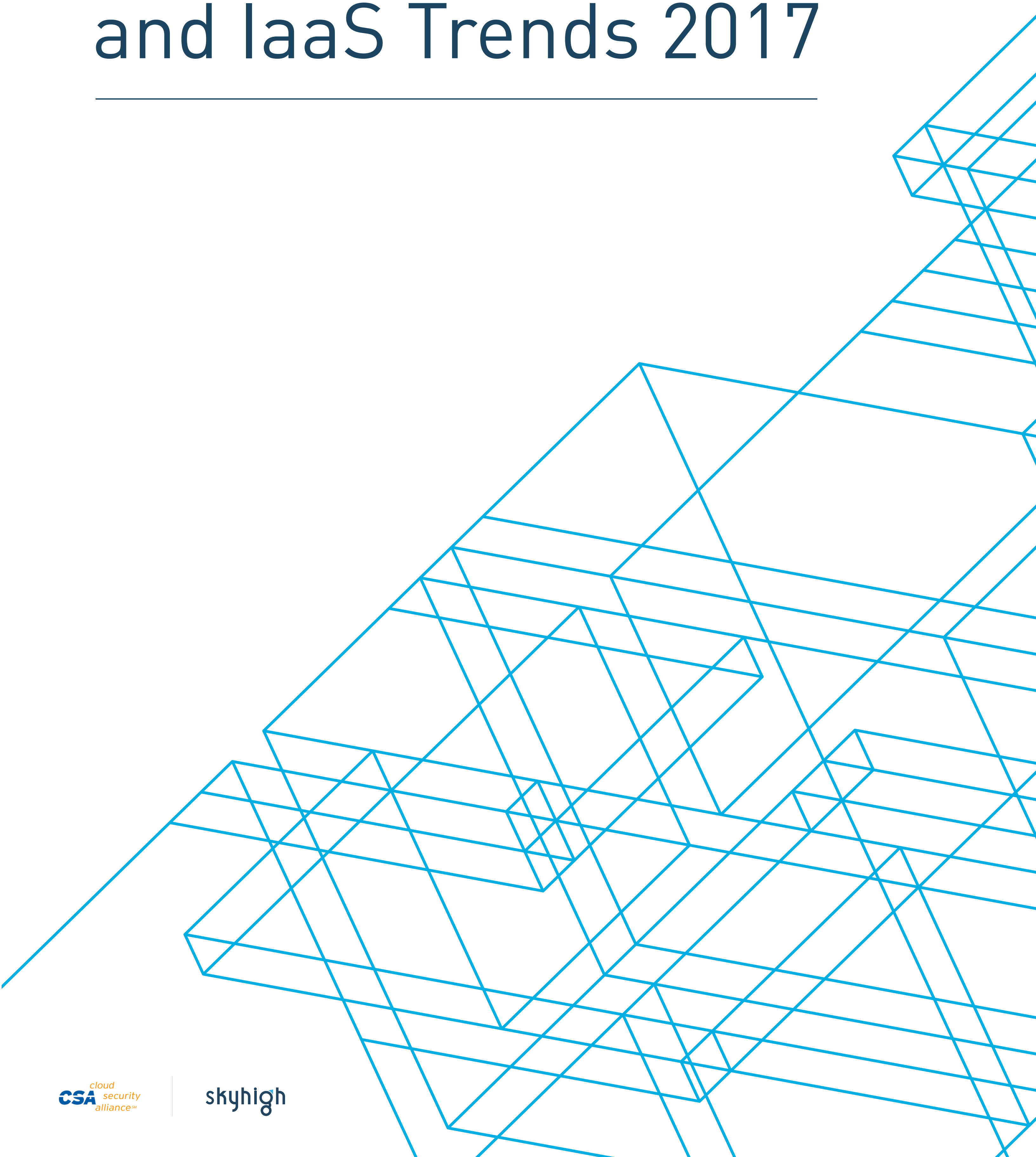
Custom Applications and IaaS Trends 2017



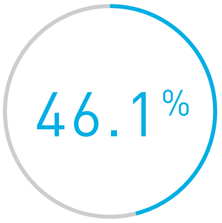
CSA cloud security alliance

skyhigh

Table of Contents

Introduction

Despite the wide range of commercial off-the-shelf applications, both on-premises and cloud-based, enterprises continue to develop their own custom applications. For example, an airline relies on an application it developed that plots the optimal flight path for each airplane crew before they take off. A rental car company uses an application it built to support its call center representatives to input details of reservations they accept over the phone. A retail store developed an application to allow its employees to request certain days and times for their upcoming shifts and allocate work schedules based on seniority and other factors.



Of business-critical apps
are in the public or hybrid cloud

The average enterprise today runs hundreds of these applications that are internally facing for employees and externally facing for customers, partners, suppliers, etc. Increasingly, these applications are running in public cloud environments such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform. While the public cloud offers numerous advantages including scale and cost, it also makes it easier for lines of business to build and deploy applications without involvement from IT security. There is now a sizeable number of "shadow" applications developed internally that IT security is not aware of or involved in securing.

This trend is problematic. Enterprises rely on custom applications to perform business-critical functions. Any downtime could halt operations. Our survey found that while enterprises have confidence in the security of IaaS providers' underlying infrastructure compared with their own datacenters, data in custom applications is exposed to a wide range of threats independent of the platform. That includes accounts compromised by third parties—via phishing or another method. There are a growing number of examples such as Code Spaces where attackers have held data ransom and in some cases permanently deleted enterprise data in these applications.

This report summarizes the scale of custom applications deployed today, where they are deployed, how they are secured, and who is responsible for securing them.

