GLOBAL EDITION

THALES
Building a future we can all trust

2021 Data Threat Report

Data Security in the Era of Accelerated Cloud Transformation and Remote Work

#2021DataThreat

cpl.thalesgroup.com

Contents

About this study

The COVID-19 pandemic has had an immediate and dramatic impact on IT teams around the globe, and its long-term effects are still evolving. The 2021 Thales Data Threat Report study looked at various aspects of those impacts in a wide-ranging survey of security professionals and executive leadership that touched on issues ranging from COVID-19 and work-from-home (WFH) strategies to quantum computing.

451 Research

S&P Global
Market Intelligence

Source: 2021 Data Threat custom survey from 451 Research, part of S&P Global Market Intelligence, commissioned by Thales

Our sponsors are:

ARROW

SENETAS

versasec

KEYFACTOR

SYNNEX
WESTCON

Canon
Canon Marketing Japan Inc.

NTT DATA
NTT DATA INTELLILINK Corporation

F9C
Walking Together

FIRST TECH

Adistec

Key Findings

> “Only a fifth of respondents (20%) indicated that their security infrastructure was very prepared to deal with the disruption.”

Introduction and Key Findings

The last year may tempt us to hope for a return to some form of pre-pandemic security procedures. However, the 2021 Thales Data Threat Report, based on data from a survey of more than 2,600 respondents in more than 10 countries across the globe, will likely convince readers otherwise. There are lasting changes regarding perspectives on the attacker community, technology expectations, and priorities in security operations and investment. This report examines the implications of the survey responses and explores their meaning to security strategies and how organizations should plan for the year ahead.

COVID Changes Everything

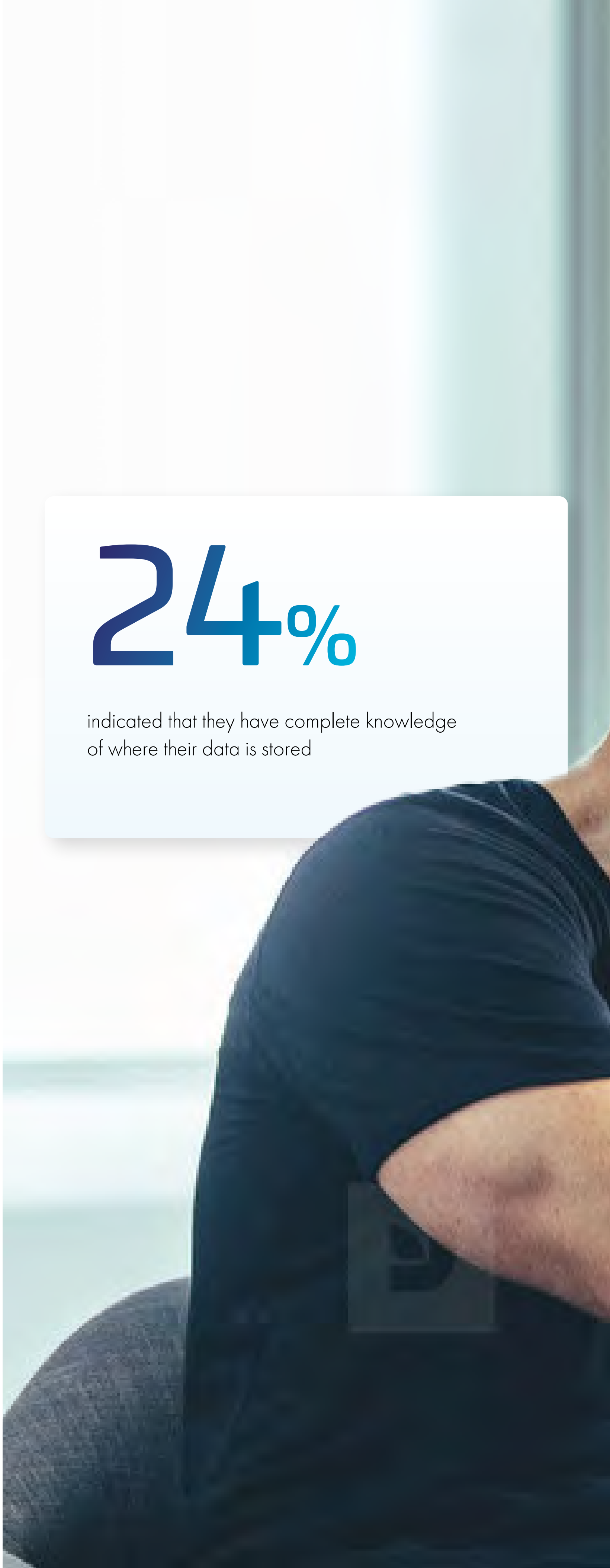
The COVID-19 pandemic forced many changes upon enterprises that caused ripple effect throughout the security community, which was evident in the survey responses. The shift to remote work and the subsequent accelerated use of cloud-based infrastructure have had profound impacts on security teams. Only a fifth of respondents (20%) indicated that their security infrastructure was very prepared to deal with the disruption. The shift to remote work was a large contributor to that disruption. Almost 82% of respondents were somewhat or very concerned about the security risks and threats that a greatly increased remote workforce poses. Almost half (44%) were not confident that their access security systems could effectively secure remote work.

Increased cloud consumption seems to have strained security operations as well. Data protection mechanisms such as encryption don't appear to be scaling up with the increased use of public cloud. The results show strong cloud use: 31% of respondents said that 41-50% of their workloads and data resides in external clouds, and 24% reported more than half. However, only 17% indicated that they have protected more than 50% of their sensitive data in cloud with encryption. There are some glimmers of hope in that regulated industries such as healthcare and financial services are doing better than average, but the situation clearly needs work.

Risks Increasing, Security Mindsets Unchanged

Survey results indicate that there is reasonable awareness of the risks present in today's environments, but they also show that most organizations need to improve their security posture. Many organizations have experienced the consequences of successful attacks, but technologies such as encryption and multi-factor authentication (MFA) have not reached saturation levels such that the majority of applications and data are fully protected. In addition, nearly half (47%) of respondents said they are concerned about the impacts of quantum computing, indicating that longer-term issues are weighing on security practitioners as well.

As more data is distributed and stored across hybrid and cloud environments, data discovery is becoming a greater issue. Only 24% of respondents indicated that they have complete knowledge of where their data is stored, which is troubling. In terms of security measures considered most effective, just 55% have implemented MFA in any form. Although 38% of respondents indicated that they believe encryption is the most effective technology in preventing cyberattacks, much cloud data remains unencrypted, as mentioned above. Awareness of the risks and an understanding of effective technologies to mitigate those risks haven't been enough to catalyze many organizations into action. This speaks to the challenges that exist in changing security infrastructure for the better.



24%

indicated that they have complete knowledge of where their data is stored

Some of those challenges may be caused by misalignment in the perception of security challenges and in investment priorities across job titles. Survey results show that, in matters of policy and effectiveness, there is a disconnect between executive, management and practitioner viewpoints. For example, if executives don't perceive security issues to be as severe as managers believe, there is likely to be a lack of urgency in driving security improvements.

