The Cloud Balancing Act for IT: Between Promise and Peril

CSA cloud security alliance℠ | skyhigh

Table of Contents

EXECUTIVE SUMMARY 2

ONBOARDING CLOUD SERVICES 3

SYSTEMS OF RECORD: THE NEXT WAVE OF CLOUD ADOPTION 6

A CULTURE OF COMPLIANCE AND THE ROLE OF THE CISO 9

EMERGING THREATS AND COMPLIANCE REQUIREMENTS 15

SECURING DATA IN THE CLOUD 19

SURVEY RESPONDENTS 22

ACKNOWLEDGEMENTS 24

Executive Summary

Cloud applications offer numerous benefits including lower cost, faster implementation, and a better user experience. The line of business is driving this technology shift in an unprecedented way, with end users frequently asking IT professionals within their companies for new cloud-based applications. Companies have responded with formal programs to assess and onboard cloud services, and the majority of companies have plans to expand support for cloud. While cloud adoption may have started with cloud-native systems of engagement, we're entering a new phase in which companies migrate their systems of record to the cloud.

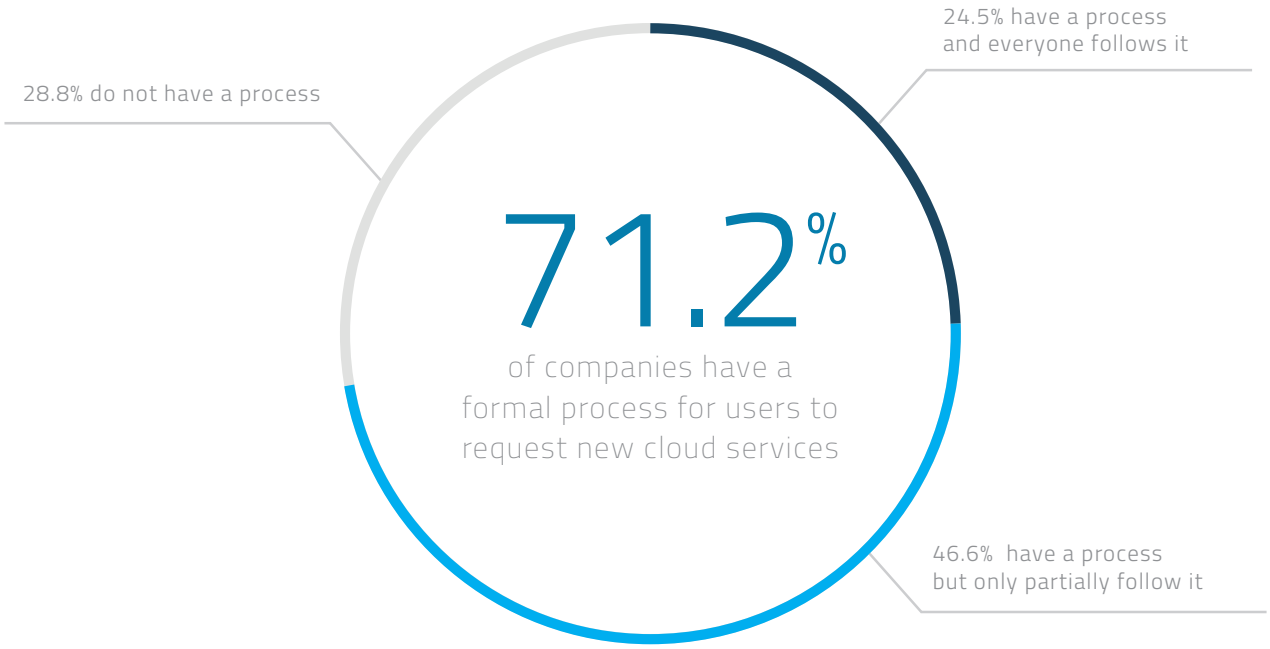
As data leaves the company data center for the cloud, IT is caught between delivering technologies to support innovation and growth in the business and securing sensitive data against proliferating threats. This survey explores the trends that are reshaping the role of IT and its relationship to the line of business as companies move to the cloud.

KEY FINDINGS INCLUDE:

- 24.6% of companies would be willing to pay a ransom to hackers to prevent a cyber attack and 14.0% would pay more than $1 million
- The top barrier to stopping data loss in the cloud is a lack of skilled security professionals – is security analyst the next hot job opportunity?
- Customer relationship management (CRM) is the most widely used cloud-based system of record today, but companies have plans to move other systems to the cloud
- Cloud confidence rising: 64.9% of IT leaders think the cloud is as secure or more secure than on-premises software
- CISOs play an important role in security – having one makes a company more likely to take steps to prepare for a cyber attack

Onboarding Cloud Services

Employees and the line of business are key elements in driving corporate cloud adoption. IT professionals we surveyed receive, on average, 10.6 requests each month for new cloud services. Even considering there is likely overlap in these requests, that's a tremendous number of cloud services that must be vetted. Perhaps that's why 71.2% of companies now have a formal process for users to request new cloud services. However, these programs are still evolving. Of companies with a formal process, 65.5% indicated that they only partially follow it.



It takes, on average, 17.7 days for a security team to evaluate a cloud service requested by the business

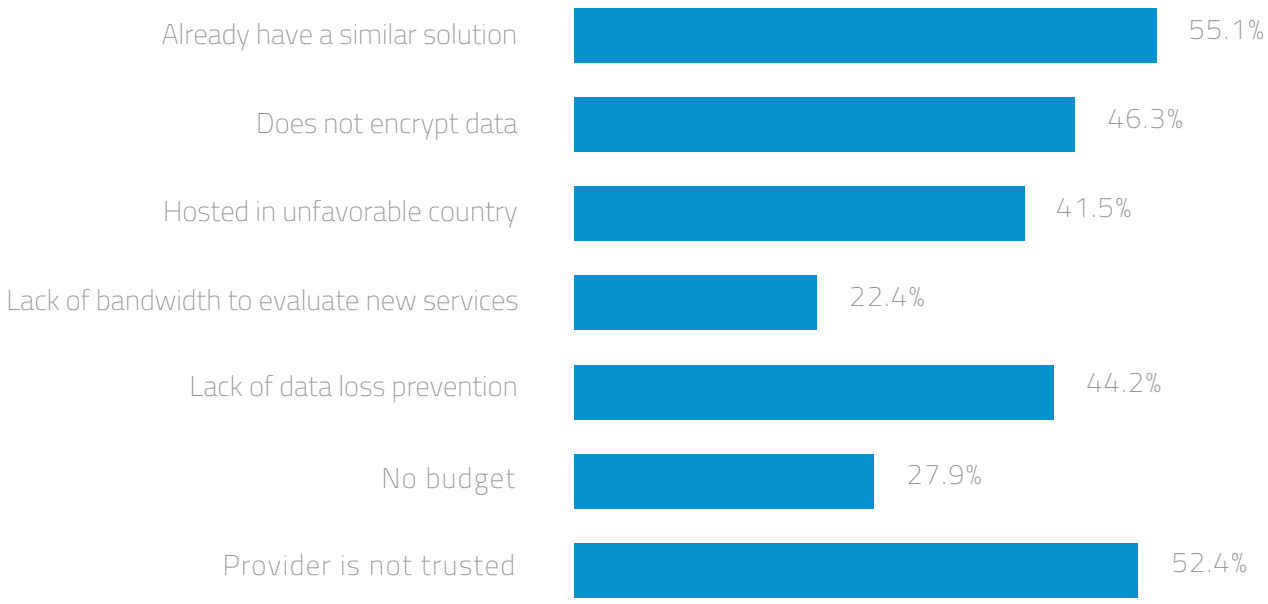
Having a formal process can help companies better respond to the large number of requests they receive each month for new cloud projects. On average, it takes an IT security team 17.7 days to evaluate the security of a cloud provider. However, 55.5% of companies are able to make a decision without a security evaluation because they already have a comparable cloud solution in place, the most common reason for rejecting a request. The next most common reason for rejecting a cloud service request is the provider is not trusted (53.6%), followed by a lack of encryption at 45.8% and a lack of data loss prevention at 43.9%.