Key findings include:

IT security is only aware of 38.4% of custom applications

1. The average enterprise has 464 custom applications deployed and IT security professionals are only aware of 38.4% of these applications

2. The number of custom applications is expected to grow 20.5% in the next 12 months as more applications are developed and deployed

3. 20.7% of custom applications currently deployed in the datacenter will move to the public cloud in the next 12 months

4. Taken together, a majority of custom applications (60.9%) are in the datacenter today but this will decline to 46.2% in the next 12 months as public cloud adoption grows

5. 72.7% of companies have business-critical custom applications (i.e. downtime would impact operations) and 46.1% of those are in the public cloud or hybrid cloud today

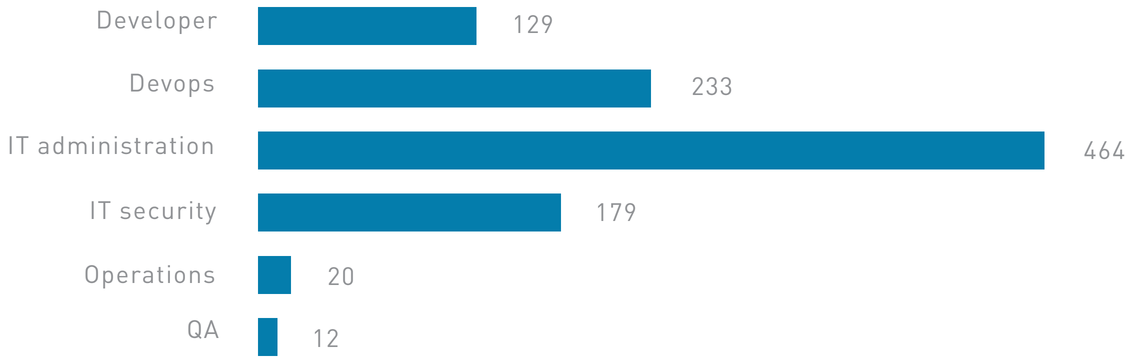
6. If business-critical data is destroyed in an attack on a custom app, 50.3% say the IT security manager will be fired, followed by 31.5% for operations, and 29.1% for the CIO

Every Company is a Software Company

The average enterprise has 464 custom applications deployed today. IT administrators have the highest awareness of the breadth of these applications, followed by devops professionals. IT security professionals are only aware of 38.4% of the applications known to IT administrators. This means that IT security teams are involved in fewer than half of these applications to ensure corporate data is protected against threats. Rather than security being a barrier to development, it appears development is occurring without involvement from security.

Awareness of Custom Applications

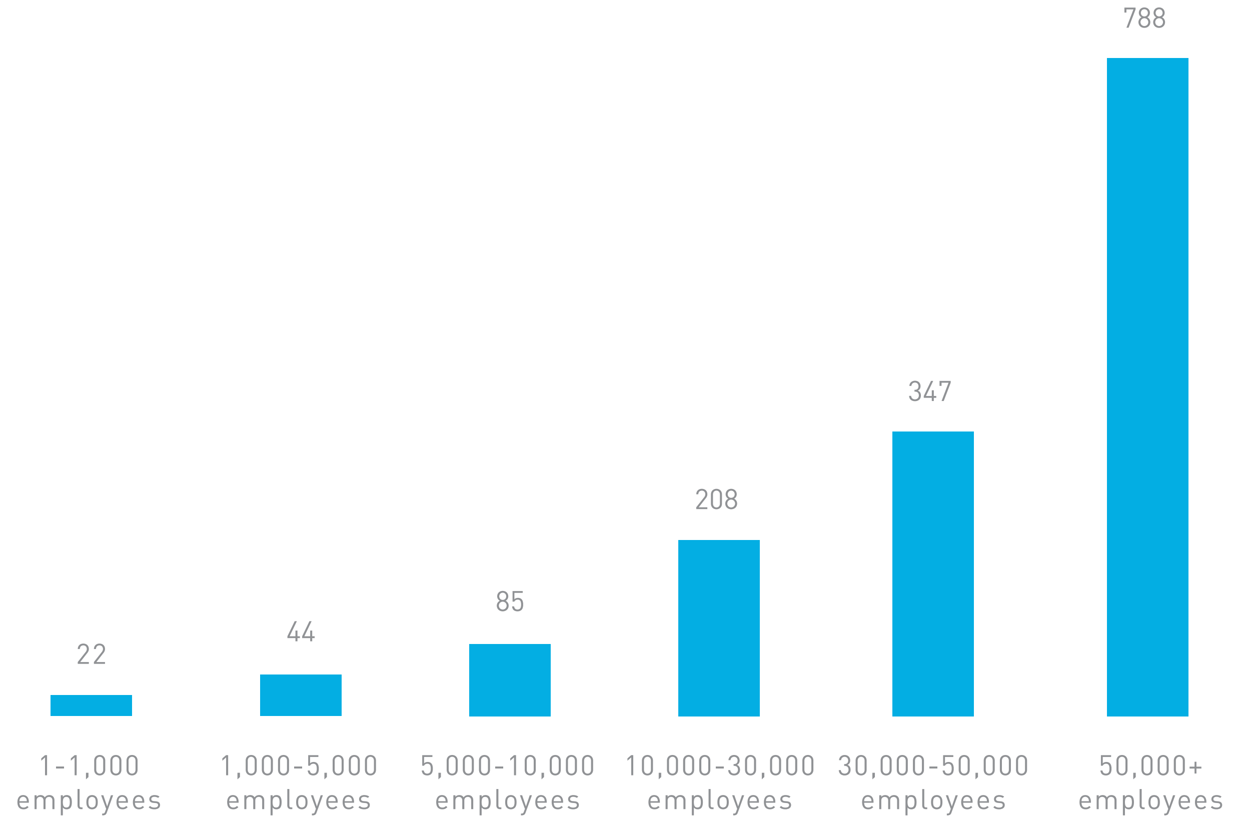
BY JOB ROLE



Respondents further estimated that, on average, they expect their organization to develop and deploy 37 new applications in the next 12 months. This rapid pace of development represents a 20.5% increase in the number of custom applications that are deployed at the average enterprise. Not surprisingly, application development is strongly correlated with company size. On average, companies with fewer than 1,000 employees run an average of 22 custom applications. The largest enterprises with more than 50,000 employees run 788, on average.

