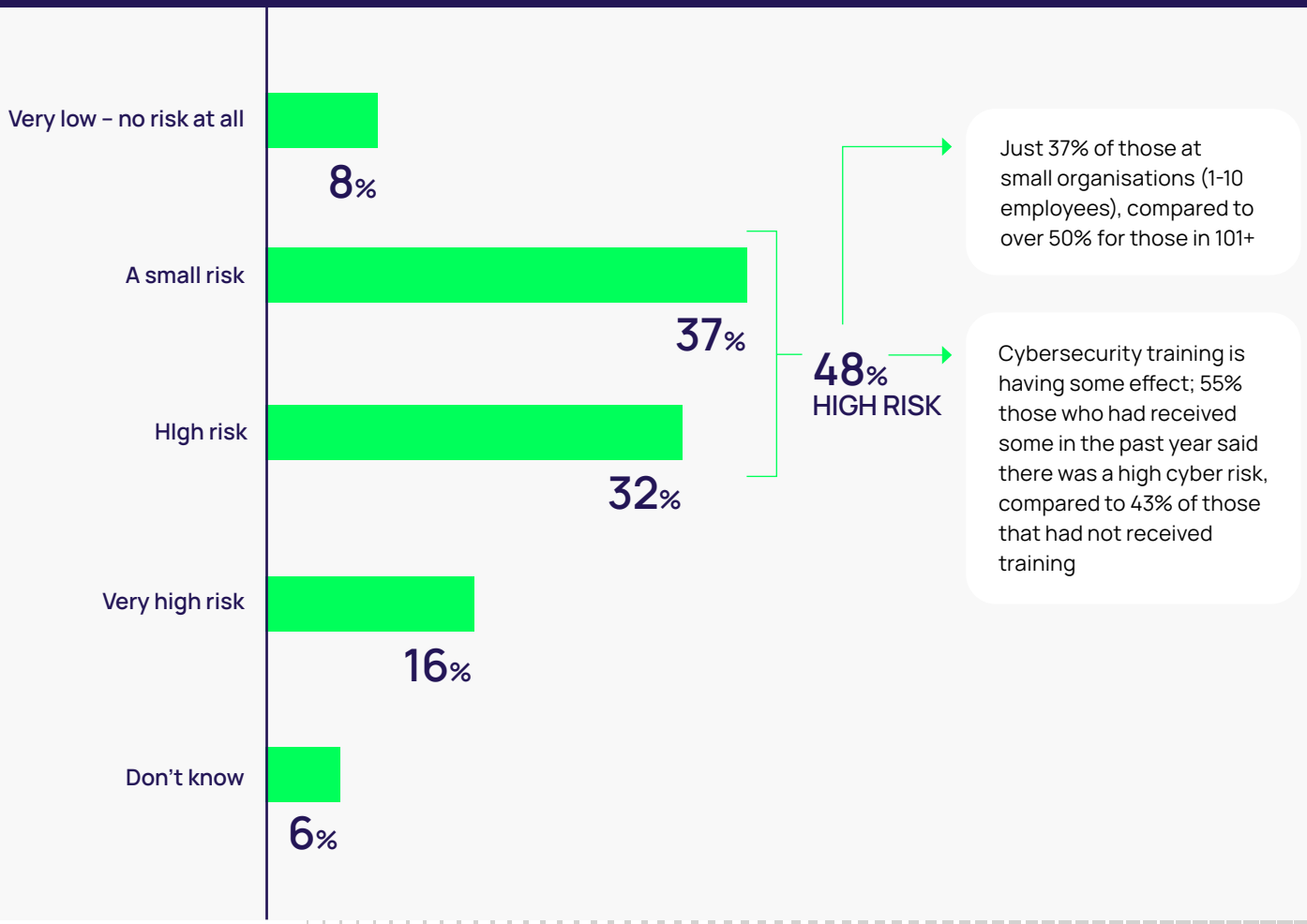
The cybersecurity reality check is that many employees believe they are not important enough to worry about security risks and, therefore, not a target. This makes them more likely to engage in risky behaviors in order to get the job done.

Survey Results

Most respondents appreciate there is a cyber risk to their organization, but just 16% of respondents view this as a very high risk.

While another 32% recognize cyberattacks as high risk, a large proportion (45%) see little or no risk to their particular organization

FIGURE 1 Overall, what is your general perception of the cyber risks to your organization, that is the threat of a cyberattack resulting in data loss or loss of access to your systems (ransomware) to your organization?



Delinea

FIGURE 2 | Employee perception of risk, by country

When it comes to assessing risk, there is considerable variation among countries. More than one out of three Swedish knowledge workers, for example, are least likely to see a high or very high risk (36%) from cyberattack, while two-thirds of Japanese knowledge workers are most likely (66%) to know the risk from an attack as high risk. Japanese knowledge workers are also least likely to have engaged in risky business, such as clicking on unknown links or using repeated passwords, while those in India are the most likely to have done so.

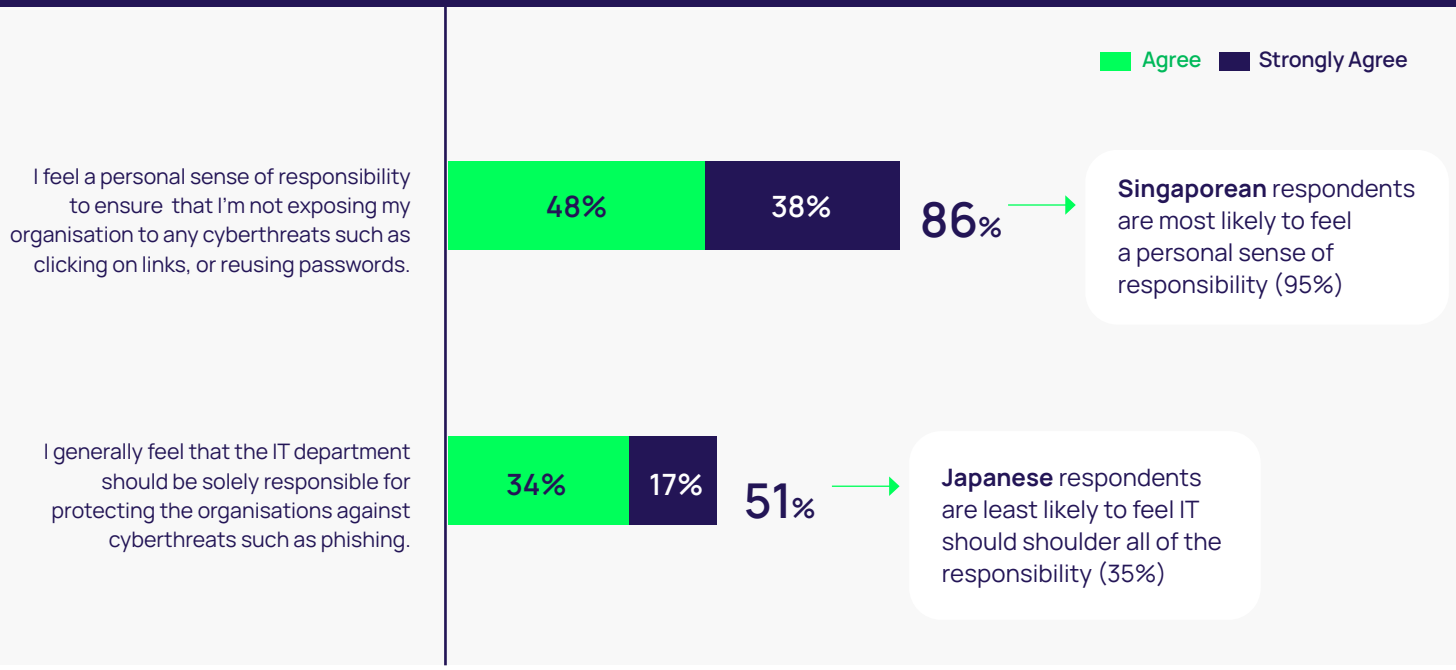
	Total	UK & Ireland	Sweden	Nether-lands	France	Spain	Germany	Australia & NZ	Singapore & Malaysia	India	Japan	USA	Canada
Very low – no risk at all	8%	7%	8%	9%	8%	7%	11%	10%	4%	11%	5%	8%	6%
A small risk	37%	37%	48%	43%	37%	36%	38%	40%	32%	30%	17%	38%	46%
High risk	32%	35%	28%	33%	35%	36%	33%	28%	38%	34%	31%	28%	28%
Very high risk	16%	15%	8%	7%	13%	18%	12%	15%	23%	22%	35%	20%	13%
Don't know	6%	6%	8%	8%	7%	4%	6%	7%	3%	3%	11%	7%	7%
High/Very high risk	48%	50%	36%	40%	48%	54%	45%	43%	61%	56%	66%	48%	41%
Base, n=	8041	1005	500	502	501	501	1000	1000	501	506	512	1004	509