Smaller companies, defined as those with fewer than 5,000 employees, were more likely to decline a cloud service request due to a lack of budget (28.4%) compared with companies with more than 5,000 employees (23.5%). Smaller companies were also more likely to decline a request because they already had a similar solution (54.5% versus 48.5%). At the same time, larger companies were more likely to reject a service because it didn't encrypt data (51.5%) versus smaller companies (37.5%). Larger companies were also more likely to decline a request because the service did not support data loss prevention (44.1% versus 39.8%).

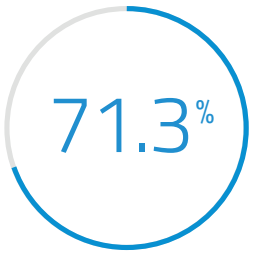
IT professionals receive, on average, 10.6 requests for new cloud services each month

Rejecting Cloud Service Requests

PERCENTAGE OF RESPONDENTS INDICATING
TOP REASON FOR REJECTING A SERVICE



As quickly as companies are responding to requests to enable cloud services, they may not be responding quickly enough or sufficiently to meet the demand. An overwhelming majority of IT professionals surveyed, 71.3%, say their companies have plans to offer more support for cloud to the lines of business. Much of the attention on cloud adoption has been focused on innovative social media, file sharing, content sharing, and communication applications. However, most businesses also rely on back end systems that at their core maintain records on employees, customers, and materials as they move through the supply chain. Companies are beginning to move these applications to the cloud as well.



Of companies have plans to offer greater cloud support to the line of business

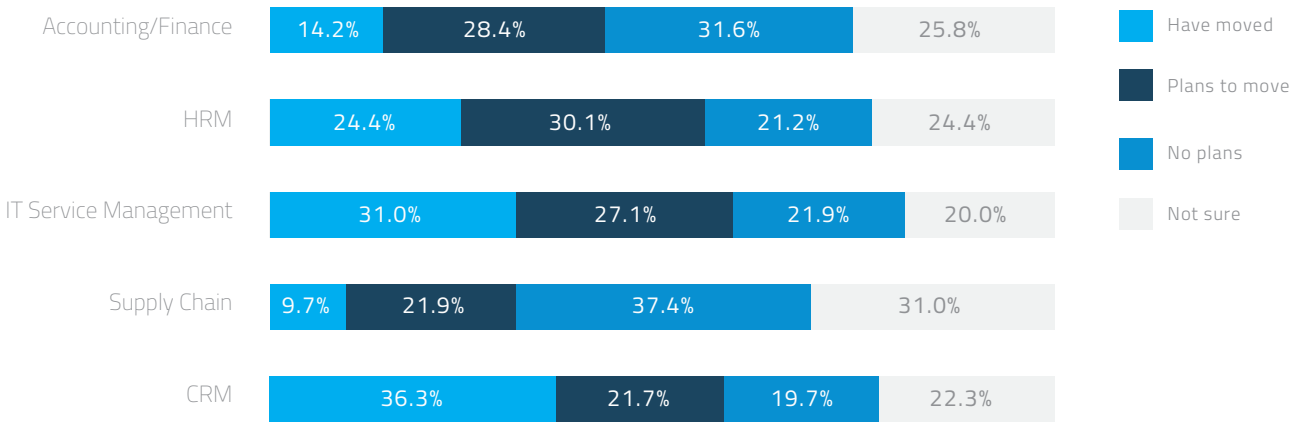
Systems of Record: The Next Wave of Cloud Adoption

In 2011, Geoffrey Moore introduced the concept of systems of engagement and predicted they would be the next wave in enterprise IT. Systems of record, which capture every dimension of data relevant to a company and process that data, were the focus of information technology initiatives last century. The new focus, he said, was on systems of engagement that enabled greater collaboration and communication. These new tools allow users to share files and information and communicate in real time via video and chat, and they were built from the ground up to run in the cloud.

Fast-forward a couple years and Moore's prediction appears prescient. Companies have invested in a new generation of communication and collaboration tools that are cloud-native. However, as more companies experience the benefits of cloud computing, they are beginning to look toward extending these benefits to their systems of record. Systems of record, far from being left behind in legacy on-premises data centers, are starting to move to the cloud. The most common system of record to be deployed in the cloud today is customer relationship management (CRM) solutions and 36.3% of companies now use a cloud-based CRM.

Systems of Record

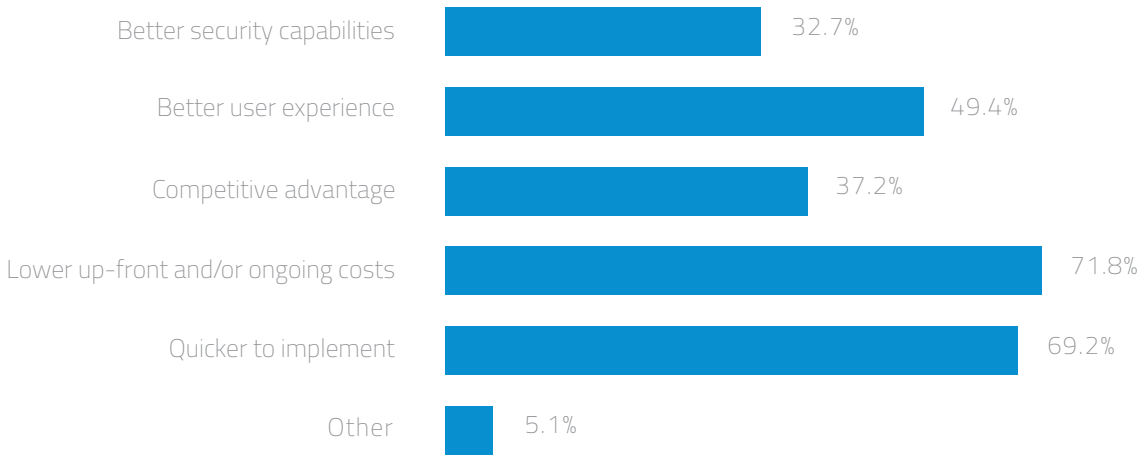
PERCENTAGE OF ORGANIZATIONS AT
EACH STAGE OF MIGRATION TO THE CLOUD



CRM is followed by IT service management, a category that includes applications like ServiceNow, with 31.0% of companies using a cloud-based IT service management application. Next, 24.4% of companies have moved their human resources management (HRM) application to the cloud. Some companies also have plans to use cloud-based systems of record. 30.1% of companies are planning to move their HRM solution to the cloud and 27.1% plan to move their IT service management solution to the cloud. While only 14.2% of companies use a cloud-based accounting/finance application, 28.4% plan to move to one.

Benefits of the Cloud

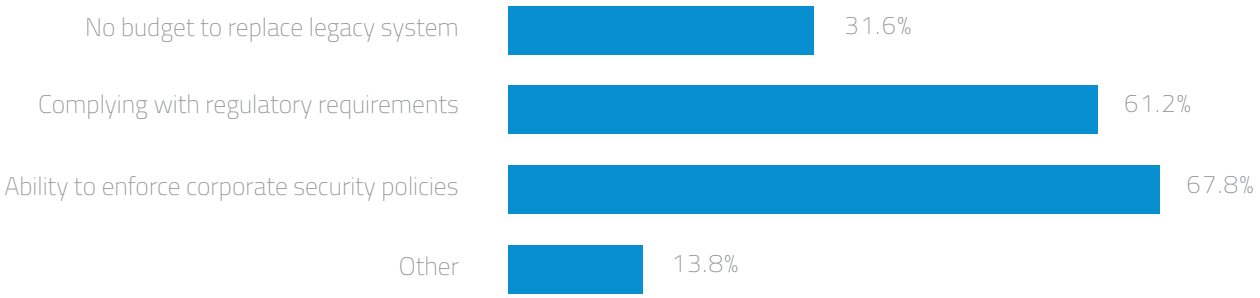
PERCENTAGE OF RESPONDENTS EXPERIENCING
BENEFIT OF MOVING SYSTEM OF RECORD TO THE CLOUD