Number of Custom Applications

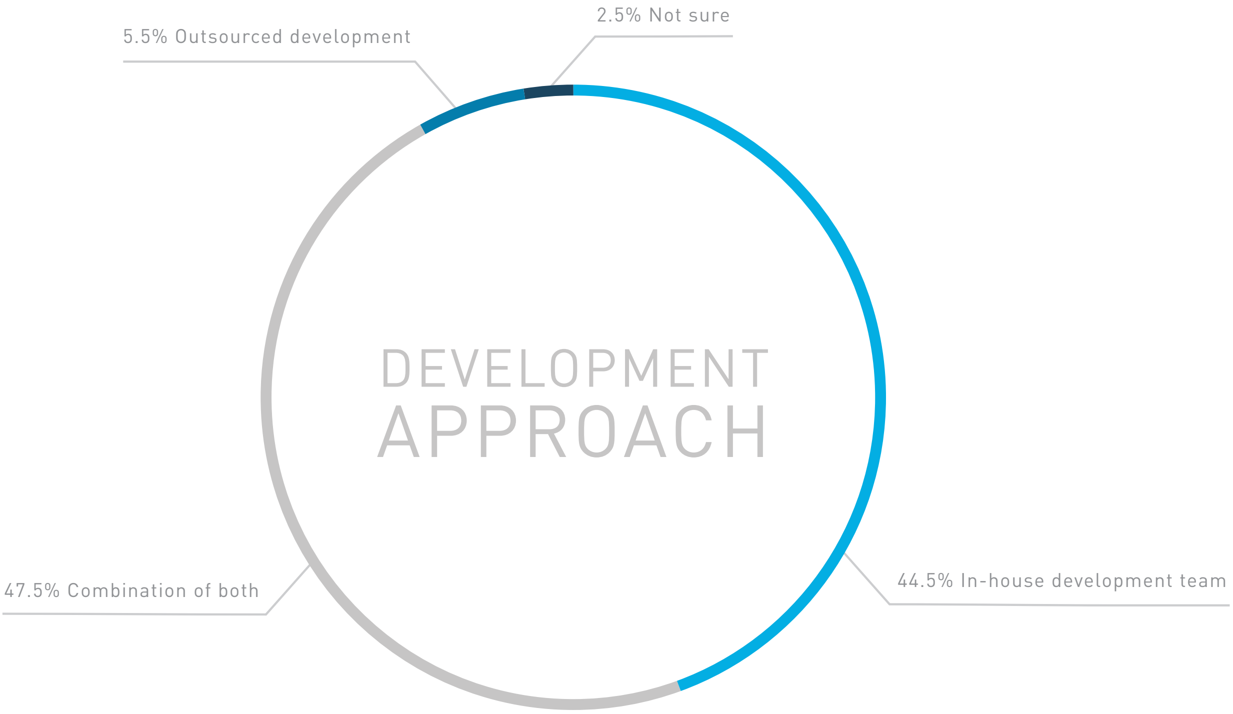
BY COMPANY SIZE



The overwhelming majority of enterprises (92.0%) have some software development resources in house, which they use for developing their own applications; 44.5% of enterprises rely entirely on internal development teams and another 47.5% rely on a mix of internal development teams and outsourced developers. A small number (5.5%) of enterprises rely entirely on outsourced development and have no in-house developers. Whether developers are internal or outsourced, some enterprises map developers to specific applications for the life of the application while others fluidly move a pool of developers between different apps.

Approach to Development Resources

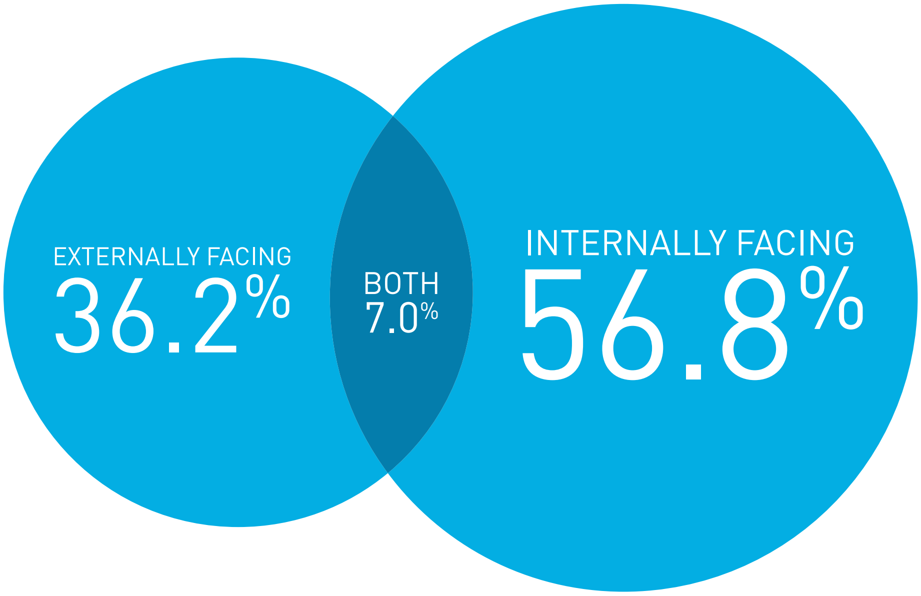
PERCENTAGE OF ENTERPRISES



A slight majority of applications (56.8%) are consumed by internal employees. Examples include a sales application that pulls data from multiple systems showing a salesperson the accounts in their territory that are set for renewal this quarter and a customer service application that allows call center employees to enter case details and retrieve suggested fixes. A little over one-third of applications (36.2%) are consumed by customers, partners, and suppliers. Examples include an Internet-enabled application that enables customers to schedule appointments with in-store technicians for support and an application that delivers training for partner sales teams.