Even though 86% of employees expressed a personal sense of responsibility to ensure they are not exposing their organization to cyberthreats, more than half (51%) of respondents say their IT department should have sole responsibility to protect them and their organizations from cyberthreats.

It appears that one of the main reasons employees continue to take risks is because they believe the IT and security teams are protecting them. Many organizations now have a formal IT security team and have made significant investments in IT security products. As a result, employees may naturally assume these professionals and tools automatically protect them.

Thus, employees continue to take risks based on the assumption that even if they do something wrong that causes a security incident, their security team will take care of the problem for them. This situation likely represents a major communication challenge as IT security teams and their organizations too often fail to educate employees on their individual responsibilities, and the extent to which cybersecurity depends on employees adhering to stated security policies and fundamental security hygiene practices.

FIGURE 3 | Overall, to what extent do you agree or disagree with the following statements?



To get the job done, employees are still engaging in very risky behaviors

Overall, 79% of employees surveyed indicated they have engaged in practices that put their organizations and personal credentials at risk of compromise, ranging from sharing passwords to connecting their personal devices to a company network.

More than a third of employees (35%), for example, continue to save passwords within their internet browsers on all of their devices, including personal and work devices. If an attacker successfully gains access to only one of those devices, the attacker can easily access all the passwords stored within the browser. This helps the attacker elevate privileges without being detected and gain access to the employees' email, company cloud applications, or even sensitive data.

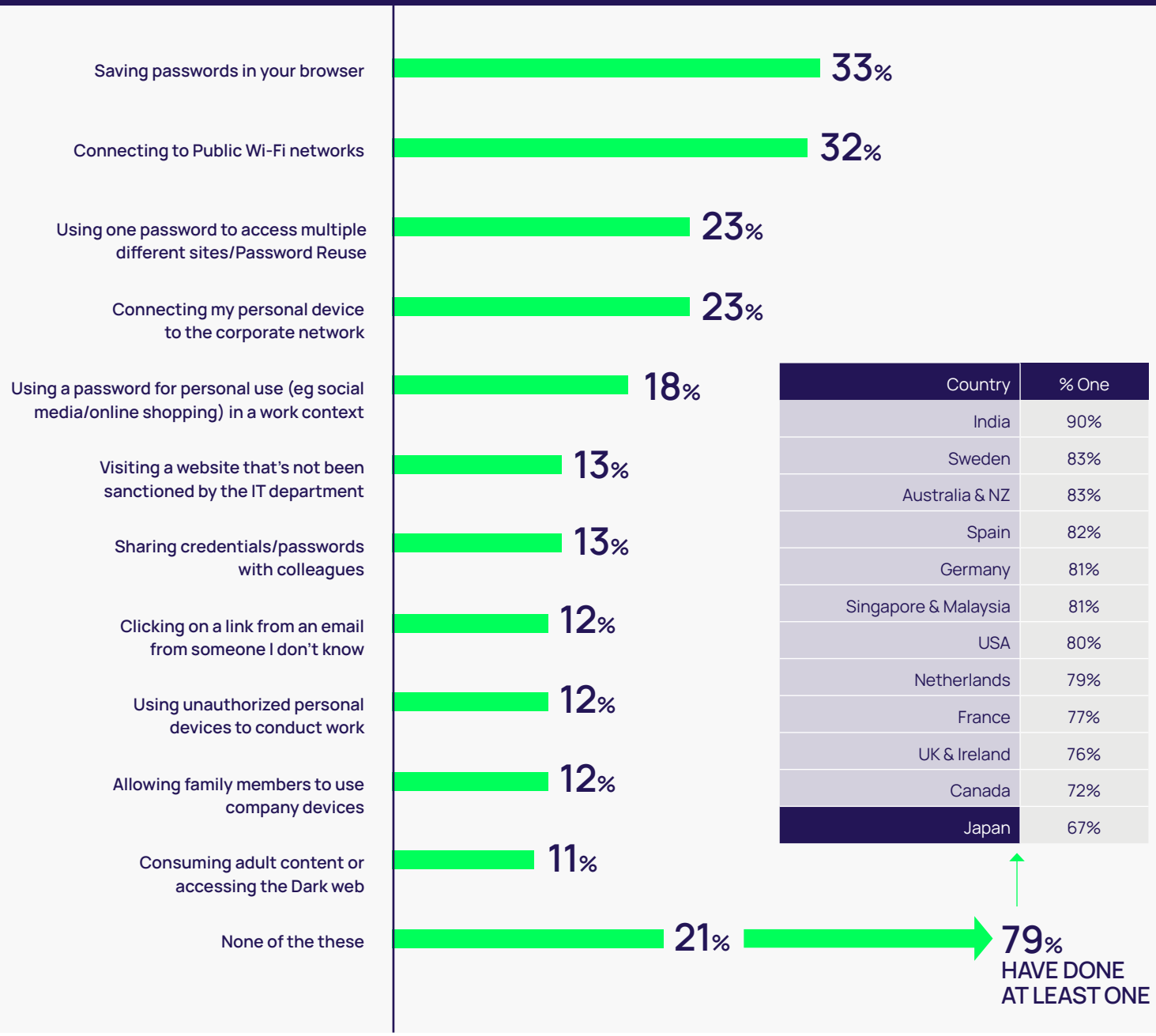
Employees too often rely on default settings for their browser security, which means there is no additional security protection enabled for most. A simple click on the reveal password button within the browser quickly reveals the clear text password to any attacker. While browsers make it easy for an employee the save and not have to remember passwords, they also make it easy for the attacker to exploit.