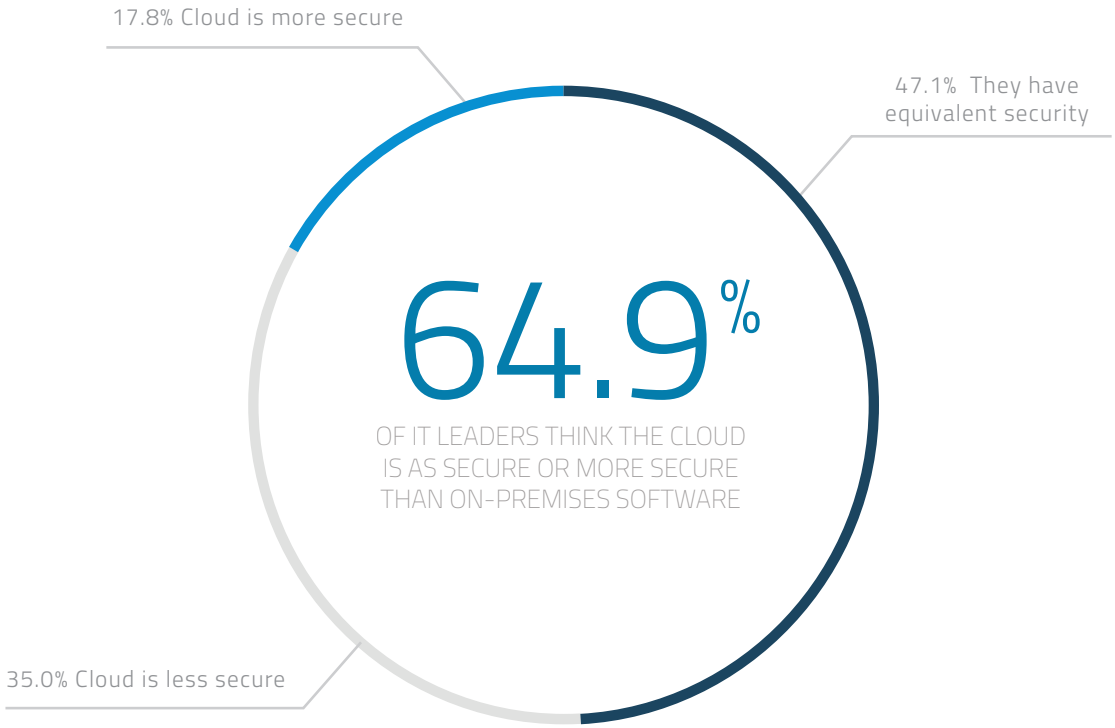
There are several primary benefits driving this next wave of IT transformation. Across respondents who have moved their system of record to the cloud or plan to do so, the most common perceived benefit, referenced by 71.8% of respondents, is lower up-front or ongoing costs. Nearly as many respondents (69.2%) indicated that faster implementation was a benefit. About half of respondents (49.4%) indicated that a better user experience was a benefit of moving to new cloud-based options compared with their legacy solution.

Barriers to Cloud Adoption

PERCENTAGE OF RESPONDENTS EXPERIENCING
BARRIER TO MOVING SYSTEM OF RECORD TO THE CLOUD



When asked about the barriers to moving systems of record to the cloud, the primary obstacle noted by 67.8% of companies was the ability to enforce their corporate security policies. Next, 61.2% of companies said that concern about complying with regulatory requirements was a barrier. Budget-related constraints do not appear to be a major hesitation when it comes to replacing a legacy on-premises system of record with a cloud-based equivalent.



While not explicitly identified by respondents, another potential benefit of cloud-based systems of record is the ability to integrate these applications with an expanding ecosystem of third party apps. There are over 2,000 apps on Salesforce's AppExchange and the average company says that it connects 2.6 third-party applications to their Salesforce environment. However, this is still fewer than the number of apps companies connect to their systems of engagement. The average company connects 17.2 apps to their Google environment.

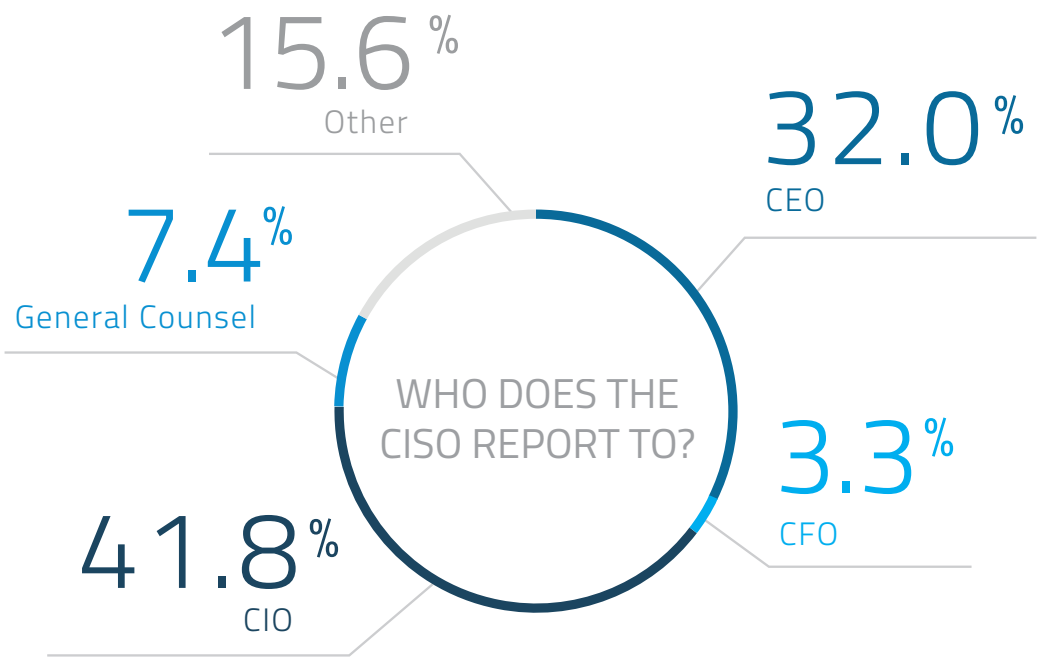
Despite concerns about the security of corporate data moving to the cloud, just 35.0% of IT and IT security professionals believe that, as a general rule, cloud-based systems of record are less secure than their on-premises counterparts. A majority, 64.9%, say that the cloud is either more secure than on-premises software or that they have equivalent security. One potential reason for this is that cloud providers like Salesforce and Workday have invested heavily in security, extending beyond even what some of their customers do to secure their on-premises applications.

Of companies have a Chief Information Security Officer (CISO)

A Culture of Compliance and the Role of the CISO

Considering the financial impact that a major data breach can have on a company, information security is an increasingly important function to reduce the risk and the potential impact of these incidents. Recognizing the importance of security, more companies are appointing a senior executive, the Chief Information Security Officer (CISO), to manage the information security team. Today, 60.8% of companies have a CISO. A CISO's role can vary, but it often includes setting security policies, overseeing regulatory compliance, and taking responsibility for data privacy.

Company size appears to have a significant effect on whether a company has a made an investment in hiring a CISO to head the information security team. Larger companies are significantly more likely to hire a CISO versus their smaller counterparts; 82.4% of companies with more than 5,000 employees have a CISO, while only 50.6% of companies with fewer than 5,000 employees have one.