Application End User

PERCENTAGE OF APPLICATIONS

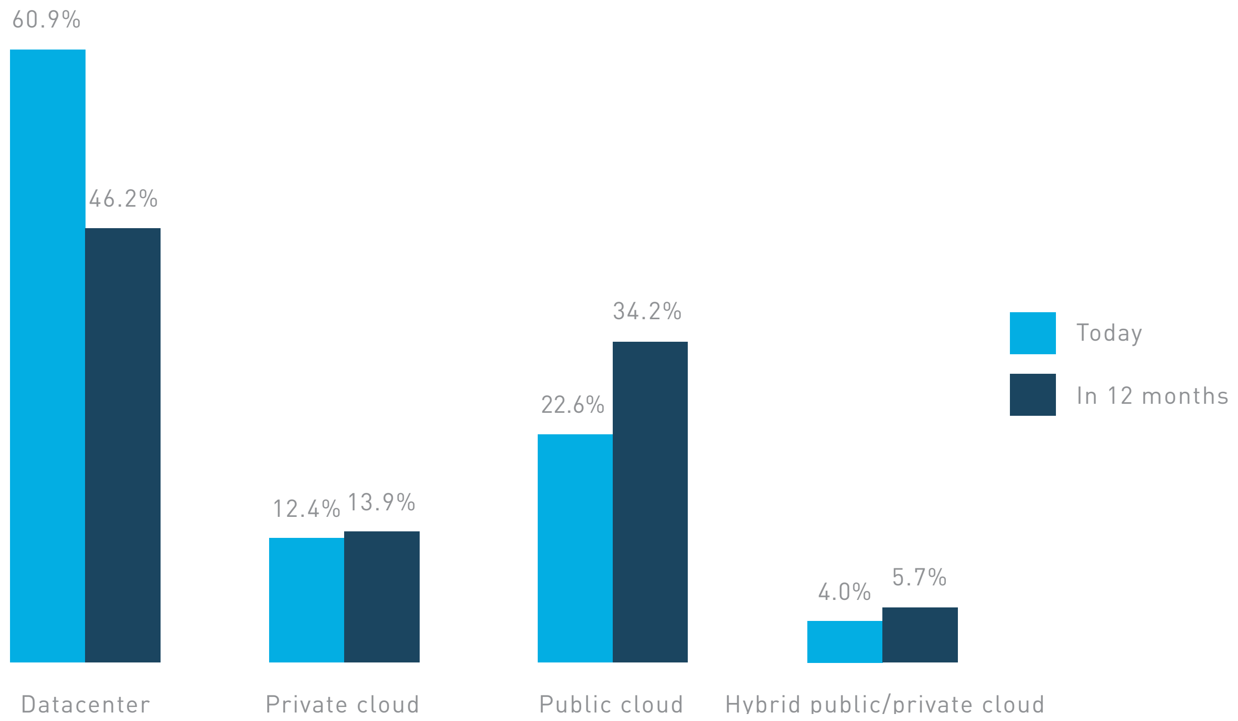


The Death of the Datacenter

Enterprises have talked of divesting from their datacenters and moving application workloads—both testing and production—to the public cloud for at least a decade. It turns out this process is unfolding in two ways: gradually and then suddenly. Today, a majority (60.9%) of applications workloads are still in enterprise datacenters. However, it's expected that in 2017 a tipping point will occur and fewer than half (46.2%) of workloads will remain in the next 12 months. This rapid shift is partially due to new applications that are deployed in the public cloud, and because enterprises expect to migrate 20.7% of their existing applications running in datacenters to the public cloud during this time.

Application Workloads

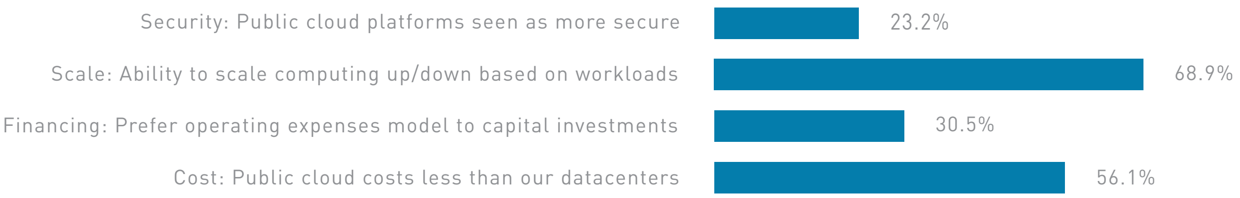
PERCENTAGE DEPLOYED BY INFRASTRUCTURE TYPE



By far, the primary driver for moving custom applications to public cloud infrastructure (68.9% of respondents) is the ability to scale workloads up and down on demand. The second most common driver is cost savings over maintaining a datacenter (56.1%). Public cloud offers companies a less expensive option when faced with large, costly datacenter upgrades. Rather than invest in new hardware, enterprises make the move to the cloud. Trailing at just 30.5% of respondents is the ability to shift from capital investments to an operating expenses model with a public cloud subscription. Finally, a small but significant 23.2% of enterprises move to the cloud to benefit from better security than their datacenter.