If the employee has saved multiple passwords within the internet browser, the attacker can readily see whether they are all the same or simple variations such as one character difference. With this information, they can use password cracking tools and wordlists to create all possible combinations of an employee's password choices. It is then only a matter of time before the attacker gains access to all of an employee's accounts, including their company's applications and systems.

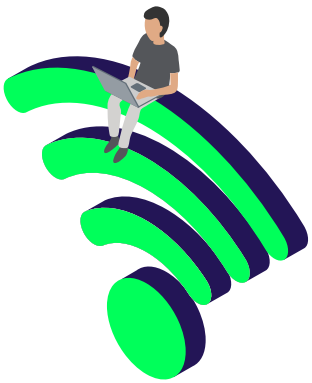
More than a third (35%) of respondents have saved passwords in their browsers in the last year. Just 21% have done none of these things, indicating 79% are engaged in risky behaviors.

Delinea

FIGURE 4 | Which of these have you done in the past year? Please select all that apply



Country	% One
India	90%
Sweden	83%
Australia & NZ	83%
Spain	82%
Germany	81%
Singapore & Malaysia	81%
USA	80%
Netherlands	79%
France	77%
UK & Ireland	76%
Canada	72%
Japan	67%

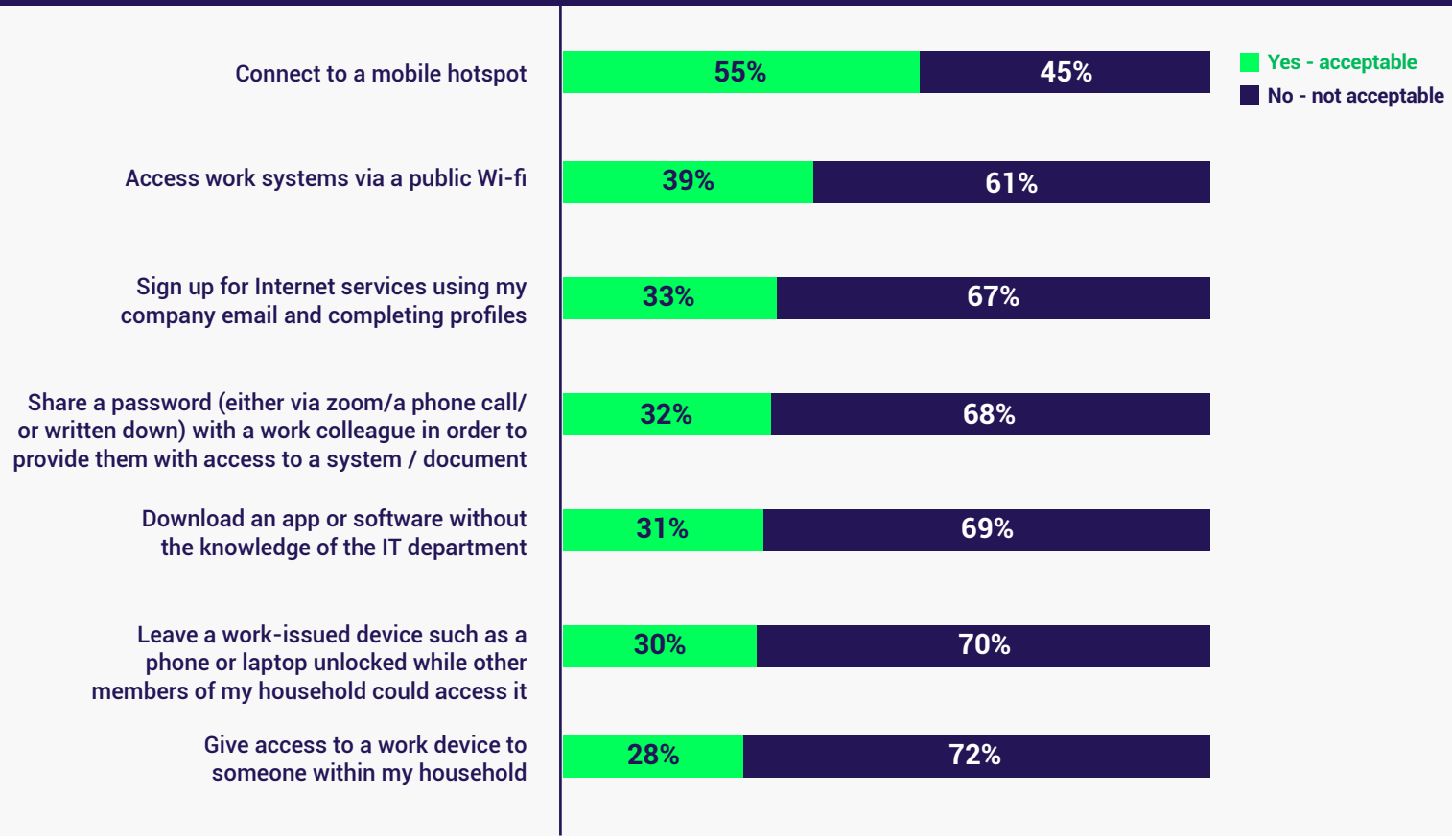


The constraints and pressures of working remotely have also contributed to workers taking on risky behaviors.

Over half (55%) believe it's OK to connect to a mobile hotspot in a work-based scenario, and 3 in 10 (30%) don't see a problem leaving a work-issued device unlocked where other household members could access it.

FIGURE 5

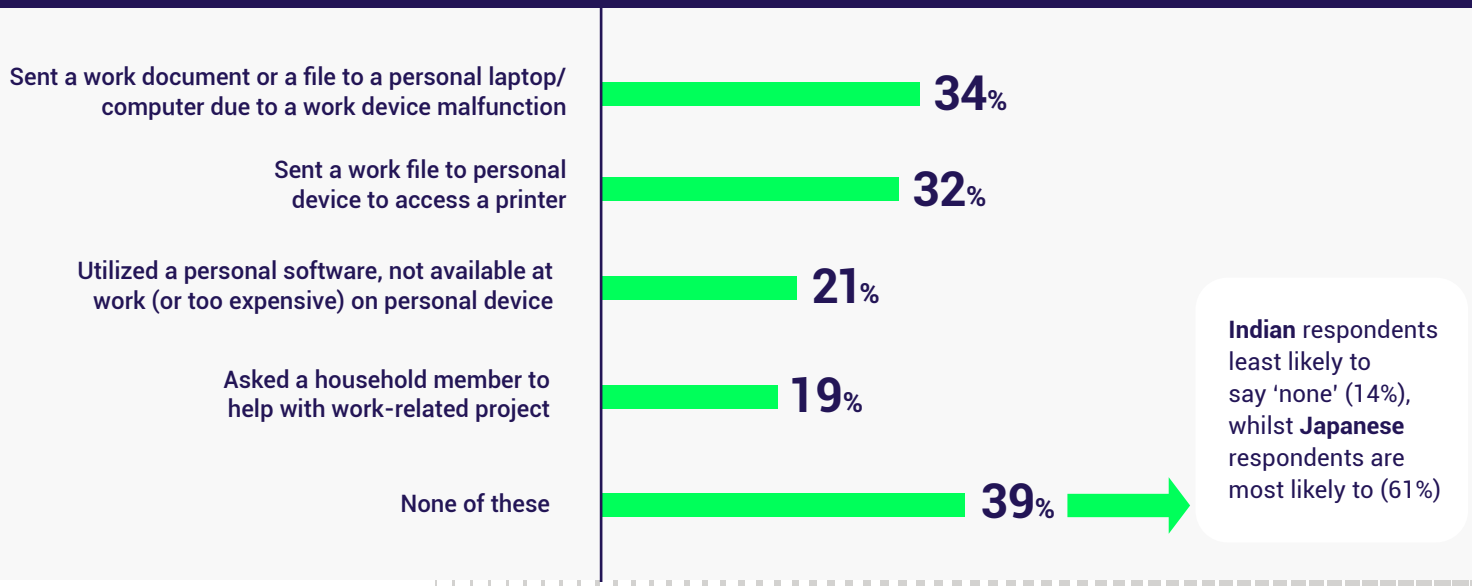
In a work-based scenario, which of the following would you consider acceptable in order to get your work completed? Please select either 'Yes - acceptable', or 'No - not acceptable' for each option