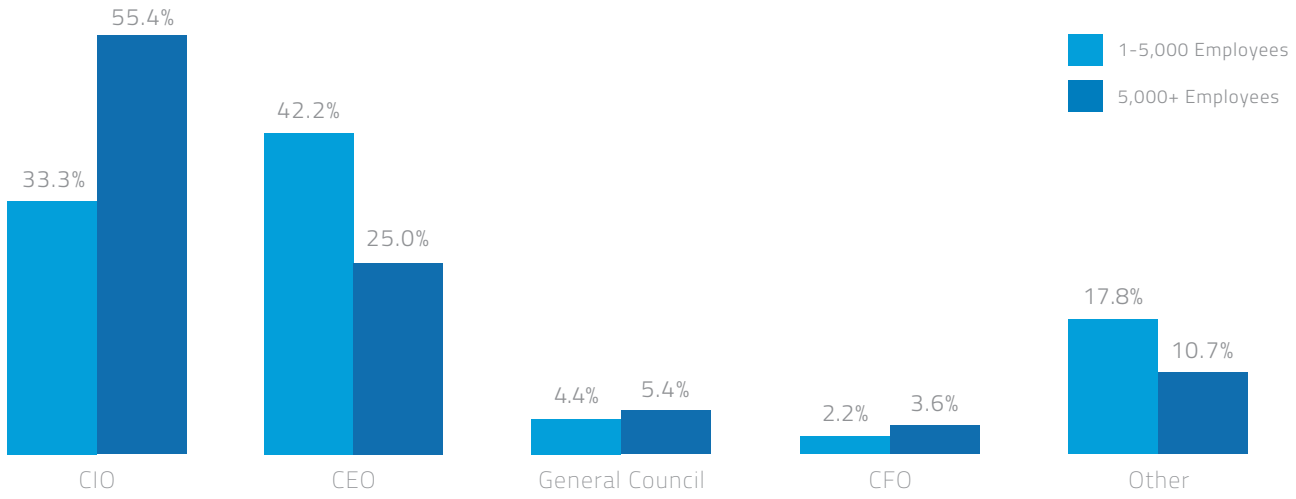
A key question when a company creates a CISO position is the best reporting structure. Some people argue that since information security is a core aspect of information technology, the CISO should report to the Chief Information Officer (CIO). Others argue that the CIO's mission to enable the business with new technology conflicts with the CISO's mission to protect the company's information. The security of a company's information has become so business-critical that it's a function that should report directly to the CEO, these people say.

We found that 41.8% of CISOs report to the CIO. Another 32.0% of them report directly to the CEO. Reporting structure is highly dependent on the company's size, however. At companies smaller than 5,000 employees, the CISO is most likely to report to the CEO. At companies with more than 5,000 employees, the CISO is most likely to report to the CIO. One possible explanation is that while the span of control for CEOs of large enterprises has doubled in the past several decades to 10 direct reports[1], and while CEOs increasingly manage functional specialists like the CIO, security is not yet perceived as something that CEOs should directly manage.

[1]National Bureau of Economic Research "The Flattening Firm: Evidence from Panel Data on the Changing Nature of Corporate Hierarchies"

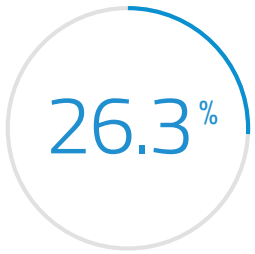
CISO Reporting Structure

PERCENTAGE OF COMPANIES WITH REPORTING STRUCTURE



As systems of record move from on-premises data centers under the direct control of the company to the cloud, 26.3% of companies are very concerned about data loss. Another 32.2% of companies are somewhat concerned about data loss. When you look at the companies that have a culture of security, or at least concern about security, these organizations are significantly more likely to have a CISO.

An impressive 65.7% of organizations that are concerned about data loss have a CISO, while only 50.0% of companies that aren't concerned about data loss have a CISO. It's not clear if a culture of security makes it more likely that a company will invest in hiring a CISO, or if a CISO instills a stronger culture of security, or if both reinforce the other.

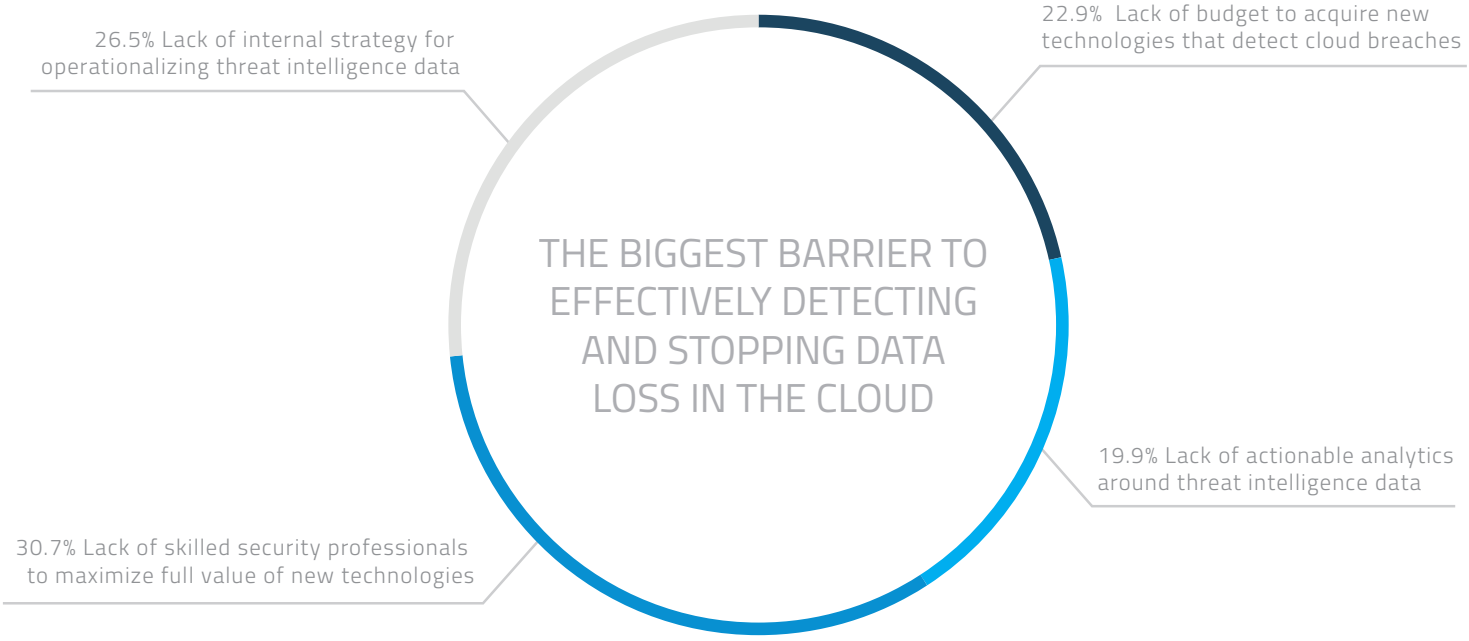


Of companies are very concerned about data loss as systems of record move to the cloud

Likelihood of Hiring a CISO

PERCENTAGE OF COMPANIES WITH A CISO

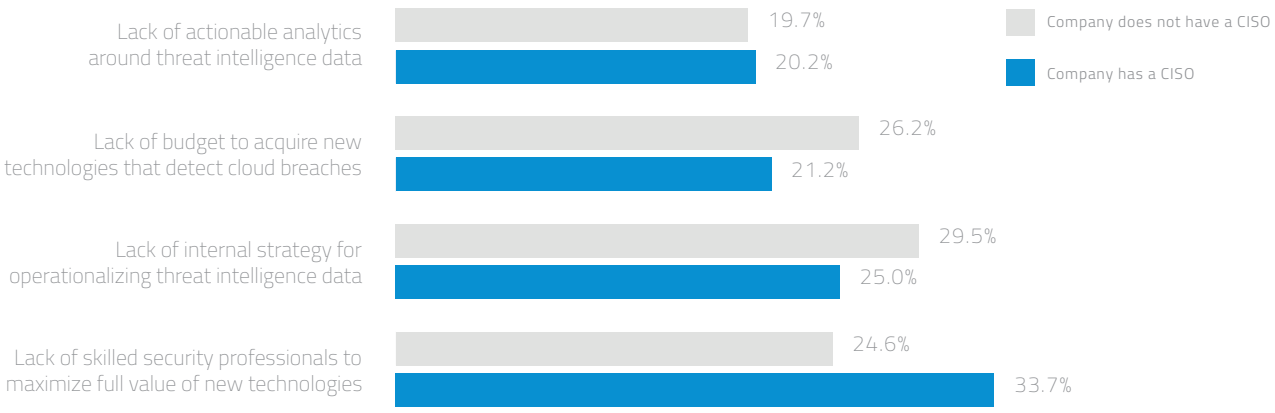
What is clear is that companies that have a CISO perceive their security challenges differently from those without a CISO to manage information security. Across the board, there's a skills shortage. Companies are finding it challenging to recruit and hire people to fill information security positions. The lack of security professionals to maximize the value of technology investments is the top barrier to detecting and stopping data loss, respondents say. However, the top challenge for companies without a CISO is the lack of an internal strategy to operationalize security.