Drivers of Public Cloud Adoption

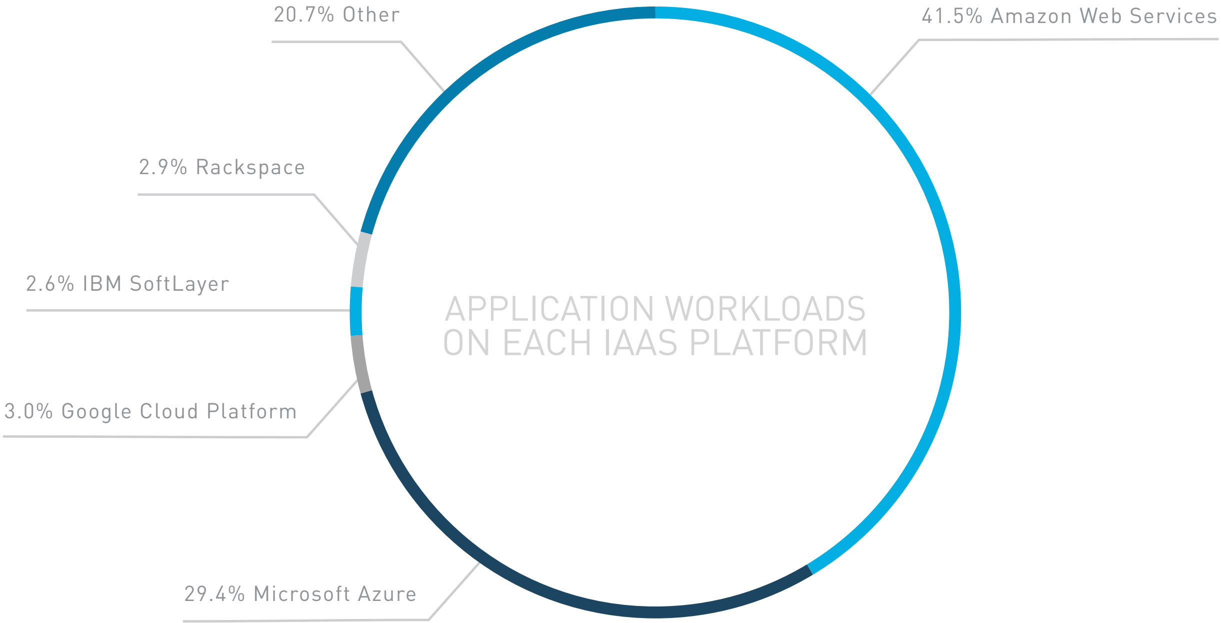
PERCENTAGE OF RESPONDENTS



According to survey respondents, Amazon Web Services is the most popular public cloud infrastructure platform, comprising 41.5% of application workloads in the public cloud. While Amazon has long been viewed as the dominant provider of public cloud infrastructure, Microsoft Azure is gaining ground quickly. Azure currently holds 29.4% of the installed base measure by application workloads. Google Cloud Platform trails with 3.0% of application workloads followed by IBM SoftLayer, Rackspace, and a long tail of providers that comprise another 20.7% of the market. The scope of long tail provider usage is surprising, and may indicate the market is still at an early stage of maturity.

IaaS Platform Adoption

PERCENT OF APPLICATIONS DEPLOYED

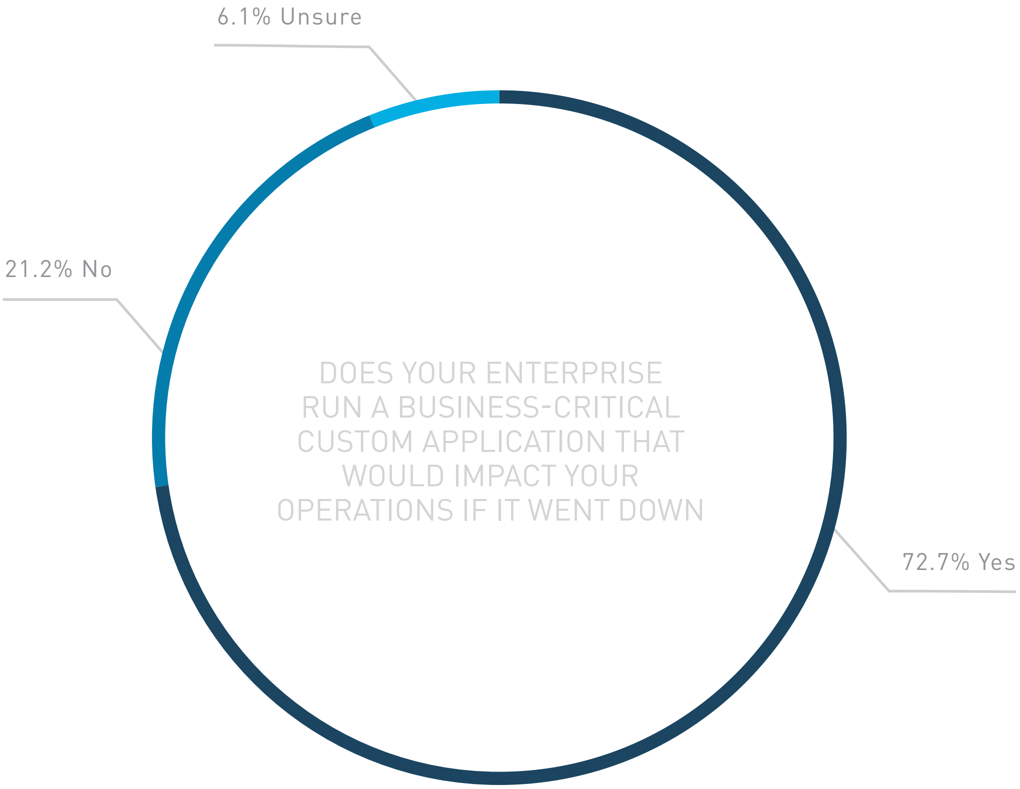


Business-Critical Custom Applications

A sizable majority of enterprises (72.7%) have business-critical custom applications—defined as an application that, if it experienced downtime, would significantly impact the organization's ability to operate. Consider some of the example applications discussed earlier in this report. An airline cannot operate if their flight path application goes down because planes are grounded. A rental car company cannot take reservations over the phone if their call center application goes down.

