Cyber security and the cloud

Enterprise security leaders have their say

NOMINET
CYBER
SECURITY

NOMINET
NTX

Real-time threat prediction, detection and blocking

Contents

Enterprises take to the clouds

A short time after the turn of the century, large tech companies such as Google and Amazon started to refer to the delivery of software over the web as 'cloud computing'. Although the term was somewhat older, the mid to late noughties marks the point at which cloud computing entered common usage and the technology started being considered seriously as a delivery method for enterprise IT systems.

So successful was the technology that by 2015, 90% of global enterprises reported using the cloud as part of their business. Today, the global cloud market is worth more than $325bn and has arguably done more than most technologies to bring about the disruptive digital innovations that define the modern business world.

But this path to success was by no means assured. The cloud by its nature requires that enterprise IT teams relinquish some control of their systems and data to third parties, something that was thought unconscionable for heavily regulated industries such as financial services and healthcare. Exacerbating this adoption barrier was the belief that cloud computing was less secure than on-premise systems and that opening up to cloud services would seriously expose businesses.

Given cloud adoption rates today, to some extent these concerns have been overcome. But how? What has happened to reassure enterprise security teams? And what role do they see for cloud-first propositions in the security solutions of the future?

To help answer these and other key security questions relating to the uptake of cloud in enterprises and public sector organizations, we polled the views of nearly 300 Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), Chief Technology Officers (CTOs) and other security professionals in the UK and US. Our research reveals that:

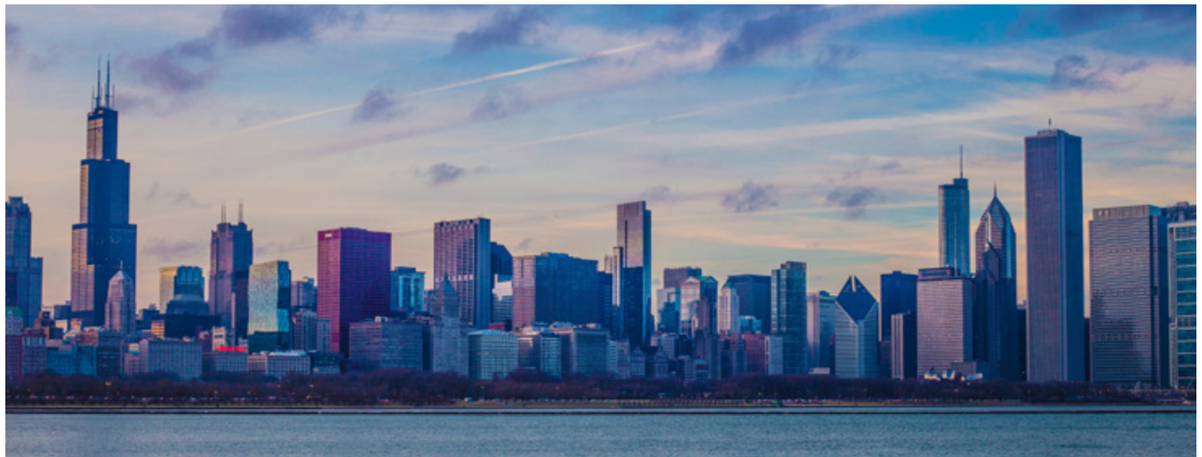
- Most businesses are committed to using the cloud more, and although important security concerns remain, the risk is now perceived as comparable to that of on-premise systems
- The cloud is not only seen as a security challenge: cloud-based tools are being embraced by security teams to bolster their enterprise defences
- Security professionals place a high value on security solutions that can seamlessly integrate with existing infrastructure, both cloud or on-premise

61%

of security professionals believe the risk of a security breach is the same or lower in cloud environments compared to on-premise

92%

of security professionals report that their business is adopting cloud-based security solutions



The great cloud opportunity

The clouds roll in

Cloud computing is fast becoming the frontrunner when it comes to the delivery of enterprise infrastructure, software and platforms.

The vast majority (88%) of respondents to our survey reported that their organization is currently engaged in, or is planning to, adopt cloud and Software-as-a-Service (SaaS) solutions. This strong appetite for cloud services runs across all the industries covered by our research, with only critical national infrastructure (CNI) organizations lagging in the field (64%), possibly due to elevated security concerns in this sector.