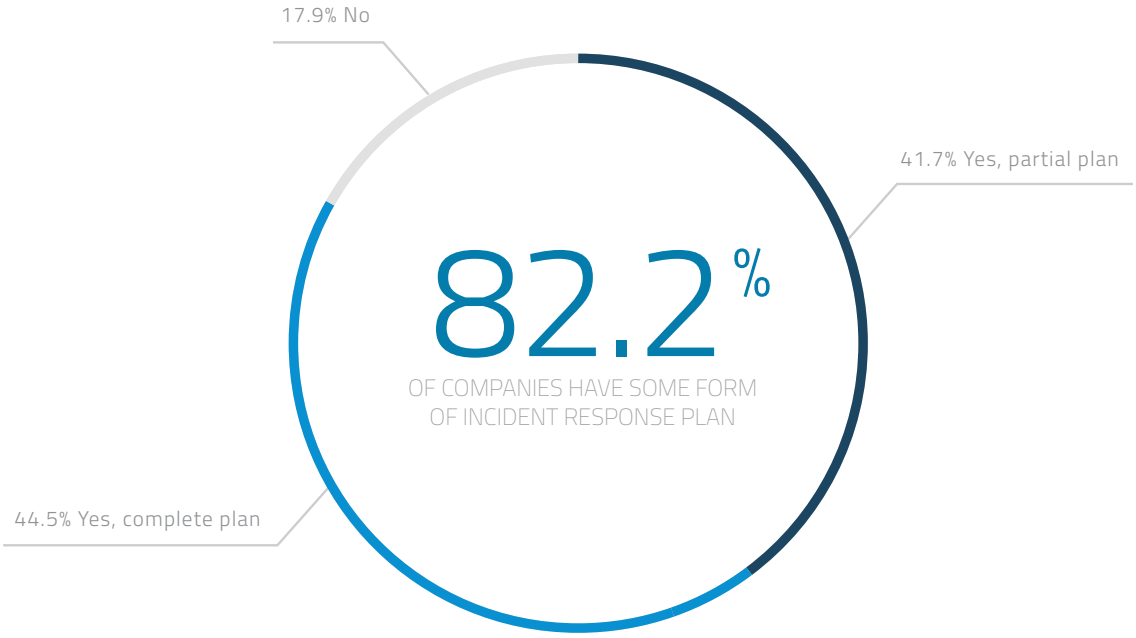
For companies with a CISO, the lack of technology professionals is an even greater perceived barrier to stopping data loss. This means that one of the biggest challenges of CISOs today is recruiting and retaining people to analyze data coming from a wide variety of security software tools available and use that information effectively to detect threats and stop incidents. It also means that the role of security analyst is quickly becoming a hot career path as companies invest heavily in expanding information security initiatives, with more jobs available than qualified applicants to fill them.

Security Challenges

PERCENTAGE OF COMPANIES FACING CHALLENGE



One of the reasons that companies with a CISO may be more confident about their internal strategy is that they are more likely to have an incident response plan. Across all companies, 82.2% have some form of an incident response plan that details how the company would respond to a serious breach, including security remediation, legal, public relations, and customer support. However, fewer than half of these companies have a complete plan that covers all of these areas.



Just 19.0% of companies without a CISO have a complete incident response plan. However, 53.8% of companies with a CISO have a complete incident response plan. Companies with a CISO are also more likely to have cyber insurance to protect against the cost of a data breach. Across all companies, 24.6% have cyber insurance. However, just 17.2% of companies without a CISO have insurance compared with 29.2% of companies with a CISO.

Cyber Security Insurance

PERCENTAGE OF COMPANIES WITH INSURANCE COVERAGE

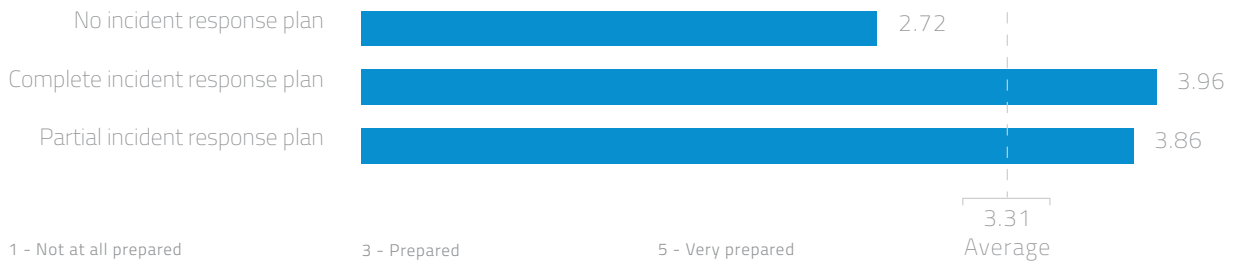
Securing corporate data starts with a culture of security and putting the proper organizational structure in place. Having a CISO is strongly correlated with other positive security steps companies take including developing a solid internal strategy, preparing an incident response plan, and acquiring cyber insurance to mitigate the financial impact of a breach. However, CISOs are challenged by a shortage of security professionals they need to implement their plans.

Emerging Threats and Compliance Requirements

Cyber attacks are increasing in frequency and their impact can be immense. While it's well known that attackers attempt to steal valuable data that can be resold, such as credit card numbers and Social Security numbers, there's a growing trend of cyber attacks whose purpose is to extract a ransom from a company, or inflict financial damage for political reasons. In the Sony cyber attack, hackers contacted the company and demanded a ransom before making over 100 terabytes of sensitive company data public and crippling its IT infrastructure.

Cyber Attack Preparedness

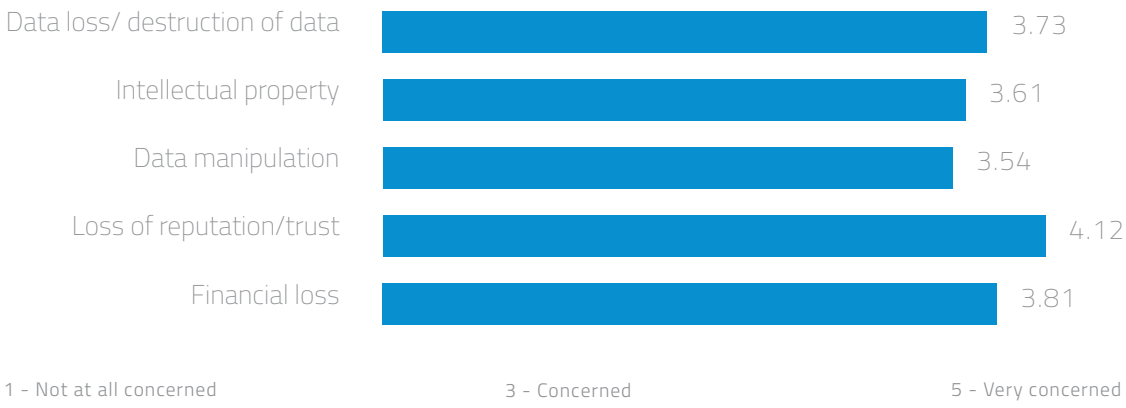
ON A SCALE OF 1-5 HOW PREPARED IS YOUR COMPANY FOR AN ATTACK



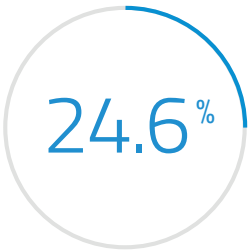
When asked how prepared their company is for a major cyber attack on a scale from 1-5, with 1 being not at all prepared and 5 being very prepared, respondents on average rated their preparedness at 3.31. However, responses varied widely depending on whether the company has a formal incident response plan. Companies with any form of incident response plan indicated they were significantly more prepared for a major cyber attack, compared with those without a plan. Companies with a comprehensive plan felt they were the most prepared.

Cyber Attack Concern

ON A SCALE OF 1-5 HOW CONCERNED IS YOUR COMPANY ABOUT THESE POTENTIAL IMPACTS OF AN ATTACK



The greatest concern companies have when it comes to a cyber attack is loss of reputation and trust. That's followed by financial loss, which in the case of Sony is estimated to be roughly $35 million to handle the immediate aftermath of the breach. External analysts estimate it could cost the company another $83 million to completely rebuild its damaged IT infrastructure. Next, companies are concerned about data loss and the destruction of data, followed by loss of intellectual property and manipulation of their data.