More than a third (34%) of respondents have sent a work document to a personal computer due to a work device malfunction.

FIGURE 6

In order to get your work completed, have you ever done the following: Please select all that apply



Indian respondents least likely to say 'none' (14%), whilst **Japanese** respondents are most likely to (61%)

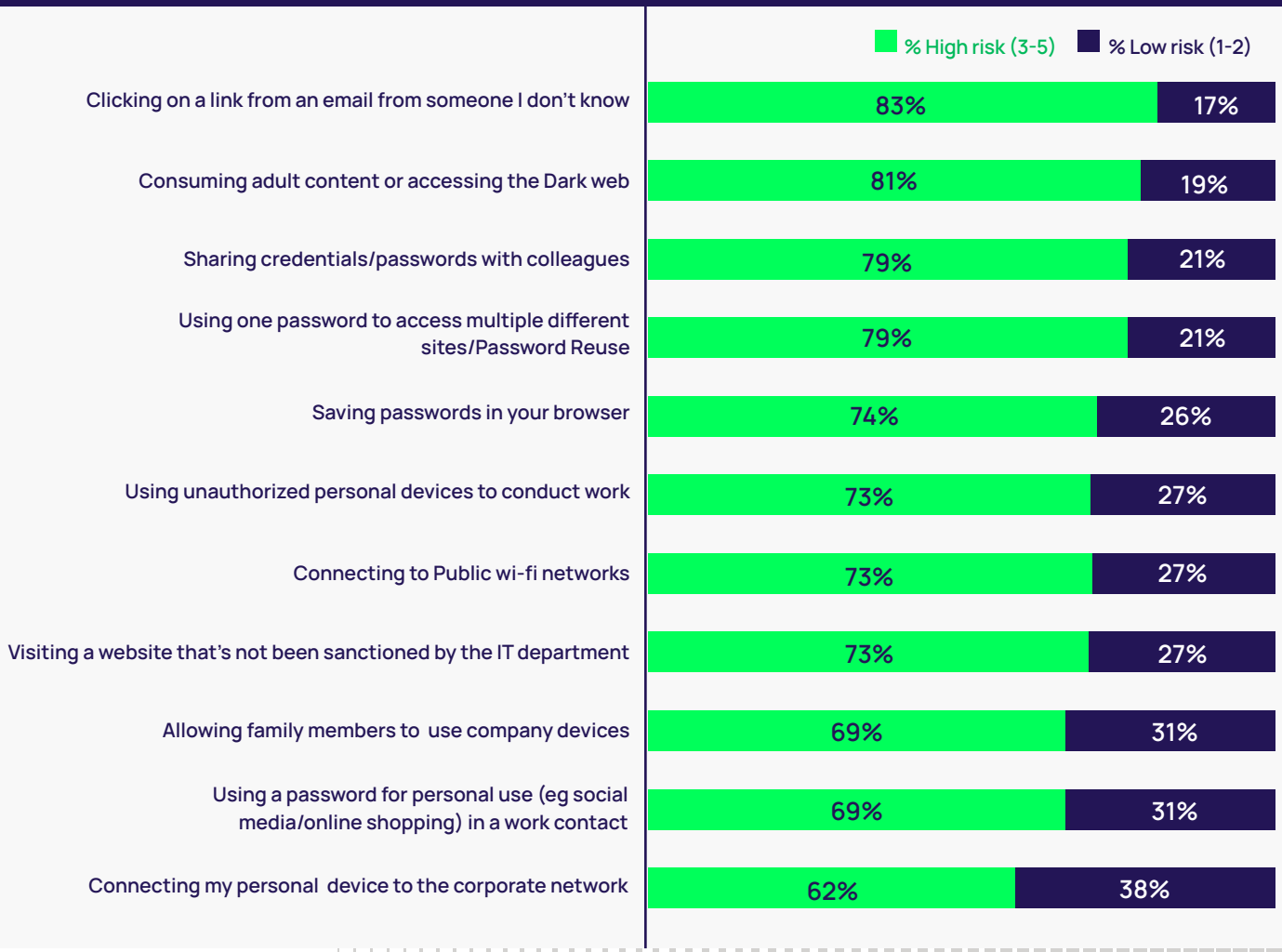
Cybersecurity awareness increases, but risk perceptions vary widely

Employees are aware of the major risks related to cybersecurity; however, their perception appears somewhat misguided. While almost 50% have moved to working remotely just 44% have received cybersecurity awareness training to deal with the change in working environment. With nearly 80% seeing a significant increase in phishing attacks in the past year, respondents likely have received some cybersecurity awareness training focusing on phishing techniques. However, this has probably created a situation where other high-security risks are perceived as lower.

While phishing attack awareness has increased, other high risks such as reusing passwords, storing passwords within the browser, sending company data to personal devices, connecting personal devices to company networks, or using public Wi-Fi for work may be pushed into the background and not considered as great of a risk.

Clicking on a link in an email from someone they don't know is most likely to be seen as high risk (83%) among respondents. Connecting a personal device to the corporate network is most likely to be seen as low risk (38%).

FIGURE 7 | **Which of the following would you consider risky? That is, it may put your organization at risk of a cyberattack Please rank these from 1 to 5 with 1 being 'very low risk' and 5 being 'very high risk**