The report explores the results in more detail and looks at the impacts on organizations as they navigate the complex security environment that they find themselves in today.

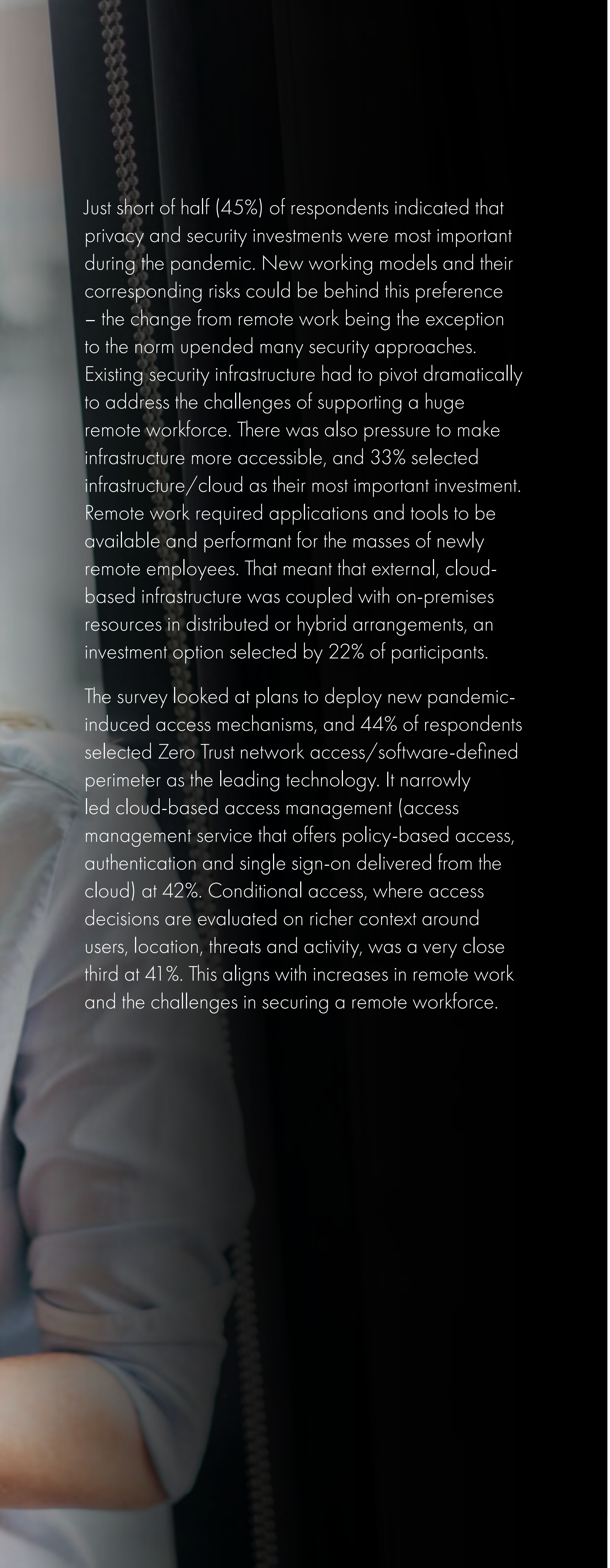
Key Findings

- Pandemic pressures are impacting security approaches and spending.
- Remote work is a risk that needs to be managed more effectively.
- There is significant momentum in cloud migration, but many necessary controls are lagging.
- Encryption use to protect sensitive data in cloud is low – a significant risk.
- Global awareness of changing risks is high, but this hasn't catalyzed organizations to address them.
- Breaches and their impacts weigh on security planning.
- Misalignment in understanding security impacts between management and practitioners could impact planning and budgeting.
- Traditional security concerns remain constant.
- The risks of quantum computing are raising concerns regarding security planning.

COVID Has Changed Security Strategies

The effects of the COVID-19 pandemic have roiled IT teams around the globe, and the impact on security is still evolving. The 2021 Thales Global Data Threat Report covers various aspects of those impacts and is based on data from a wide-ranging survey of more than 2,600 security professionals and executive leaders. We queried the panel about issues ranging from COVID-19 and cloud transformation to the threats of quantum computing to find out their current situation and how they plan to move forward.

The pandemic cast a long shadow over the security landscape, visible in its impact on remote working arrangements and hastening cloud migrations. When questioned about security infrastructure preparedness to handle pandemic-induced risks, 46% of respondents said that their infrastructure was not prepared (29% somewhat not prepared, 17% not at all prepared) at some level. Only 20% said that their infrastructure was very prepared, indicating that the new operational models brought on by the pandemic strained existing security infrastructure.



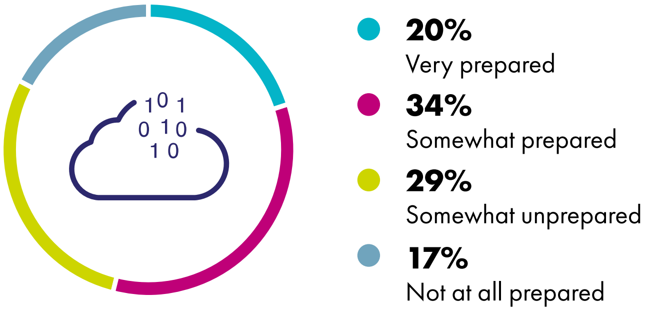
Just short of half (45%) of respondents indicated that privacy and security investments were most important during the pandemic. New working models and their corresponding risks could be behind this preference – the change from remote work being the exception to the norm upended many security approaches. Existing security infrastructure had to pivot dramatically to address the challenges of supporting a huge remote workforce. There was also pressure to make infrastructure more accessible, and 33% selected infrastructure/cloud as their most important investment. Remote work required applications and tools to be available and performant for the masses of newly remote employees. That meant that external, cloud-based infrastructure was coupled with on-premises resources in distributed or hybrid arrangements, an investment option selected by 22% of participants.

The survey looked at plans to deploy new pandemic-induced access mechanisms, and 44% of respondents selected Zero Trust network access/software-defined perimeter as the leading technology. It narrowly led cloud-based access management (access management service that offers policy-based access, authentication and single sign-on delivered from the cloud) at 42%. Conditional access, where access decisions are evaluated on richer context around users, location, threats and activity, was a very close third at 41%. This aligns with increases in remote work and the challenges in securing a remote workforce.

FIGURE 1

Preparedness of Security Infrastructure

Q: How prepared was security infrastructure to handle the range of risks associated with the new business operating environment caused by the pandemic?



Source: 451 Research's 2021 Data Threat custom survey

> “44% of respondents selected Zero Trust network access/software-defined perimeter as the leading technology.”