Of companies would pay a ransom to stop a cyber attack

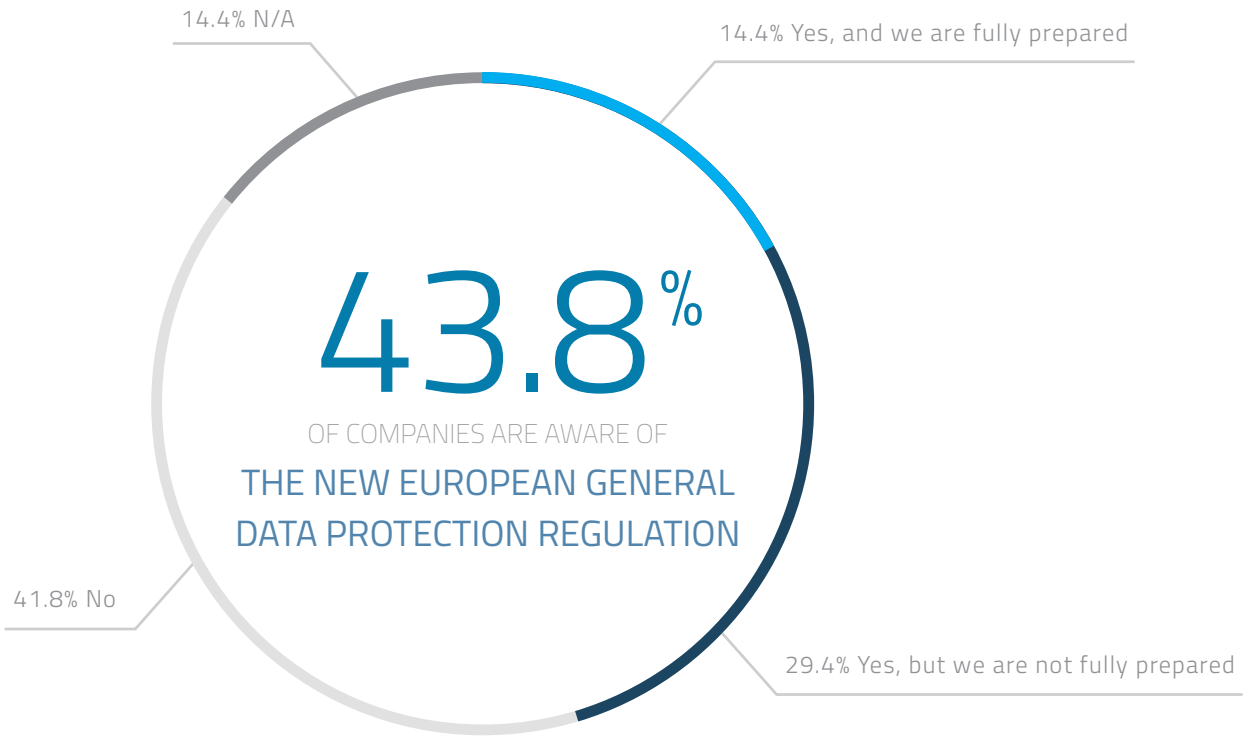
It's not clear whether Sony could have stopped the release of company data if it had responded to hacker demands in the days leading up to data dump (or if, indeed, the company attempted to answer the demands of the attackers). Nevertheless, if faced with a situation in which hackers have stolen information in a major breach and plan to make the information public, 24.6% of companies would be willing to pay a ransom to prevent the release of sensitive information. Across all companies, 14.0% would be willing to pay a ransom in excess of $1 million to prevent the release of such information.

Following a breach, many companies rely on cybersecurity insurance to cover part of the cost of the incident. Following the Target credit card breach in 2013, the company's insurance covered $90 million of the $264 million cost related to the attack. Many cyber insurance plans now offer the option of cyber ransom coverage, which pays for the costs associated with making ransom payments to cyber attackers.

The willingness of a company to pay a ransom to stop a catastrophic release of stolen information is correlated with whether the company has cyber insurance. Companies without cyber insurance are less likely than average to pay a ransom. Just 22.6% of these companies would pay a ransom. Across companies with cyber insurance, 28.6% would pay a ransom, higher than average.

Willingness to Pay Ransom

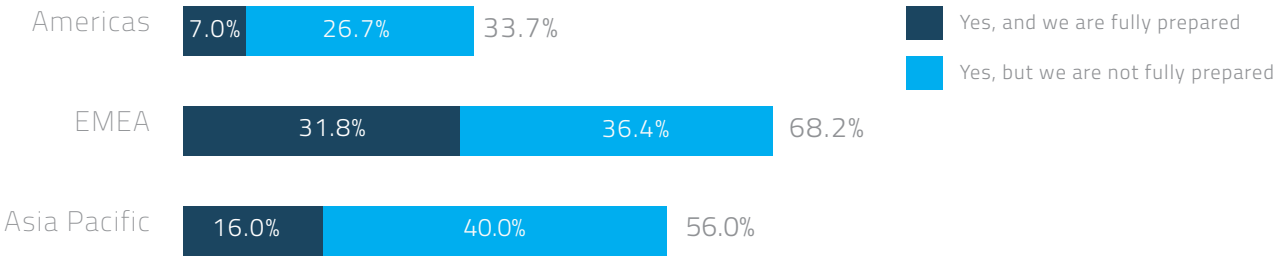
PERCENTAGE OF COMPANIES WILLING TO PAY A RANSOM TO STOP A DATA BREACH



Cyber attacks are not the only concern companies have when it comes to moving their systems of record to the cloud. As noted earlier, 61.2% of companies see compliance with regulations as a major barrier to cloud adoption. One of the most significant new regulatory schemes is the upcoming EU General Data Protection Regulation, which will introduce extensive requirements for any organization doing business in Europe or storing data about European Union residents. Despite the strict fines that companies may incur for violations of the new law, including up to €100 million or 5 percent of global revenue (whichever is higher), only 14.4% of companies are fully prepared to meet its requirements.

Awareness of EU General Data Protection Regulation

PERCENTAGE OF COMPANIES AWARE OF THE NEW LAW

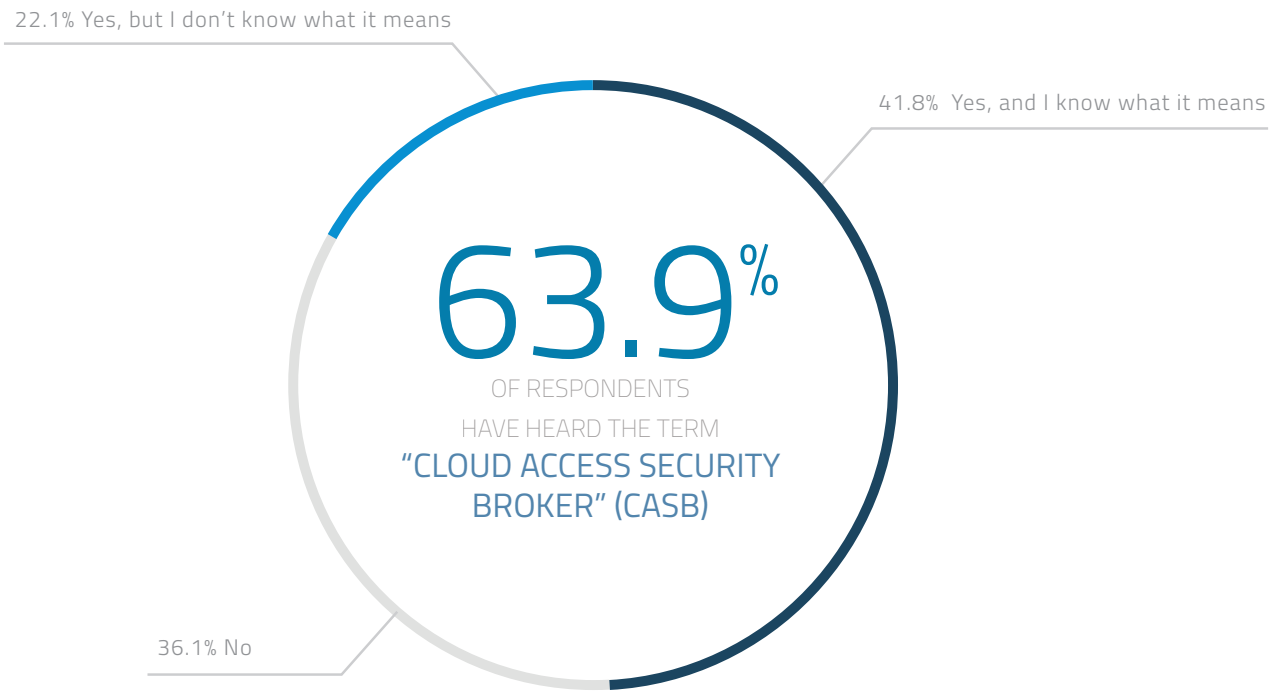


Awareness of the law and preparedness is highest in the EMEA region, where 68.2% of respondents are aware of the law and 31.8% are fully prepared. Companies headquartered in the Americas trail their European and Asia Pacific counterparts. Only 33.7% of companies based in the Americas are aware of the new law, and only 7.0% are prepared to meet its requirements. While not all of these companies will need to meet requirements under the law, given the global nature of business it's likely that many of them have requirements they are not aware of today.