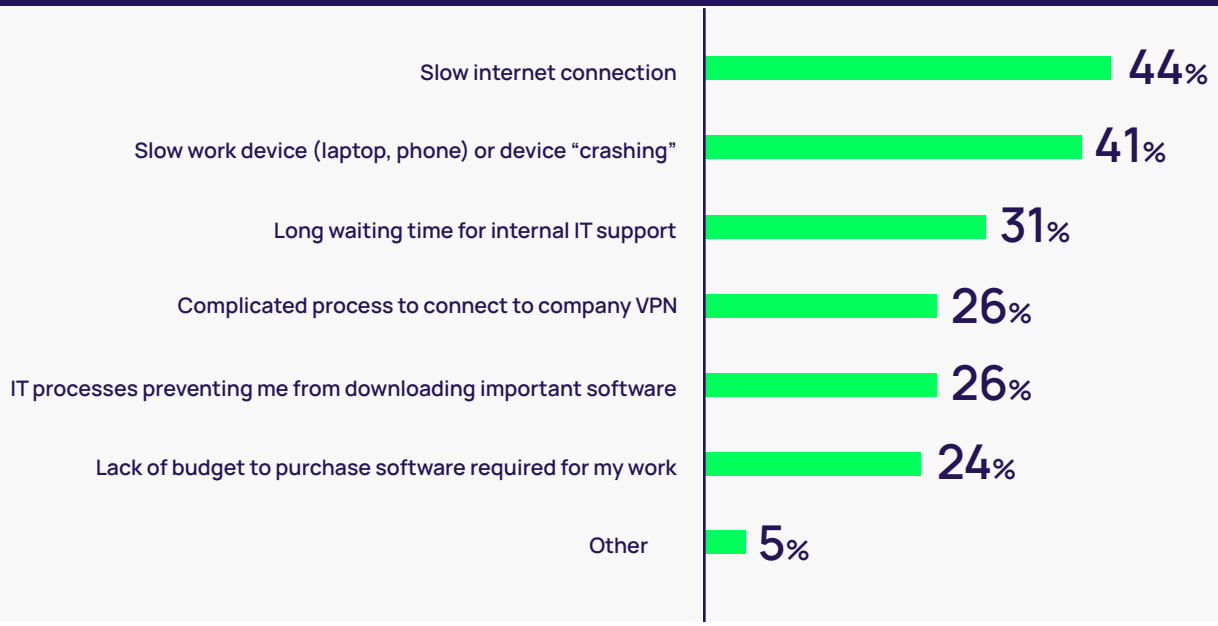


Barriers to productivity persist when working remotely

According to respondents, the top two hurdles that prevent people them from getting work done in a working from home environment are slow internet connection (44%) and slow work devices (41%).

Survey results show that nearly half of all remote workers across the globe have struggled with basic issues of slow internet connections and slow work devices during the past year. Obviously, the pandemic has accelerated a trend to remote working, but the infrastructure that supports it has failed to keep up in many cases. That means any impediment to getting work done puts a strain on workers maintaining a balance between security and productivity.

FIGURE 8 What are the most common hurdles that prevent you from getting your work done in a working-from-home environment? Please select all that app



49%

of the workforce worked remotely during the pandemic

Common hurdles to working from home, by country

"Slow internet" is the top hurdle for respondents from all countries, other than the Netherlands, which suffers most with "slow or crashing devices."

FIGURE 9 | What are the most common hurdles that prevent you from getting your work done in a working-from home environment? Please select all that apply.

	Total	UK & Ireland	Sweden	Nether-lands	France	Spain	Germany	Australia & NZ	Singapore & Malaysia	India	Japan	USA	Canada
Slow internet connection	44%	48%	36%	36%	38%	40%	38%	47%	60%	53%	41%	44%	44%
Slow work device (laptop, phone) or device "crashing"	41%	44%	37%	39%	35%	37%	36%	46%	50%	45%	33%	42%	37%
Long waiting time for internal IT support	31%	31%	22%	30%	27%	30%	30%	33%	38%	41%	19%	32%	27%
Complicated process to connect to company VPN	26%	22%	23%	22%	22%	27%	25%	29%	30%	38%	28%	26%	24%
IT processes preventing me from downloading important software	26%	19%	22%	25%	24%	21%	24%	27%	36%	47%	22%	28%	17%
Lack of budget to purchase software required for my work	24%	21%	**21%**	22%	21%	22%	20%	26%	31%	33%	**19%**	27%	18%
Base, n=	6202	814	344	410	373	407	749	732	466	497	308	732	370

Tips for Cybersecurity Leaders

- Engage with your peers to understand and listen to their business priorities. It is important that cybersecurity leaders help them to be successful while reducing cybersecurity risks. Align security to your organization's business goals.
- Be the team that asks "let's find out how" rather than the team that "always says no." Too often security leaders are perceived as the team that slows everybody down, rather than enabling the business.
- Be the team and leader who helps make your peers jobs easier and better by ensuring security is a positive experience. Provide tools and solutions such as Password Managers that will help reduce employee cyber fatigue.
- Communicate effectively on how the Security team has prevented cyberattacks and its measurable benefits such as the amount of revenue the cybersecurity team has saved the company. All too often business leaders only hear from security when a security incident is occurring that impedes business productivity.
- Promote a Cybersecurity ambassador or mentors within other business units to bridge the cybersecurity awareness gap and provide a line of communication directly between the teams.

Recommendations

This report serves to remind us that striking a balance between risk, security, and productivity is more challenging than ever in a world where workers are increasingly remote. It is essential that cybersecurity teams make sure that secure behaviors are built into the workplace wherever possible. Far too many organizations are still protected with just a simple password, with employees given the responsibility for creating and managing their complexities on a continuous basis. As the research in this report shows, that approach falls far short in a world dominated by ever more sophisticated cyberthreats.

Cybersecurity teams should move password and privileged access security into the background so that their employees do not need to create, rotate, or manage them. This will go a long way to enabling employees to concentrate on the things that really matter, including staying productive, meeting their business goals, and being successful in their organizations.

1. **Move Passwords into the background and automate password security with a Privileged Access Management solution.** PAM software solutions are available to help fit any size organization, as well as accommodate needs at any stage of cybersecurity program maturity.

2. **Make sure that cybersecurity measures and guidelines are as usable as possible.** Usable cybersecurity tools must be easy to install, deploy and manage for business users as well as IT managers. Tools or techniques that interfere with employee productivity are doomed to failure. User experience needs to be a top priority.

3. **Educate employees on their responsibility on cybersecurity and communicate clear, easy guidelines.** The best way to create a security culture is to align security goals with the business goals and empower employees so they are not afraid to ask for advice. Rolling out a cyber mentor/ambassador program is a good way to connect security strategy and awareness within the different organization departments. Staff can be held accountable only when they are clearly informed of their responsibility and the risks of abusing them by not following the process. If it is something like an accidental click on a link that infects a machine, it may be on par with clicking on stuff is part of the employees' job.

Resources

Invisible PAM: Balancing Productivity and Security Behind the Scenes

This free whitepaper illustrates the security benefits of enterprise Privileged Access Management software showing how it can be integrated to protect privileged access and be virtually invisible to the user.

Definitive Guide to Securing Privileged Access

Complete guide for enterprise cybersecurity teams for how to secure vulnerable apps, devices, and cloud data through least privilege access.