Era of Remote Working

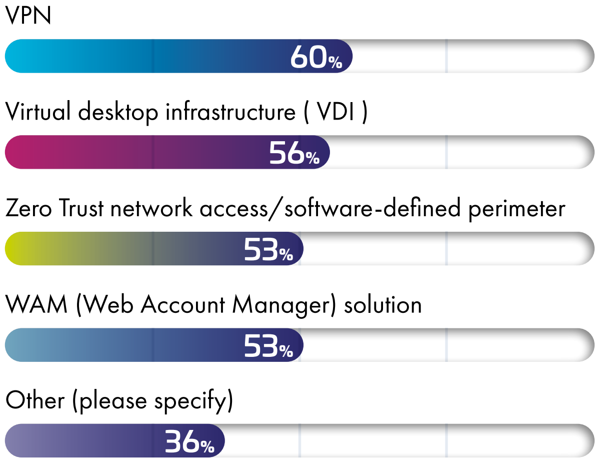
The pandemic created a huge push to implement remote work policies, but that shift to remote work created problems for security teams: 82% of respondents expressed some level of concern about the security risks/threats of employees working remotely (39% were very concerned and 43% were somewhat concerned). The percentage was even higher among US federal government respondents at 84% (34% very concerned and 49% somewhat). This is an indication of the level of caution with which respondents have approached the remote work risk, a concern echoed in a lack of confidence in their existing security controls. For example, 34% of global respondents were somewhat confident that their current access security products could effectively enable employees to work remotely in a secure and easy manner, but 44% were not confident at some level.

The lack of confidence may be due to the tools that are in place to manage remote working. When we asked how organizations were implementing remote access, traditional approaches dominated. VPN continues to lead with 60% of respondents selecting it as the primary method for remote access. Virtual desktop infrastructure (VDI from VMware, Citrix, others) was second (56%) and Zero Trust network access/software-defined perimeter ranked third (53%). That's a troubling result because traditional approaches often lack the granularity of control needed to effectively manage the much more diverse work patterns that the wholesale shift to remote work has required. Most traditional approaches were designed for tactical use in special cases and may not have received the comprehensive reviews needed to secure a much larger user population.

FIGURE 2

Current Remote Access Technologies

Q: How do employees currently access their applications remotely?



Source: 451 Research's 2021 Data Threat custom survey

Organizations should expect to invest time and resources to better understand the models of work that they'll be moving toward in the longer term. A separate 451 Research study found that remote work is expected to continue at high levels, and that there's growing acceptance that employees can work effectively in a remote setting. That means that organizations will need security controls and remote access mechanisms that can be effective in the hybrid working environments that organizations have begun to embrace.

69%

of enterprises indicate at least 75% of their workforce can work effectively remotely.

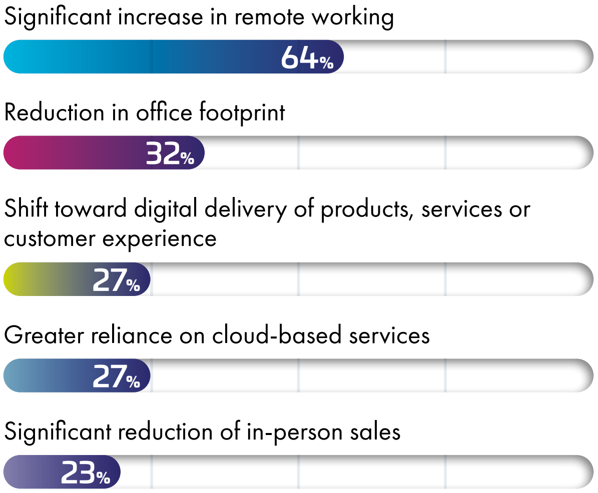
> "VPN continues to lead with 60% of respondents selecting it as the primary method for remote access."

FIGURE 3

COVID-19-Inspired Practices Become Permanent Policy

Q: Which, if any, of the following permanent changes has your organization made due to the influence of the coronavirus (COVID-19) outbreak? Please select all that apply. (n=378)

Base: All respondents



Source: 451 Research's Voice of the Enterprise (VotE): Digital Pulse, Coronavirus Flash Survey October 2020

> “An area of concern is the amount of sensitive data in cloud that isn’t encrypted.”

Cloud Momentum Accelerates

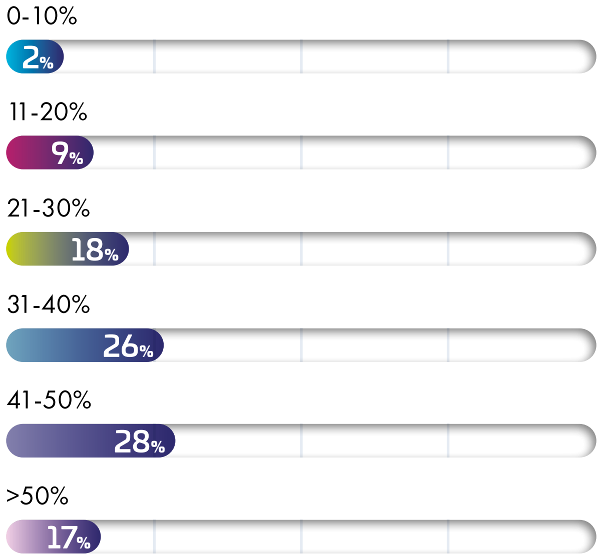
Respondents in the study are showing considerable use of cloud-based infrastructure, and this trend appears to be accelerating in the wake of the pandemic. Just under a third (31%) of respondents stated that 41-50% of their data is stored in external cloud, and 24% indicated more than 50% is stored there. That mirrors the data we have gathered in other 451 Research studies. The VotE Storage Data Management study found that over 60% of participants already had cloud storage in use. An area of concern is the amount of sensitive data in cloud that isn't encrypted. Survey results indicate that this could be explained by how cloud security policies are defined and implemented: not quite half (45%) have policies that are centrally defined, but technical standards and enforcement are left to individual cloud teams. This likely represents a troubling potential shift in the profile of cloud security stakeholders, making them more aligned with engineering-type concerns over traditional security concerns.

That could explain why 83% of respondents said that less than 50% of the sensitive data stored in cloud is encrypted. Only 17% of respondents stated that more than 50% of their sensitive data stored in cloud is encrypted. There is some improvement in regulated industries; for example, 33% of healthcare respondents said that 41-50% of data is encrypted.

FIGURE 4

Encryption of Sensitive Data in Cloud

Q: What percentage of your sensitive data in the cloud is encrypted?