Securing Data in the Cloud

As more corporate data moves to the cloud, companies are looking to enforce corporate security policies and meet regulatory compliance requirements. While individual cloud providers now offer controls recommended in the CSA Cloud Controls Matrix, the availability of these controls varies widely from provider to provider. That's why companies are also looking for a centralized solution.

Gartner refers to the emerging technology category that offers a centralized control point for cloud services as Cloud Access Security Brokers (CASB). Across industries, 63.9% of respondents have heard of this term, however only 41.8% of respondents have heard the term and are familiar with what it means. By 2020, Gartner estimates 85% of enterprises will use a CASB, up from less than 5% in 2015.

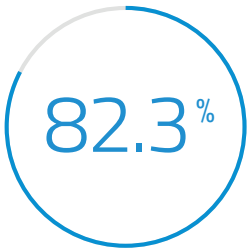


CASB solutions offer the ability to enforce different types of security policies. One of the capabilities that respondents say is important is access control. An overwhelming 87.3% of respondents indicated this is an important feature. Access control can include enforcing different levels of data access and cloud service functionality based on a user's role, device, location, and operating system.

Most respondents (83.4%) indicated encryption is important for cloud security. One use case involves encrypting data before uploading to a cloud service with encryption keys controlled by the company, making it indecipherable to third parties including the cloud provider storing the data. Next, 73.9% of respondents indicated data loss prevention is an important element of cloud security, which can include preventing certain types of sensitive data from being uploaded to the cloud, or shared from the cloud to a third party.

Cloud Security Capabilities

PERCENTAGE OF RESPONDENTS
WHO VIEW CAPABILITY AS IMPORTANT

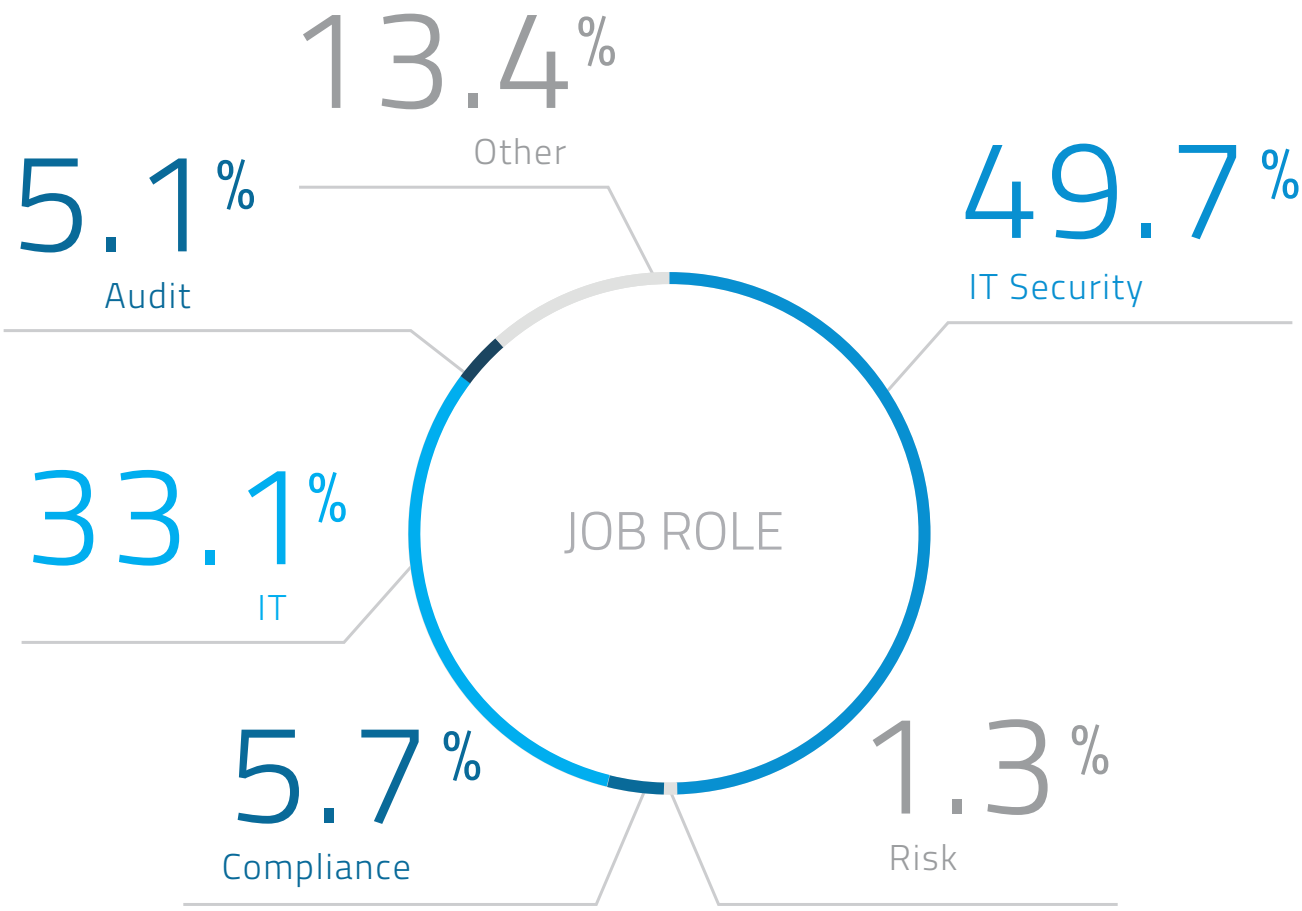


Of respondents think the "cloud access security broker" category is appropriately named

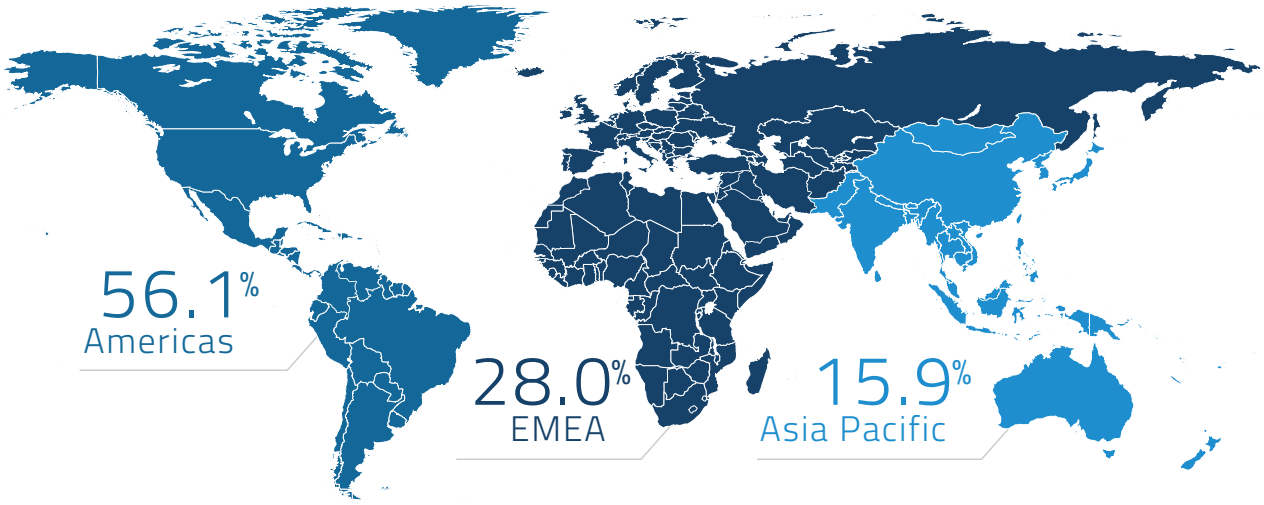
While other terms exist to describe the cloud access security broker category, IT and IT security professionals have embraced Gartner's definition. 82.3% of respondents who have heard the term believe that the category is appropriately named.