Live Hack Demo: Securing privileged access to stop attackers in their tracks

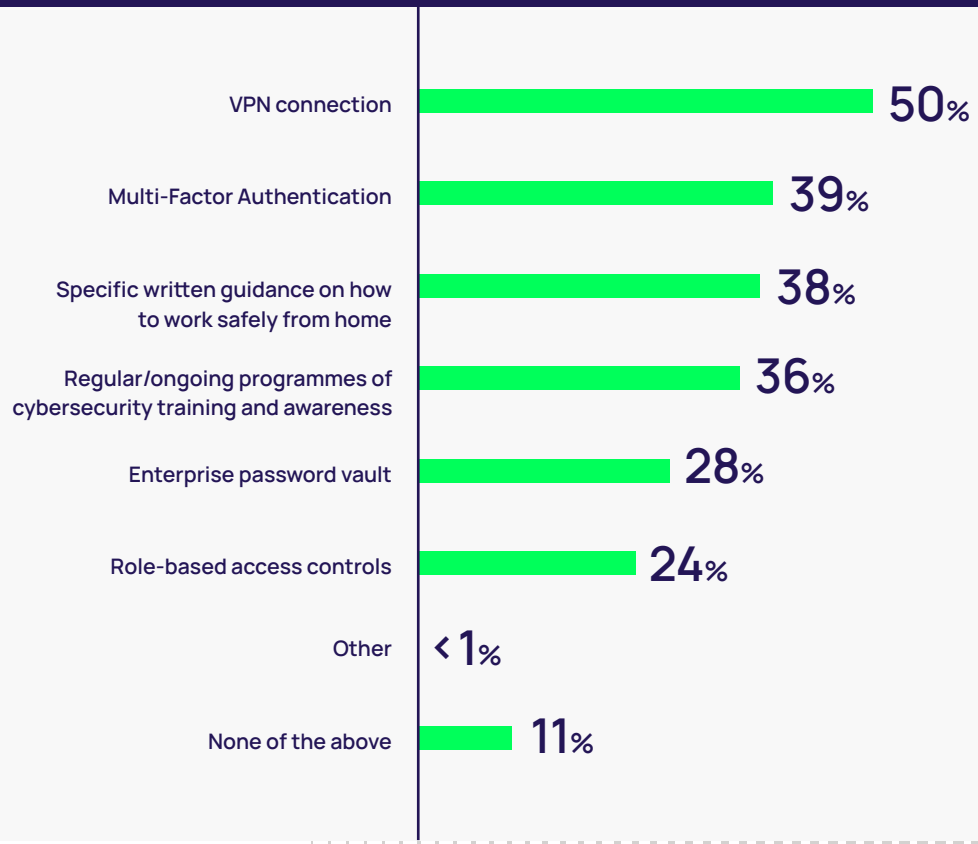
Delinea Chief Security Scientist Joseph Carson demonstrates how an attacker captures an employee password on an endpoint, gets hold of an email account, and escalates the exploit to access a critical cloud application—all undetected by typical security controls. He shows how you can stop these endpoint attacks and protect privileged access to critical cloud applications with PAM security solutions.

KEY TAKEAWAY #2:

SMB's are at higher risk over other organizations as they are frequently forced to sacrifice security for productivity

Smaller organizations are least likely to have implemented protection such as multi-factor authentication (MFA), or Virtual Private Networks (VPN's, and least likely to have received training in the last year compared to larger organizations. Unfortunately, effective cybersecurity solutions are not always a viable option for all companies and for most SMB's they may be out of reach due to budget or limited resources. Defensive measures such as cybersecurity training, VPN's or Multi-Factor Authentication are typically less available for SMB's compared to larger organizations. This means the risks and impact of cyberattacks against SMB's are much higher. In dealing with the pandemic and shift to remote working, most SMB's may have been forced to sacrifice cybersecurity to focus on keeping workers productive.

FIGURE 10 Since you moved to home working, has your company implemented any of the following specifically regarding how to protect your devices and data from cyberattacks? Please select all that apply

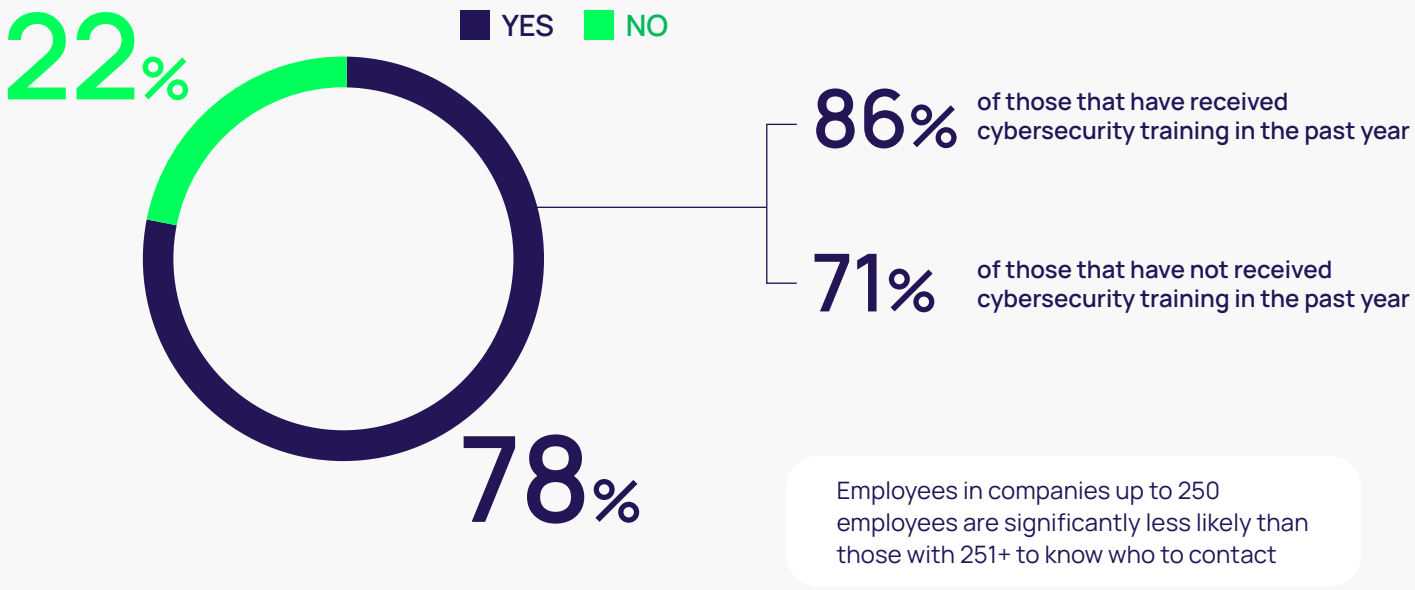


Smaller organisations (with 1 to 10) employees are least likely to have implemented any of these, whilst larger are more likely to have done so

The vast majority of respondents know who to contact within their organization to report suspicious cyber activity (78%).

Those who have received training are more likely to know who to contact (86%) than those in larger organizations. But here again, SMB's fall behind larger organizations in the percentage of employees who know what to do when a security incident occurs.

FIGURE 11 | Do you know who to contact within your organization to report any suspicious cyber activity, such as receiving a phishing email?



In addition, SMB's also perceive a much lower risk of cyberattacks against them. This is likely due to the misconception that cybercriminals are interested only in large organizations with more money or higher valuations. Unfortunately, this is not the reality. Research shows most cybercriminals target companies with less security, making SMB's prime targets and in the eyes of cybercriminals and are more likely to pay a ransom to regain access to their business information.

> "Cybercriminals mostly target companies with the least security implemented and that means SMB's are a prime target."

Recommendations

Size does not matter when it comes to cybersecurity incidents and data breaches, with user credentials a top target no matter the organization size. Everyone is a target, and anyone can become a victim with the simple click of an email link or opening an attachment. For many companies it is only a matter of time before they become victims. Thus, it is important to invest in and prepare a solid incident response plan as well as a business continuity plan to enable you to recover both well and with speed. Companies that have a solid incident response plan can reduce the costs of a security incident by almost 50%.