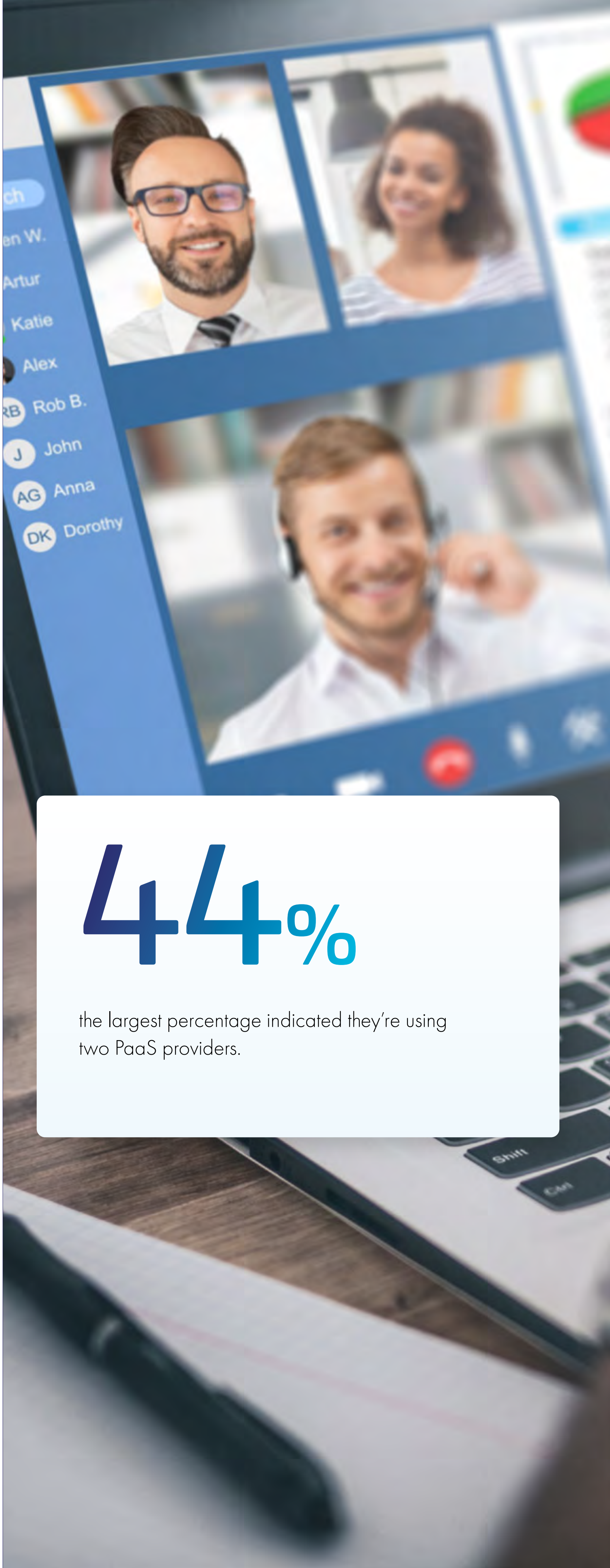
Source: 451 Research's 2021 Data Threat custom survey

While there is greater use of cloud infrastructure, 46% of respondents agreed that it is more complex to manage privacy and data protection regulations in a cloud environment than in on-premises networks within their organization (22% strongly agreed and 24% agreed). Several factors could drive this. Persistent skills gaps in both security and cloud infrastructure have strained security teams as they deal with increases in cloud use. In the most recent 451 Research VotE Information Security study, cloud platform expertise was the highest reported security skills gap. Adapting traditional security strategies and teams to cloud operational models is also a complex endeavor.

Most Firms Using a Multicloud Strategy

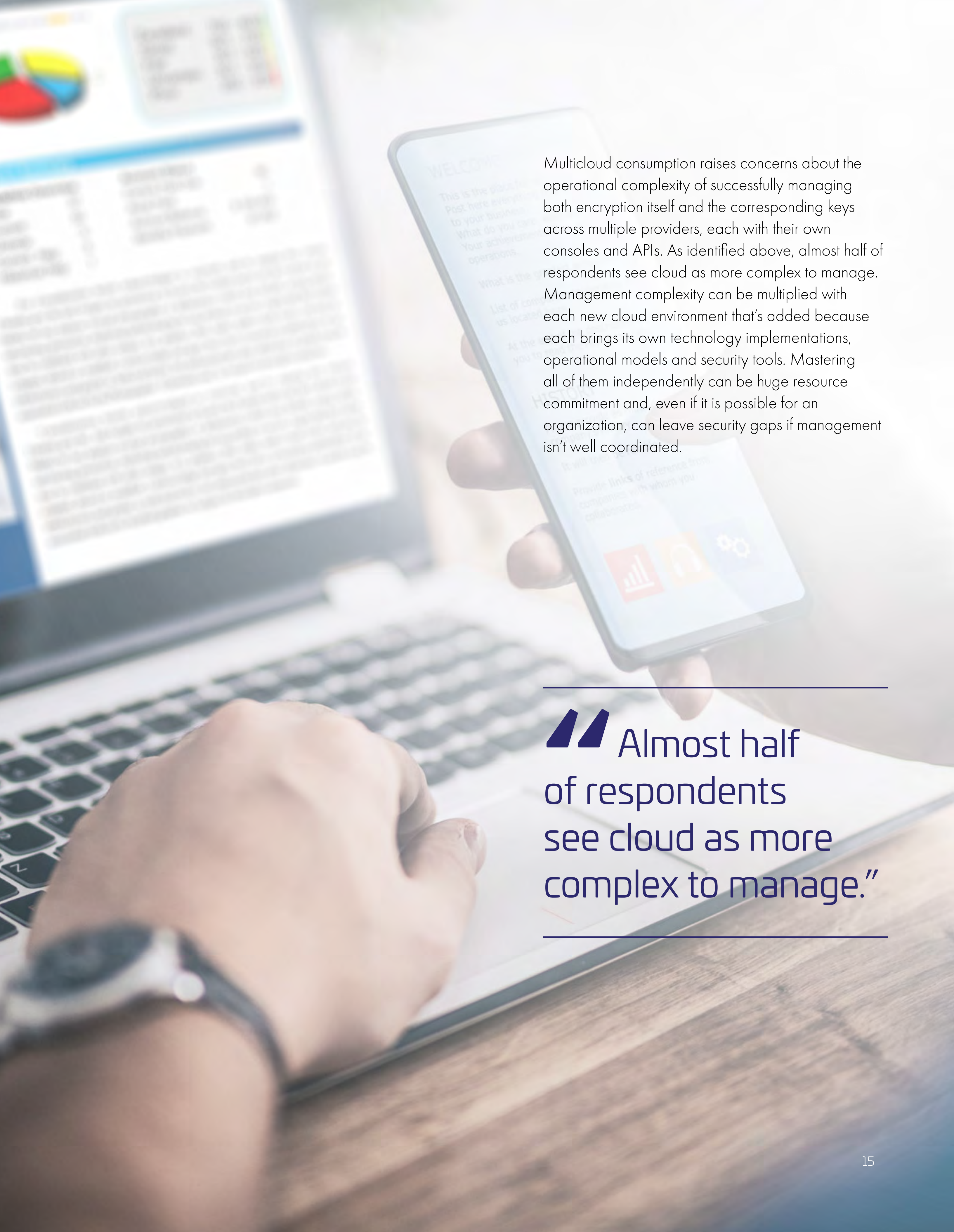
The nature of cloud use is evolving alongside the increase in use. The 2021 Thales Data Threat Report explored the extent to which participants are using multiple cloud providers. Organizations are already using multiple providers for infrastructure as a service (IaaS). Some 53% of respondents employ AWS as their IaaS provider and 41% Microsoft Azure with considerable overlap across Google Cloud, IBM Cloud, Oracle and Alibaba. The number of platform-as-a-service (PaaS) providers organizations are leveraging is more measured. The largest percentage indicated they're using two (44%) PaaS providers. Some 21% identified that they use three PaaS providers. The use of multiple SaaS-delivered applications was, not surprisingly, much higher, with 27% using more than 50 SaaS apps and 16% using 51-100 SaaS applications.