Survey Respondents

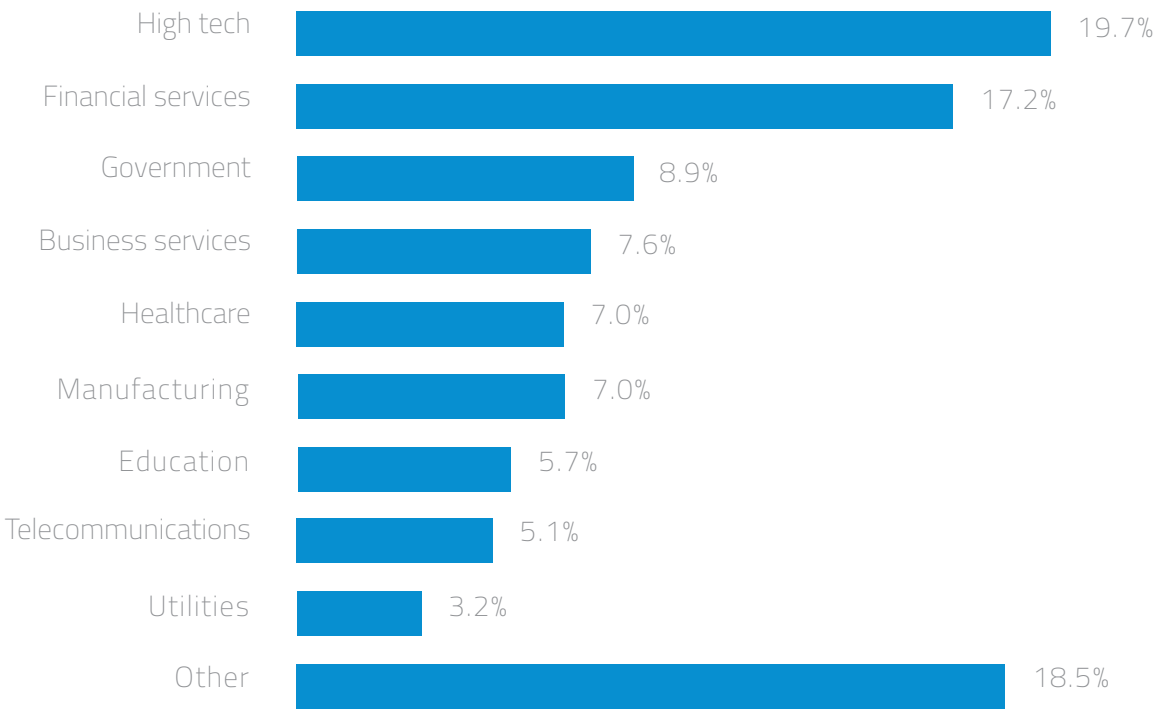
We surveyed 209 professionals at companies across industries worldwide. Here's a breakdown by company industry, job role, geography, and company size.

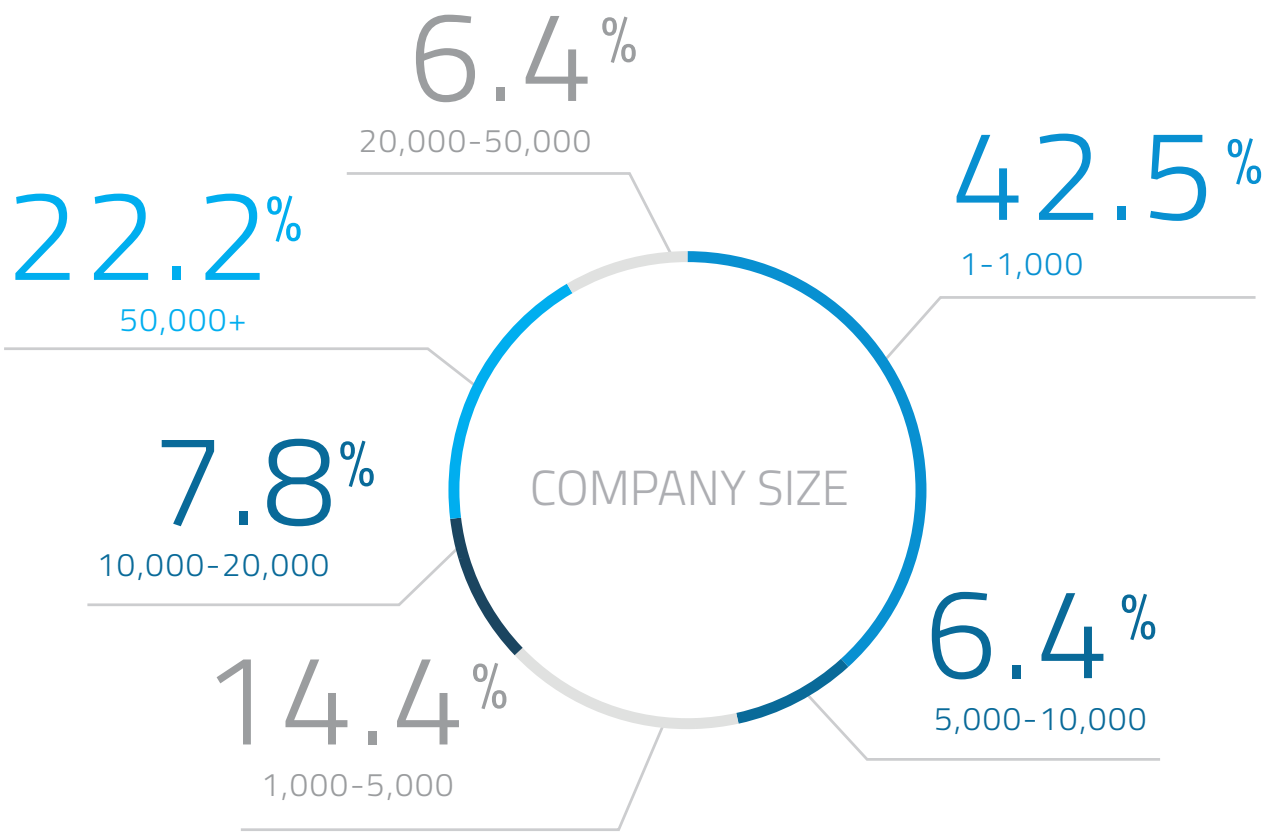


Region



Industry





Acknowledgements

MANAGING EDITORS

Cameron Coles

John Yeoh

CONTRIBUTORS/RESEARCHERS

Hillary Baron

Cameron Coles

John Yeoh

ABOUT THE CLOUD SECURITY ALLIANCE

The Cloud Security Alliance is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. For further information, visit us at http://www.cloudsecurityalliance.org/ and follow us on Twitter @cloudsa.

ABOUT SKYHIGH NETWORKS

Skyhigh Networks, the cloud security and enablement company, helps enterprises safely adopt cloud services while meeting their security, compliance, and governance requirements. Over 500 enterprises including Aetna, DIRECTV, HP, and Western Union use Skyhigh to gain visibility into all cloud services in use and their associated risk; analyze cloud usage to identify security breaches, compromised accounts, and insider threats; and seamlessly enforce security policies with encryption, data loss prevention, contextual access control, and activity monitoring. Headquartered in Campbell, Calif., Skyhigh Networks is backed by Greylock Partners, Sequoia, and Salesforce.com. Learn more at https://www.skyhighnetworks.com/.