Business Critical Applications

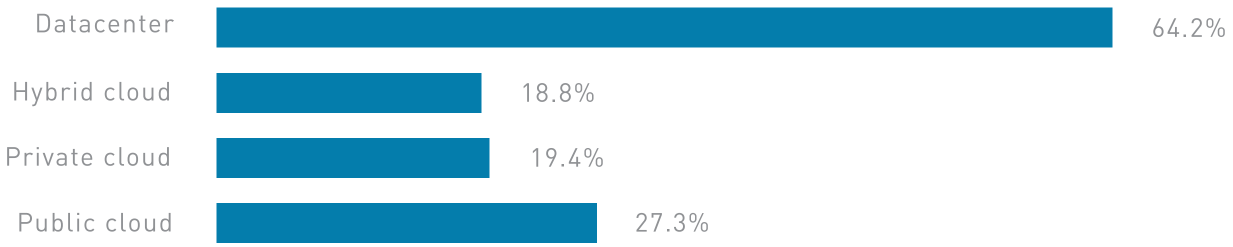
PERCENT OF ENTERPRISES WITH AT LEAST ONE



These applications are increasingly deployed in the public cloud; 46.1% are either fully deployed in the public cloud or in a hybrid public/private cloud and IT security professionals have incomplete visibility into their deployment and operations.

Business Critical Applications Deployed

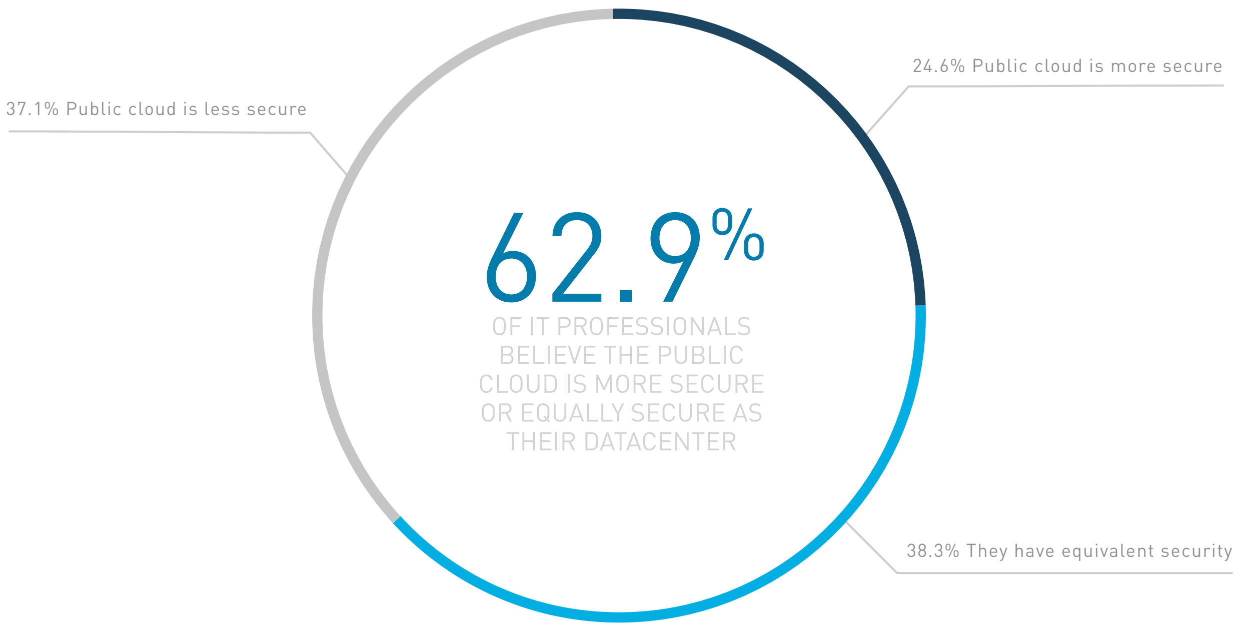
PERCENT OF ENTERPRISES WITH AT LEAST ONE APPLICATION FOR EACH DEPLOYMENT



Perhaps one reason why enterprises have rapidly moved these applications out of the datacenter to the public cloud is that, generally speaking, they view public cloud providers as being secure. A majority of respondents (62.9%) say the public cloud is as secure or more secure than their own datacenter.

Security of Public Cloud vs Datacenter

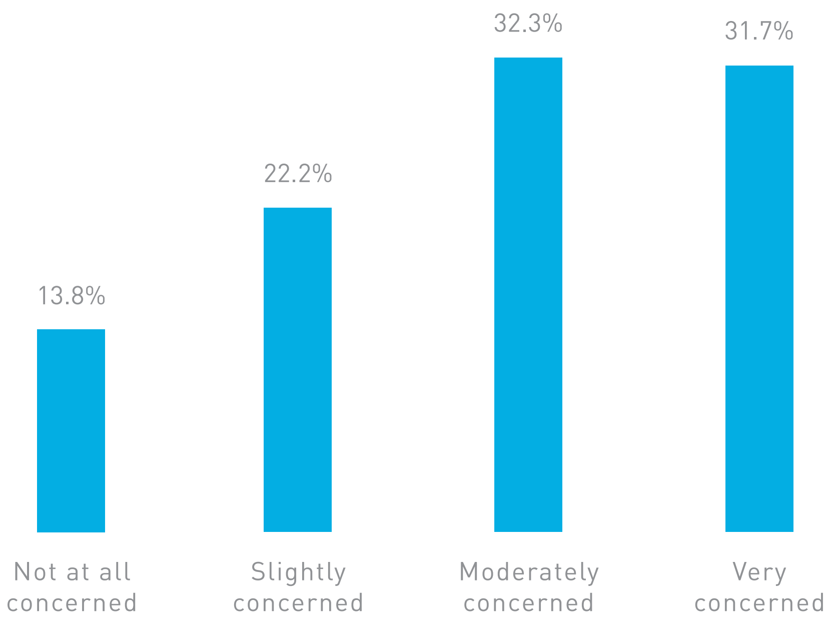
PERCENT OF RESPONDENTS



Despite confidence in the security of public cloud platforms, there remains a deep level of concern about the security of custom applications deployed in the public cloud. We found that 31.7% of respondents are "very concerned" about the security of these applications while another 32.3% are "moderately concerned". At first glance this may appear to be a contradiction. Enterprises rightly view the platforms provided by companies such as Amazon, Microsoft, and Google, with their extensive security resources, as being equally or better protected against intrusions than their own datacenters. However, the applications deployed in the public cloud are still exposed to a wide range of threats that can threaten a company's data.