> **"Organizations are already using multiple providers for infrastructure as a service (IaaS)."**



44%

the largest percentage indicated they're using two PaaS providers.



Multicloud consumption raises concerns about the operational complexity of successfully managing both encryption itself and the corresponding keys across multiple providers, each with their own consoles and APIs. As identified above, almost half of respondents see cloud as more complex to manage. Management complexity can be multiplied with each new cloud environment that's added because each brings its own technology implementations, operational models and security tools. Mastering all of them independently can be huge resource commitment and, even if it is possible for an organization, can leave security gaps if management isn't well coordinated.

> “Almost half of respondents see cloud as more complex to manage.”

Breaches and Their Impact

Arguably, the ultimate strength of an organization's security protections is preventing breaches. Respondents reported breaches at a relatively high rate, with 56% globally identifying a security breach at some point. Out of these, 41% said they experienced a breach in the last 12 months. The high percentage of recent breaches could be an indication that organizations face challenges meeting improved attacker techniques.

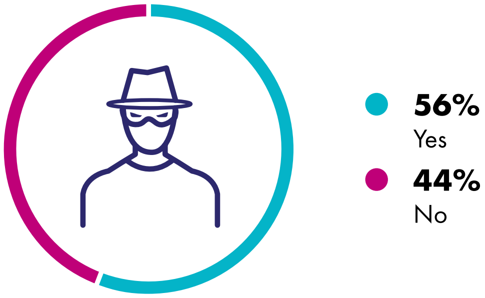
A deeper look at some demographics of the breach data found that:

- More than half (56%) of US respondents reported experiencing a breach, 47% in the last 12 months, slightly higher than the global average.
- From a vertical perspective, globally:
    - ◊ Retail ranked first with 71% of respondents saying they experienced a breach at some point and 39% in the past 12 months.
    - ◊ More than half (58%) of financial services respondents said they have experienced a breach at some point vs. 29% in the last year, possibly an indication that the higher levels of security investment typically associated with the financial services sector could be paying off in lower breach rates.

FIGURE 5

Prevalence of Breaches at Organizations

Q: Has your organization ever been breached?

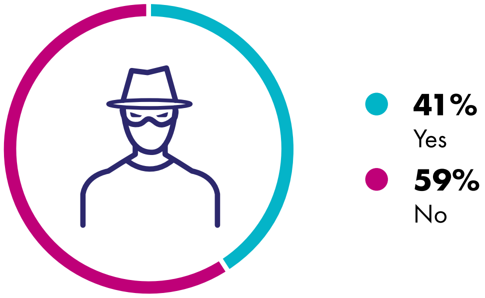


Source: 451 Research's 2021 Data Threat custom survey

FIGURE 6

Prevalance of Recent Breaches

Q: Has your organization been breached in the past 12 months?



Source: 451 Research's 2021 Data Threat custom survey

One encouraging report finding was that 46% of respondents said that they have avoided a breach notification because leaked data was encrypted or tokenized (54% of respondents said they had not). That's an indication that the growing use of data protection technologies could reduce one of the impacts of a breach event. Comparatively, 36% of global respondents had to issue a breach notification because a breach occurred.

The use of cloud-based infrastructure exposes new risks as an organization's data footprint expands. The survey also looked at breaches tied to cloud; 40% reported that they had experienced a breach in their cloud environments. That aligns with the percentage identifying a breach in the last 12 months, possibly mirroring their total breach exposure. The survey found that there is a lack of maturity in cloud data security with limited use of encryption, which might imply that there are other security management gaps, such as separating data from the keys used to encrypt it and other fundamentals.

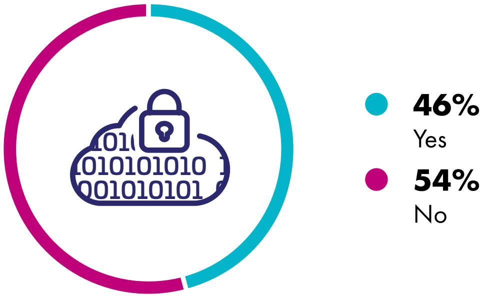
46%

of respondents said that they have avoided a breach notification because leaked data was encrypted or tokenized

FIGURE 7

Avoiding Breach Notification Process Due to Encrypted Data

Q: Have you ever avoided a breach notification process (e.g., encryption safe harbor) because the stolen or leaked data was encrypted or tokenized?

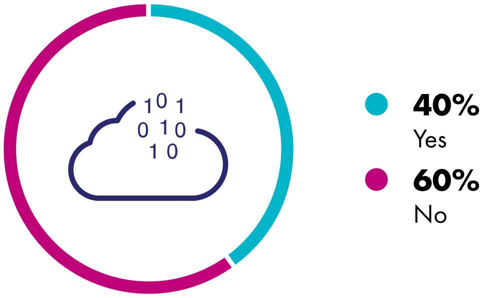


Source: 451 Research's 2021 Data Threat custom survey

FIGURE 8

Data Breach in Cloud

Q: Has your organization ever experienced a data breach involving data and applications that reside in the cloud?



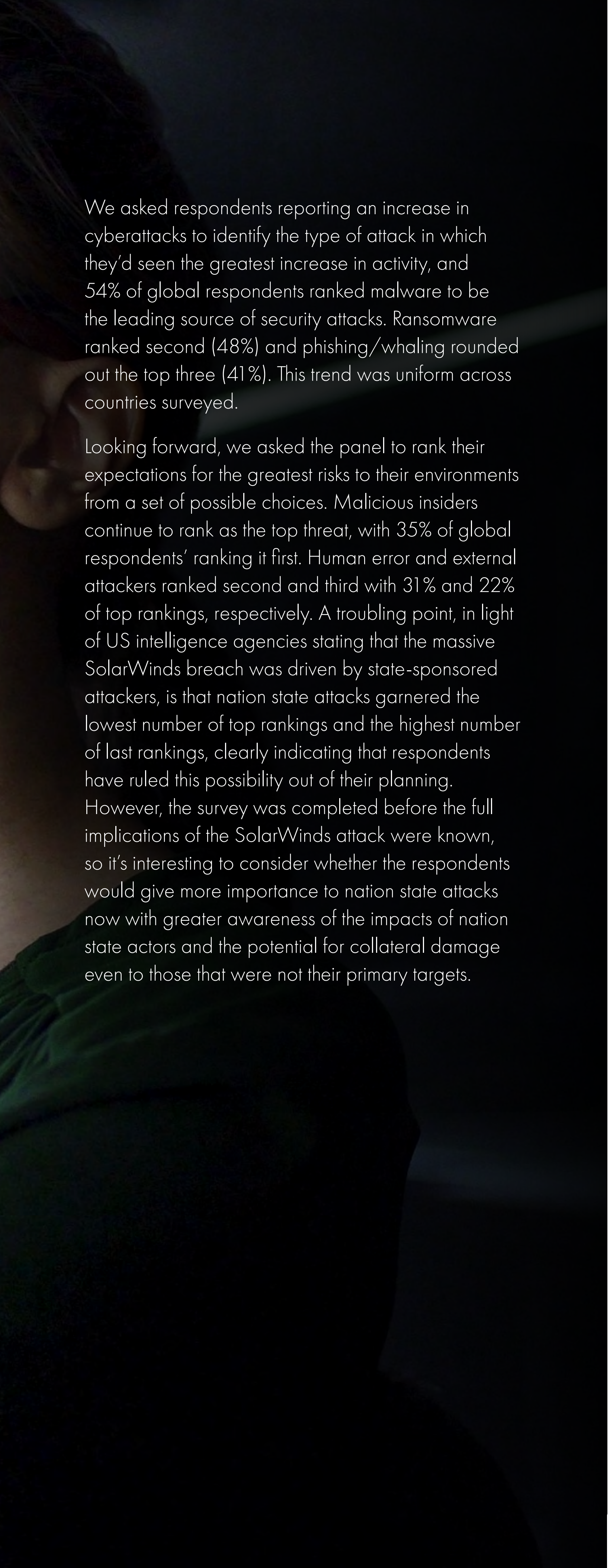
Source: 451 Research's 2021 Data Threat custom survey