Not all cyberattacks are from advanced nation-states or sophisticated hackers, even though media coverage seems to emphasize these types of threats. Most cyberattacks are surprisingly simple, and usually financially motivated. Cybercriminals nearly always choose the least noisy hacking technique with the lowest cost. Today this typically means targeting humans and taking advantage of their trusting nature.

Resources

Secret Server

Secret Server empowers privileged business users to manage passwords securely. By including business users in a central, IT-managed vault, you reduce risk and gain oversight for business user behavior without impeding productivity.

Secret Server for Business Users

Secret Server Business User empowers privileged business users to manage passwords securely. By including business users in a central, IT-managed vault, you reduce risk and gain oversight for business user behavior without impeding productivity.

Free Cybersecurity Incident Response Plan Template

The incident response plan template contains a checklist of roles, responsibilities and details for actionable steps to measure the extent of a cybersecurity incident as well as contain it before it damages critical systems. You can easily customize the template to match your incident response policies, regulatory requirements, and organizational structure.

Infographic "Turn to MFA Everywhere"

To minimize exposure to credential-based cyberattacks, cybersecurity experts, as well as a growing number of industry standards and government regulations (e.g., PCI, HIPAA, NYDFS, NIST), you should augment usernames and passwords with multi-factor authentication (MFA) to add an additional layer of security for access control. This infographic outlines the five reasons that drive the need for MFA Everywhere.

Tips for Cybersecurity Leaders

1. Implement Multi-factor Authentication (MFA) is a must for any size organization to help ensure hacking a simple user password does not lead to a significant cybersecurity incident.
2. Explore options for affordable privileged access management tools that are highly usable to help protect employees from the risks associated with credential compromise.
3. Develop an incident response plan. The question is not if, but when. Being prepared with an organized business response plan is a must. That means designating key individuals who must be involved to implement processes before, during and after a security incident.
4. Educate employees at every opportunity; in meetings, in newsletters, in all communications, reinforce the concept of cybersecurity as everyone's responsibility not only to act but to ask when unsure.

Delinea

KEY TAKEAWAY #3:

Cybersecurity awareness among employees falls short with only 44% receiving training in the past year.

Due to a major focus on phishing attacks as the main priority of cybersecurity awareness training, other threats are perceived as lower risk, contributing to riskier behaviors. At the same time, less than half of respondents received security awareness training in the past year.

Survey Results

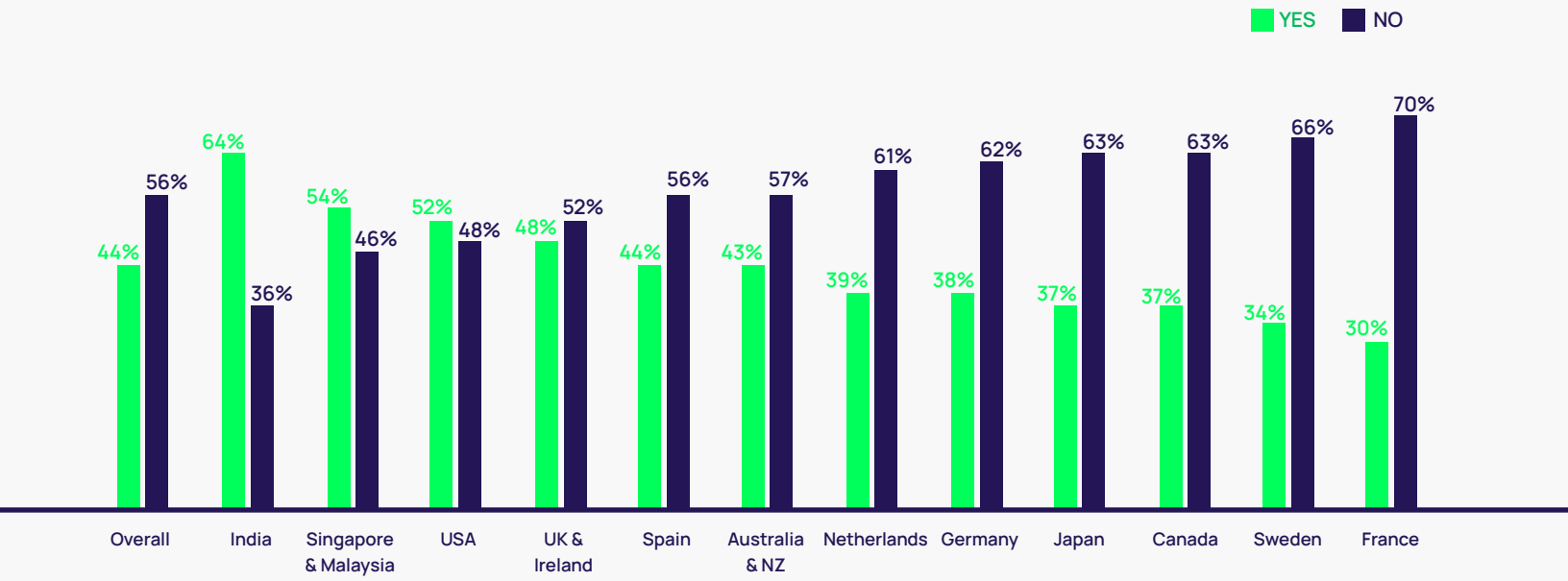
Overall, only 44% have received cybersecurity training in the past year.

India has the highest portion of employees that received cybersecurity training (64%), and France has the smallest (just 30%)

In most situations, while employees are better at identifying phishing attacks today due to the high focus on phishing awareness training but on the other hand other high security risks employees do not know what to look for or how to identify such as when changing passwords how to do that safely or how to log on to remote systems and applications securely. Today this means the awareness training is focused on the risk but not the how an employee does something safely.

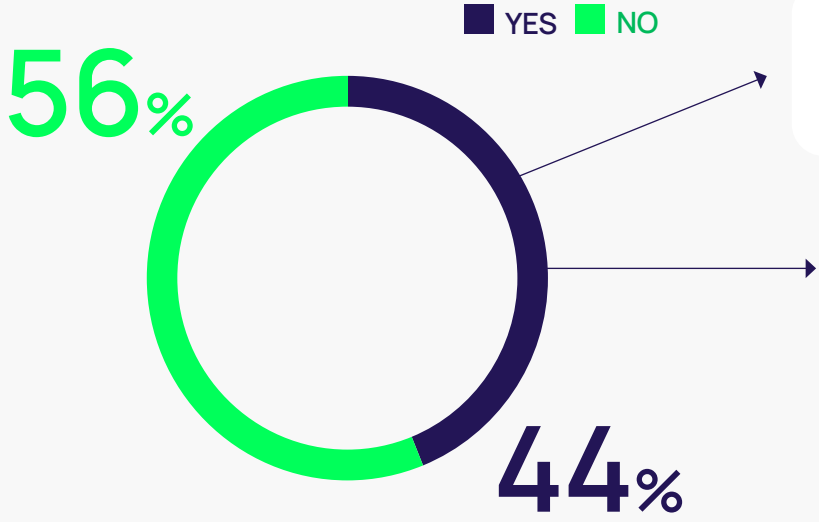
We need to move from a cybersecurity checkbox awareness approach to a long-term cybersecurity training strategy that incorporates Awareness, Behavior and Culture.