Concern for Security of Custom Apps in the Public Cloud

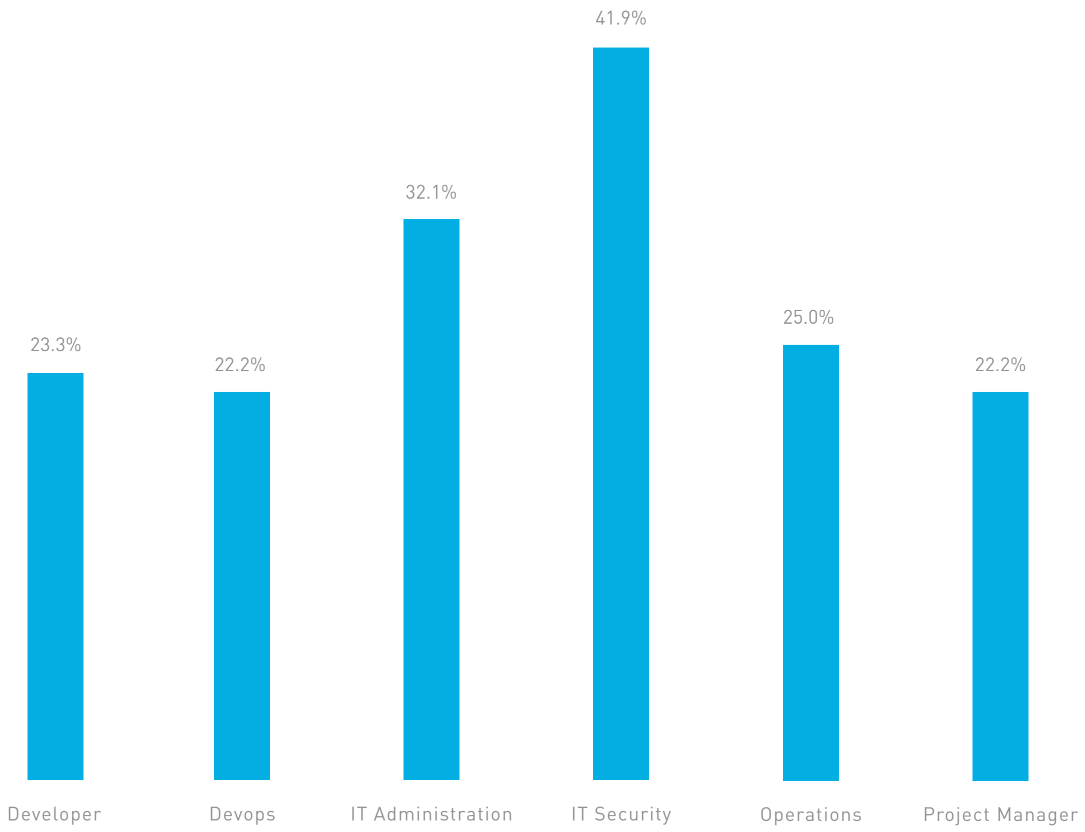
PERCENTAGE OF RESPONDENTS



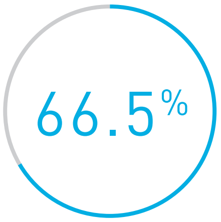
No group within enterprises today is more concerned about the security of custom applications in the public cloud than IT security professionals. A plurality of IT security professionals (41.9%) report feeling "very concerned" about the security of these applications. Rightly so, it is this group's job and responsibility to be the most knowledgeable about the threat landscape facing enterprises today. A somewhat smaller cohort of IT administrators (32.1%) report feeling "very concerned" about custom app security. Developers, devops, and operations professionals report lower levels of concern. Perhaps it is a lack of concern about security that is preventing developers, devops, and operations professionals who are responsible for the development and launch of applications in the public cloud from including their IT security counterparts in the process.

Concern for Custom Apps Security by Job Role

PERCENTAGE OF RESPONDENTS VERY CONCERNED



Threats to Applications Deployed in the Cloud



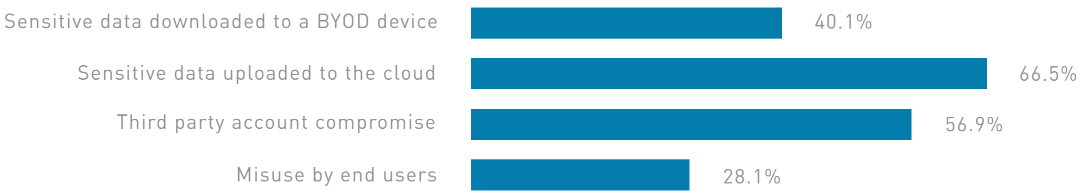
Of respondents said sensitive data in the cloud is a potential threat

In a cyber attack on the company Code Spaces, whose principal product was a code repository application on AWS, hackers gained access credentials for the company's AWS console and held their application and data hostage for a ransom. When Code Spaces did not comply, attackers permanently deleted its customers' data along with backups of that data maintained within the same AWS account. The attack was so devastating that it resulted in Code Spaces going out of business. It is an attack that did not compromise the integrity of the AWS platform, but rather an account password, which can easily be stolen via a phishing attack.