Security Threats

Breaches are a trailing indicator of security effectiveness. The survey also examined forward-looking metrics, including perceptions about security threats. The panel was asked to identify levels of attack activity and understanding about attack risks. Almost half (47%) of respondents reported seeing an increase in the volume, severity and/or scope of cyberattacks in the past 12 months. There were some reported global hotspots: Australia, New Zealand and the Netherlands reported significantly more (52%, 63% and 60%, respectively).

One concerning aspect of the data is the notable difference in perceptions of attack rates by organizational role. Those who are more likely dealing directly with the impacts of greater attack density reported higher levels of activity than those in senior roles, who are generally more removed. Over half (56%) of practitioners reported an increase, but only 46% of managers, and only 40% of senior management reported an increase. If senior management is unaware of increases, it could be more difficult to fund efforts to strengthen cyber defenses or realign organizational priorities. This is a caution to executive teams to increase their understanding of the situation on the ground in their environments to ensure that they're not underinvesting in their defenses.

> **“56% of practitioners reported an increase, but only 46% of managers, and only 40% of senior management reported an increase.”**



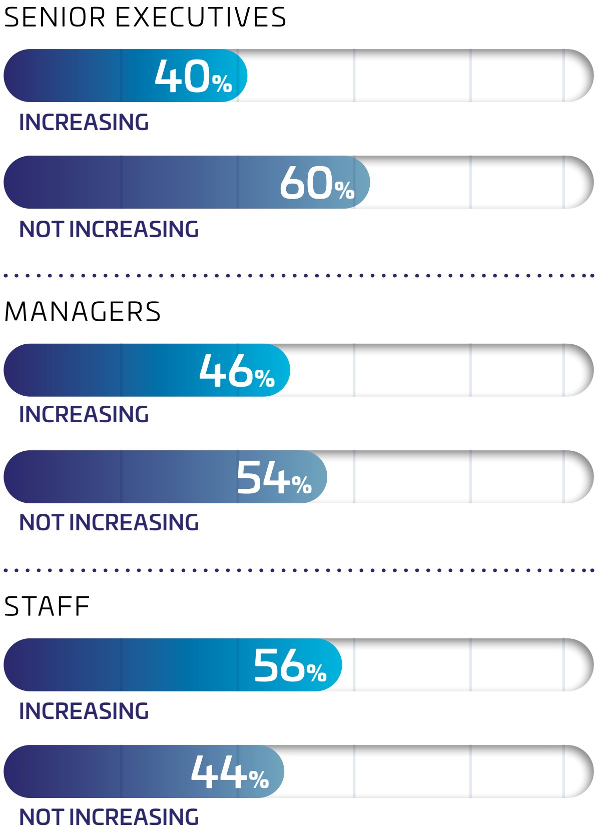
We asked respondents reporting an increase in cyberattacks to identify the type of attack in which they'd seen the greatest increase in activity, and 54% of global respondents ranked malware to be the leading source of security attacks. Ransomware ranked second (48%) and phishing/whaling rounded out the top three (41%). This trend was uniform across countries surveyed.

Looking forward, we asked the panel to rank their expectations for the greatest risks to their environments from a set of possible choices. Malicious insiders continue to rank as the top threat, with 35% of global respondents' ranking it first. Human error and external attackers ranked second and third with 31% and 22% of top rankings, respectively. A troubling point, in light of US intelligence agencies stating that the massive SolarWinds breach was driven by state-sponsored attackers, is that nation state attacks garnered the lowest number of top rankings and the highest number of last rankings, clearly indicating that respondents have ruled this possibility out of their planning. However, the survey was completed before the full implications of the SolarWinds attack were known, so it's interesting to consider whether the respondents would give more importance to nation state attacks now with greater awareness of the impacts of nation state actors and the potential for collateral damage even to those that were not their primary targets.

FIGURE 9

Attack Perceptions Differ

Q: Have you seen an increase in the volume, severity and/or scope of cyberattacks in the past 12 months?



Source: 451 Research's 2021 Data Threat custom survey

Security Threats Continued

The investigation also asked respondents to identify what they felt were the biggest targets for cyberattacks. Globally, third-party vendor networks ranked first the most often (38%). Web applications and cloud-based storage were close behind at 37%. The rankings were very closely grouped. In ranked vote scoring, cloud databases scored highest, with total accumulated first and second rankings, but this wasn't a strong lead. Cloud-delivered and cloud-hosted applications were closely matched with on-premises legacy applications and on-premises databases. But the high ranking of cloud as a target illuminates the inconsistency, discussed both above and below, between identifying the threat and mitigating it with encryption. Respondents identified end-user devices as slightly lower risk. To that end, headlines about data losses from lost laptops seem to have decreased, perhaps indicating propagation of best practices such as laptop full-disk encryption. IoT devices received the largest number of last-place rankings, belied by the latest headlines on crucial vulnerabilities in embedded TCP/IP stacks.

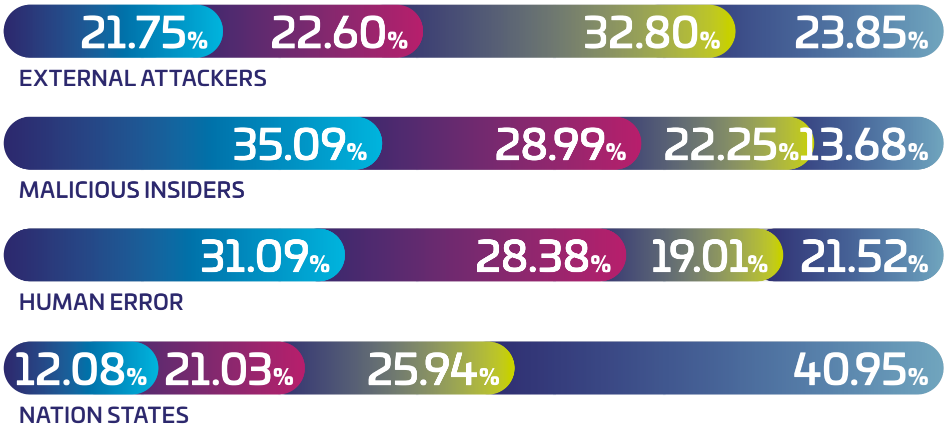
> " The investigation also asked respondents to identify what they felt were the biggest targets for cyberattacks.