FIGURE 12 | In the past year, have you received cybersecurity training from your current employer? That is, training on how to protect yourself and the company from a cyberattack.



Those who have started working from home since the pandemic are more likely to have received training in the past year (60%) than those who have not been WFH (28%).

FIGURE 13 | In the past year, have you received cybersecurity training from your current employer? That is, training on how to protect yourself and the company from a cyberattack.



Those who have started working from home since the pandemic are more likely to have received training in the past year (60%) than those who have not been WFH (28%)

Number of employees	% Yes
1 to 10	20%
11 to 50	32%
51 to 100	45%
101 to 250	48%
251 to 1,000	50%
1,001 to 5,000	51%
5,001+	47%

Recommendations

Cyber awareness is working and that means we must keep learning. Success in cyber awareness and security culture shows users are clicking less on bad stuff which shows users are becoming more aware and suspicious.

A comprehensive cyber awareness training program helps an organization reduce the risk of becoming a victim of a cyberattack. The trend shows that employees are less likely to click on a malicious email than in previous years and indicates that they are being more cautious when it comes to email threats. We need to keep up the momentum and make employees one of our strongest defenses in our cybersecurity strategy, not one of our greatest weaknesses.

Meanwhile, it is imperative for security teams to be aware of gaps in understanding for employees and prioritize automated solutions that help to bridge the gap between risk awareness and risky behaviors.

RESOURCES

Cybersecurity for Dummies

This free eBook delivers a fast, easy read that describes what everyone needs to know to defend themselves and their organizations against cyberattacks – including simple steps everyone can take to protect themselves at work and at home.

6 Things Every Company Needs to Know for Cybersecurity Awareness Month

To improve cyber resilience, it's vital to focus on the effectiveness of security controls in the context of hackers' tactics, techniques, and procedures often called TTPs. There are six best practices, based on an analysis of threat actors' TTPs, that can improve cyber resilience without the need for more resources:

Cybersecurity ABCs: Delivering awareness, behaviors and culture change

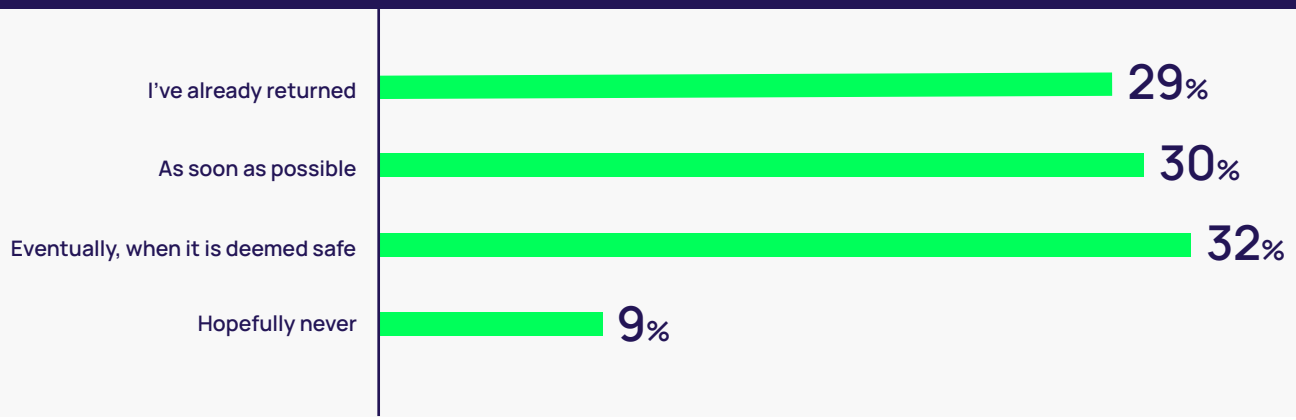
Delinea

When will employees return to the office?

Return to work in an office? Not just yet… – Just 29% of those that moved to remote working during the pandemic say that they have already returned to the office, although 50% of the respondents in France have returned to the office and only 11% in Canada. Canadians appear most reluctant to return at all, with 18% hoping never to do so, compared to the global average of 9%.

29% have already returned to the office, and just 9% hope never to do so

FIGURE 13 | When do you anticipate returning to the office? Please select one



Returning to office, by country

There is understandably a wide mix of responses by country when asked about returning to their offices, with half of respondents in France already having returned to the office. 18% of Canadians would prefer never to go back to the office, compared to 1% of Indians.

FIGURE 14 | When do you anticipate returning to the office? By country.

	Total	UK & Ireland	Sweden	Nether-lands	France	Spain	Germany	Australia & NZ	Singapore & Malaysia	India	Japan	USA	Canada
I've already returned	29%	27%	15%	27%	50%	42%	26%	39%	17%	25%	31%	33%	11%
As soon as possible	30%	28%	32%	29%	29%	30%	41%	26%	28%	45%	29%	26%	19%
Eventually, when it is deemed safe	32%	33%	46%	35%	16%	22%	26%	27%	50%	29%	26%	26%	52%
Hopefully never	9%	13%	6%	8%	5%	6%	7%	8%	5%	1%	14%	15%	18%
Base, n=	3954	505	201	295	231	266	429	407	355	374	188	457	246

CONCLUSION

Employees frequently sacrifice security for productivity. Their performance (and pay) is typically measured on getting the job done not their cybersecurity hygiene practices. Managing employee risks depends on how their manager or department goals and metrics are set. This means when balancing cybersecurity and productivity, they will most likely choose the productivity path as the logical choice even if it means sacrificing or exposing the company to a cybersecurity risk.

"When faced with a choice between productivity and cybersecurity employees will take the easy path and this mostly means sacrificing security"

Humans are curious by nature. Even when we suspect something is not quite right, we are still sometimes curious enough to click on it just to see the outcome. No matter how much training an organization gives to employees it will always have at least one employee who will click on something malicious. It only takes one employee with local admin privileges to click on a single malicious link and, only a matter of time before the attacker elevates privileges to full domain access to carry out a malicious cyberattack. Yes, it really only takes one employee to click, and it is game over.

"It only takes one employee with local admin privileges to click on a malicious link for attackers to be successful"

Organizations across the globe must strike the correct balance between people and technology to properly protect themselves from cyber threats. There is still too much complexity in the cybersecurity industry, and it is crucial that we make our solutions simpler and easier to use if we expect people to adopt them.

About the survey

The survey was conducted by Sapio Research among 8,041 knowledge workers from 15 countries in North America, Europe and Asia. The interviews were conducted online by Sapio Research in June 2021 using an email invitation and an online survey. At an overall level results are accurate to ± 1.1% at 95% confidence limits assuming a result of 50%.

Sapio Research is a London based B2B and consumer market research agency with an experienced team of researchers offering qualitative and quantitative research services and tools to help clients gain deeper insights. sapioresearch.com

Delinea

Defining the boundaries of access

Delinea provides seamless security based upon the principles of zero trust, least privilege, and just-in-time privilege elevation. If you're considering a migration to the cloud or worried that your existing cloud resources aren't properly protected, talk with one of cloud experts about PAM for the cloud.

Learn more about Delinea's solutions at **delinea.com.**