When asked about the greatest threats to applications running in the public cloud, the single most common response (66.5% of respondents) was sensitive data uploaded to the cloud. Some organizations have regulatory compliance and data residency requirements that can prevent them from uploading data to a cloud environment. That's followed closely by third-party account compromise (56.9% of respondents) like the one that shut down Code Spaces. Another concern is that applications in the public cloud make it easy to access sensitive data from BYOD devices with 40.1% of respondents concerned of users downloading this data to unmanaged personal devices lacking endpoint security controls.

Perceived Threats to Custom Apps in the Public Cloud

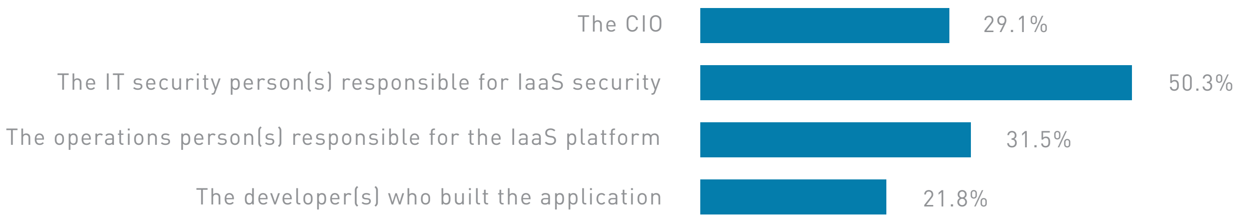
PERCENTAGE OF RESPONDENTS



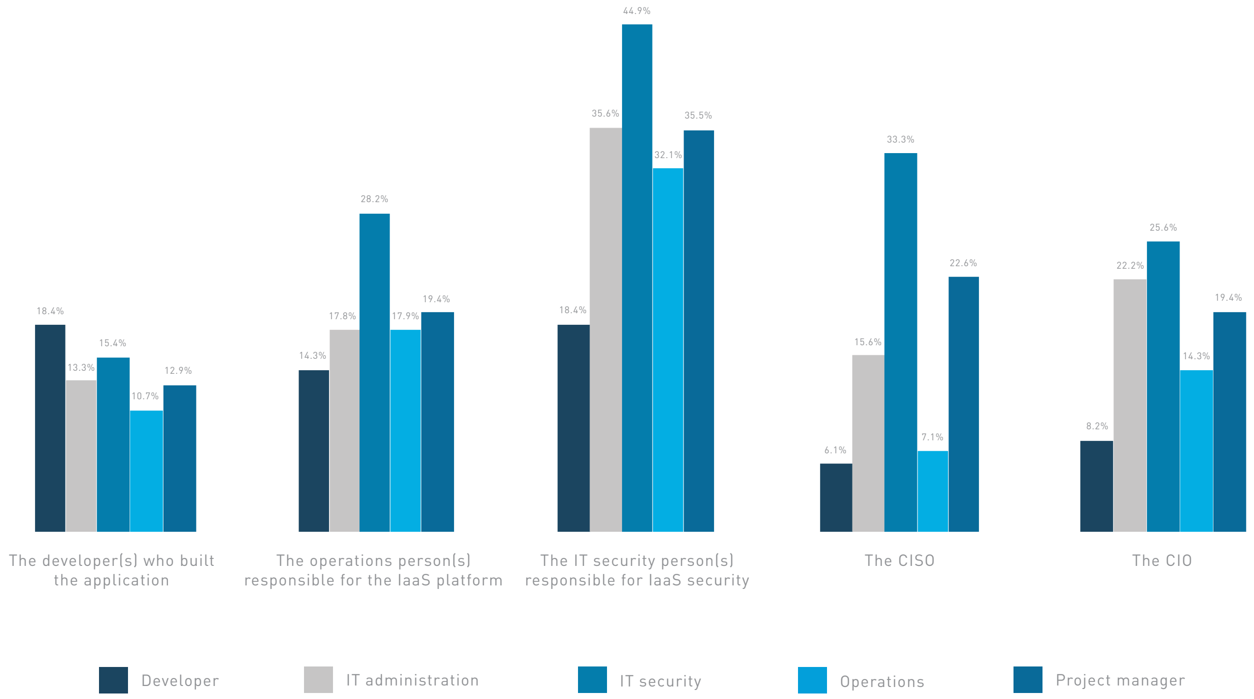
Even if a cyber attack on a custom application deployed in the public cloud does not result in permanent data loss, downtime of a few hours could result in significant costs. In August 2016, a six-hour computer outage for Delta Airlines delayed flights for hundreds of thousands of passengers and is estimated to cost the company tens of millions of dollars. These high stakes threaten the job security of anyone involved. In the event of such an attack, 50.3% of respondents said the IT security person(s) responsible for securing the public cloud would likely be fired. Another 31.5% of respondents said operations would get the ax, while 29.1% say the CIO would lose his or her job following such an attack.

Who is Fired After a Breach

PERCENTAGE OF RESPONDENTS



Rather than pointing fingers at other departments, developers and IT security professionals were the most likely to name themselves as those likely to be fired in the event of a breach versus colleagues in other functions. Perhaps this indicates that at some level, developers feel responsible for the security of custom applications and could therefore be motivated to work more closely to IT security colleagues to secure these applications.



Methodology

This study was conceived in collaboration within the CSA and Skyhigh Networks with the purpose of understanding public cloud workloads. The collaboration involved developing a pool of questions distributed to qualifying candidates between December 2016 and January 2017. CSA and Skyhigh Network analysts further studied, consolidated, and authored the report based on a survey of 314 qualified respondents. Qualified responses included software development, IT administration, IT security, operations, and devops professionals involved in developing, deploying, and securing custom applications employed by enterprises from all major industries including business services, education, entertainment/media, financial services, government, healthcare, manufacturing, retail, technology, telecommunications, transportation, and utilities. Respondents were based in the Americas, EMEA, and Asia Pacific. CSA had final editing rights of the survey questions and report before distribution to the public.