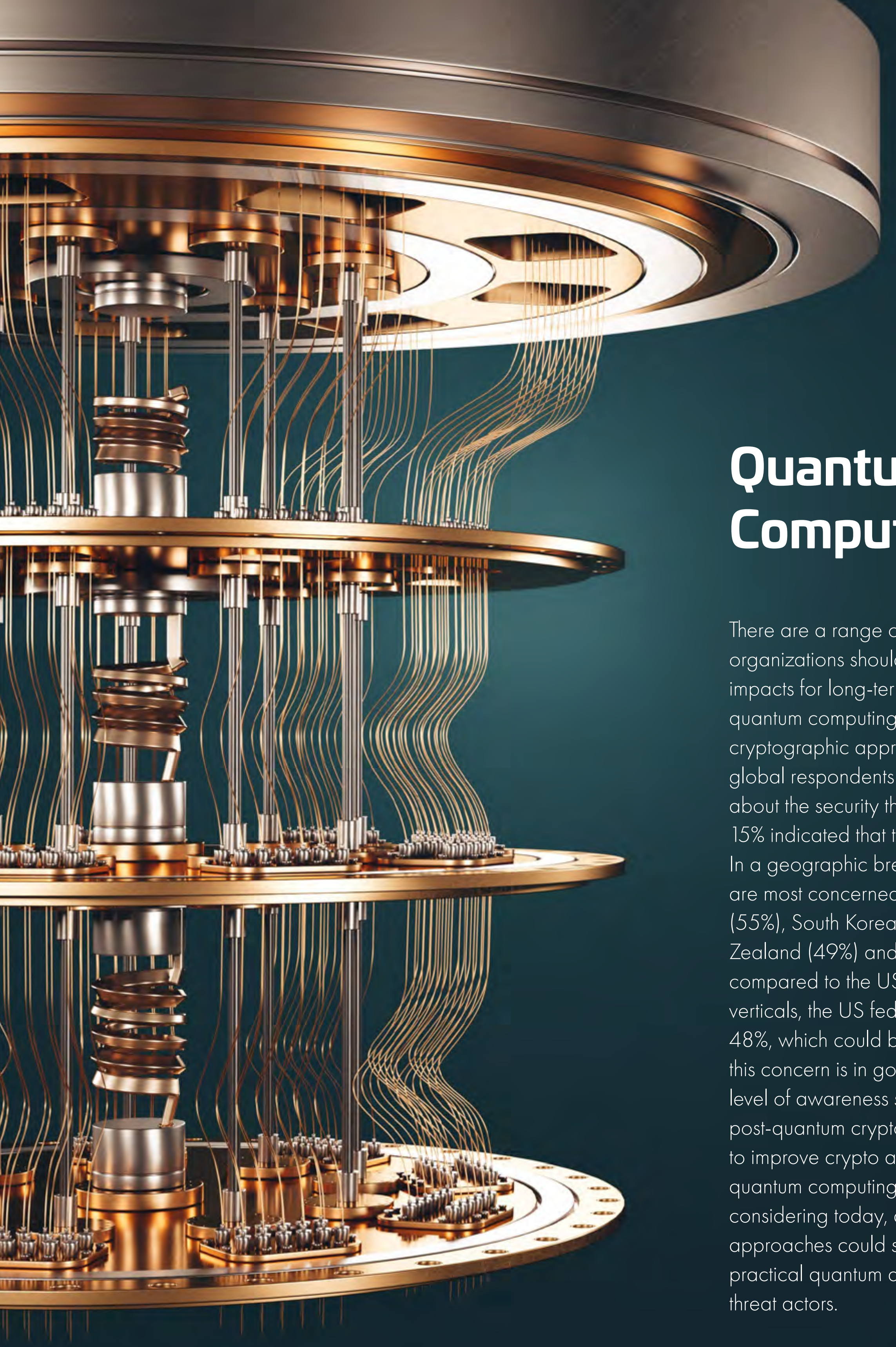
FIGURE 10

Perceptions of Greatest Threats

Q: Which types of threats do you see as the greatest?

● Rank 1 ● Rank 2 ● Rank 3 ● Rank 4





Quantum Computing

There are a range of forward-looking risks all organizations should plan for. One that has significant impacts for long-term data security is the arrival of quantum computing and its potential to break current cryptographic approaches. Nearly half (47%) of global respondents said they are very concerned about the security threats of quantum computing. Only 15% indicated that they are unconcerned at any level. In a geographic breakdown, Australian participants are most concerned (58%), followed by Hong Kong (55%), South Korea (53%), Singapore (52%), New Zealand (49%) and UAE (51%) and were outliers compared to the US and Western Europe. In industry verticals, the US federal government led the field with 48%, which could be an indication of how pervasive this concern is in government sectors broadly. This level of awareness should be generating interest in post-quantum cryptographic techniques and efforts to improve crypto agility. These are approaches to quantum computing risk that organizations should be considering today, as data protected with vulnerable approaches could still be valuable by the time that practical quantum decryption becomes available to threat actors.

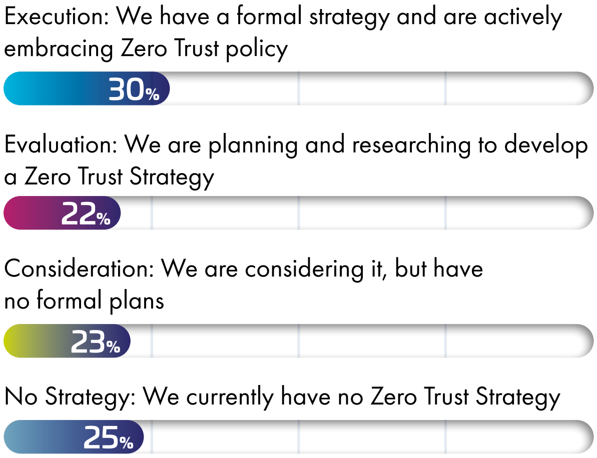
Zero Trust Goes Mainstream

Organizations are working to adapt their security strategies to address the changes in the threat models that they face. The study looked at aspects of Zero Trust and the ways in which they are being incorporated into operational security plans. When asked about their Zero Trust strategies, 30% of respondents said they have a formal strategy and have actively embraced a Zero Trust policy. Interestingly, those with a formal Zero Trust strategy are less likely to have been breached.

FIGURE 11

Zero Trust Status

Q: Where are you on your Zero Trust journey?



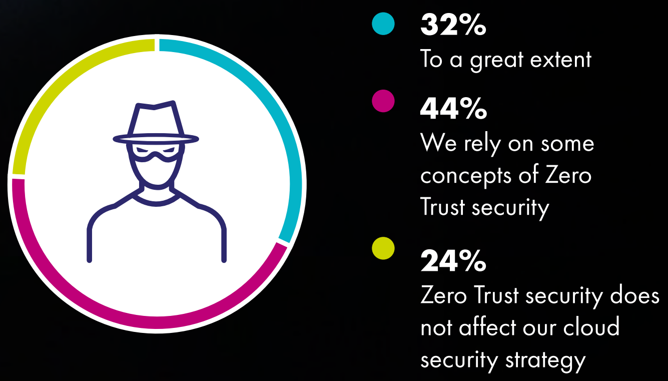
Source: 451 Research's 2021 Data Threat custom survey

We also examined the impact of Zero Trust approaches on cloud, and 32% of global respondents said Zero Trust security shapes cloud security strategy to a great extent. In comparison, the US reported lower levels at 26%. Germany was at 35%, Sweden at 38% and France at 34%. Japan led the country trend with 40%. Among industry verticals, 41% of financial services respondents said Zero Trust security shapes cloud security strategy to a great extent. However, 76% of all respondents said their cloud strategy relies to some degree on Zero Trust and Zero Trust security (combining 'great extent' and 'some extent' responses). That rolled up to 83% of financial services respondents and 77% of retail. The US was close behind at 75%, but Brazil ranked higher with 79%, and the UK was 78%. Only 24% of respondents indicated that Zero Trust does not affect their cloud security strategy.

FIGURE 12

Importance of Zero Trust to Cloud Security Strategy

Q: To what extent does Zero Trust security shape your cloud security strategy?



Source: 451 Research's 2021 Data Threat custom survey

Security Spending Misalignments

The study found that respondents' technology spending priorities and their perspectives of technology effectiveness were not fully aligned. DLP ranked first (39%) in spending priority, followed by encryption/key management with 36% and DevSecOps tools with 35%. Cloud security came very close at 34%. However, 38% of respondents selected encryption as the most effective option for protecting sensitive data. Endpoint security was second (36%) and then tokenization (35%).

Data Protection Management Strategies

Given the effectiveness of data encryption and tokenization for data protection, the foundation of data protection then rests on a combination of encryption effectiveness and key management strategies. As we've noted earlier, there is room to expand the use of encryption among the study respondents, but without better key management, increases won't improve the overall data security posture. The study looked at the current state of respondents' environments and how they're managing this important area of security operations. Not surprisingly, many indicated that they have deployed a number of encryption key management techniques. The organic growth of various approaches and the mashups created through corporate mergers and acquisitions can create a complex operational landscape that can pull together different approaches to key management and hardware security modules alongside homegrown systems and spreadsheets or flat files. Well over a third (40%) of respondents indicated that their organization currently deploys five to seven key management products, and 14% of respondents said that that they employ 8-10 key management products. The larger the number of systems in place, the greater the risk for error and the more work required to manage the combination successfully.

When we looked at tactics for data protection in cloud, encryption was the leading choice with 63% of respondents indicating that it is in place. Interestingly, 57% said that they are using key management. Using encryption without managing the keys indicates a lack of maturity in data protection implementation and leaves unaddressed risks open. It's important for organizations to understand that simply turning on protections like encryption without managing all of the aspects needed to ensure secure use will leave them open to abuse. Encryption needs to be applied with a knowledge of users, processes and applications to be effective against various threats. There needs to be partitioning of identity and techniques to address ransomware attacks or breaches caused by stolen privileged user credentials. Native cloud encryption offerings typically lack these protections. Bring-your-own-encryption (BYOE) is an approach that can offer the controls and protections needed to mitigate these risks.

In looking at industry demographics, the financial services vertical reported high levels of encryption use, at 68%, but lower key management use, at 49%. Financial services respondents indicated greater user of tokenization at 53% and MFA at 50%. Healthcare also led with encryption at 61% and reported key management at 55%.

There is a significant disconnect between interest and action. While respondents identified encryption as the most important tool for data protection, 83% reported that at least half of their sensitive data in the cloud is unencrypted.

Cloud Data Protection

Given the high rate of multicloud consumption, the responses to survey questions about cloud data protection revealed interesting responses. The survey asked about how respondents were encrypting data in IaaS and PaaS offerings that they used. A relatively small number (18%) said they rely exclusively on the provider's offerings. The largest number (37%) indicated a blend of their own capabilities and 'mostly' the provider's. That could be an indication that there is a growing understanding of the importance and value that BYOE offers, as mentioned above. Another 14.6% said they use BYOE exclusively, and 21% use mostly their BYOE, meaning that over a third (36%) are putting BYOE to work today. Another driver of BYOE can be the need to centralize data access policies and encryption key management across multiple clouds and on-premises environments. This is only possible with BYOE.

In looking at cloud key management, the results showed a similar, encouraging situation. While respondents reported blended use favoring the provider's key management systems as the leading situation today at 34%, they also reported strong use of external key management at 34% (21% mostly and 12% use all their own). Exploring how that third was accomplishing key management, more than half said they are managing them in cloud consoles (52%). Multiple options are in use, with some respondents leveraging more than one. Well over a third (40%) are managing keys through their own bring-your-own-key (BYOK) system, and 31% are using a cloud-based service. A hold-your-own-key (HYOK) approach is being used by 26%, while 34% generate their own key material but use the provider management system. The healthcare vertical parallels the average, but financial services, retail and government respondents indicated a much stronger preference for using their own BYOK systems, at 49%, 54% and 48%, respectively.

Despite the early state of cloud data protection in place, as mentioned above, a lower number (40%) of respondents reported having experienced a data breach in the cloud relative to all breaches. Retail reported a higher ever-breached rate of 52% compared to healthcare and financial services (38.2% and 43.6%, respectively). Regionally, Sweden (50%) and Netherlands (52%) claimed to have experienced a data breach in the cloud. For those who experienced a breach in cloud, 43% of respondents experienced a breach or failed an audit involving data and applications stored in the cloud this past year. Retail reported the highest level, with 61% of respondents stating they experienced a cloud breach in the past 12 months. Geographically, US respondents reported 48%, UK 52% and Australia 51%.

Moving Ahead

The results of the survey can serve as an indicator of useful paths for organizations to follow as they look to their security journey. One of the overarching takeaways that was driven by lessons learned from the pandemic is that security strategists need to increase the agility of their security controls. Infrastructure will become more hybrid, and security teams must have the capabilities to address this more complex environment efficiently. Controls and security management will have to extend to cloud in ways that keep each cloud environment from being an isolated operational realm.

The native controls and protections available in cloud environments address a set of necessary capabilities, but they're often insufficient to deliver effective protections for sensitive data and workloads, especially when it comes to compliance with regulations such as GDPR and the implications of the Schrems II ruling. Organizations need to increase their use of encryption and ensure they take full advantage of encryption's benefits by controlling the secrets that protect their data through BYOK, HYOK or BYOE approaches.

Organizations also need to make internal changes to ensure that personnel at all levels understand the security challenges and to properly align investment priorities. Senior executives need to ensure that they obtain a more complete understanding of the levels of risk and attack activity that their front-line staff are experiencing. They can't make effective strategy and security investment decisions when perspectives across the organization aren't aligned. This is especially true as regulatory changes and the potential for nation state collateral damage force them to move ever faster.

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com/data-threat-report