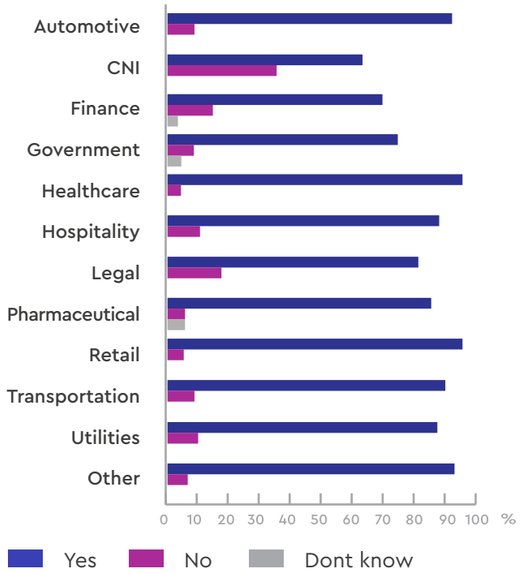
The metaphor most used for cloud adoption is that of a 'journey'. It is an apt one, with different businesses starting out at different points and adopting cloud services at different rates. This is reflected in the pace at which our respondents' organizations are adopting different elements of cloud computing.

While the majority reported that their business has adopted SaaS (71%) and Infrastructure-as-a-Service (IaaS – 60%) solutions, fewer have moved to later stage cloud services such as Platform-as-a-Service (PaaS – 48%), Business Process-as-a-Service (BPaaS – 30%) or Function-as-a-Service (FaaS – 25%). There is one exception here and that is the government sector. Here, the majority of respondents (56%) reported that their business has adopted BPaaS solutions – an even higher proportion than those that reported SaaS adoption (44%). This finding may speak to the high levels of outsourcing that have traditionally taken place in the government sector.

The findings represent a snapshot of a cloud transformation still in the process of unfolding. But the direction of travel is clear: we are well on the way to a world in which organizations are cloud-first.

When it comes to the service providers that firms are using to realize their cloud transformation, Google Cloud appears to be the market leader: 56% of respondents said that their company was using Google Cloud services, compared with other providers including IBM (49%), Oracle (44%), Microsoft's Azure (36%) and Amazon's AWS (32%).

Is your organization currently engaged in, or planning to adopt cloud / SaaS whether part of digital transformation activities, or otherwise?



With a fairly split market, it is no surprise that many firms are sourcing their cloud solutions from multiple providers. Indeed, nearly half (48%) of respondents stated that their organization had a multi cloud approach, while nearly a quarter (24%) have gone further and use a hybrid cloud solution (where various clouds are integrated into an overarching system). Just 29% of respondents said that their organization uses cloud services from just one provider.

When it comes to ensuring resilience and being able to source 'best-in-class' services, using multiple vendors makes sense. However, from a security perspective the approach also increases exposure to risk as there are a greater number of interfaces into the organization. In our survey, respondents using a multi cloud approach were much more likely to have suffered a data breach over the past 12 months: 52% vs. 24% of hybrid cloud users and 24% of single cloud users. They are also more likely to have suffered a large number of breaches: 69% of respondents from multi cloud businesses reported suffering between 11–30 breaches compared to 19% of those from single cloud business and 13% from hybrid cloud businesses.

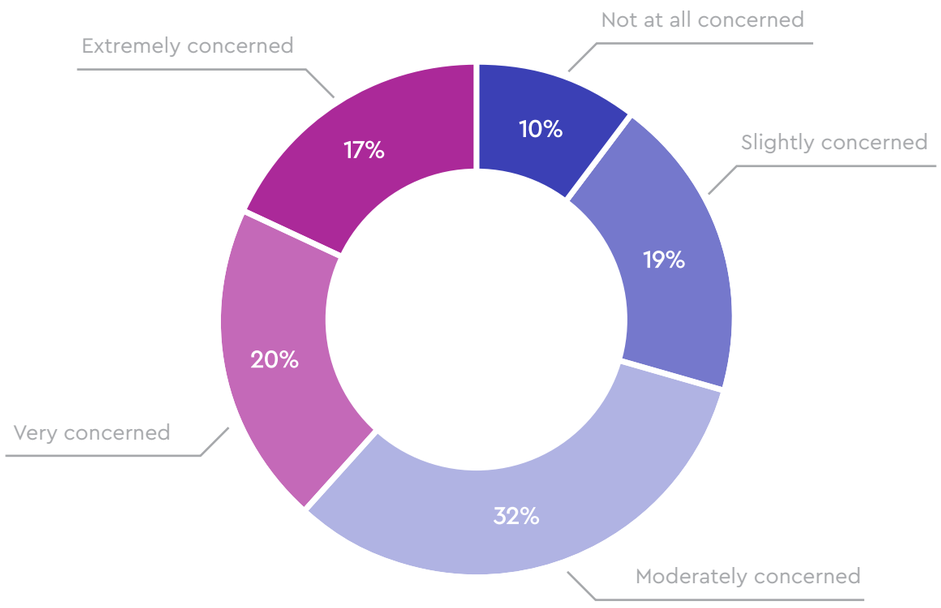
Cloud concerns

Given these figures, it's clear that cloud services, like their on-premise forebears, are targets for hackers and need to be secured. But just how concerned are security professionals about the risk of malicious activity in cloud systems?

It's clear that most respondents (71%) were either moderately, very or extremely concerned Interestingly, participants from the US were almost twice as likely than those from the UK to be extremely concerned (21% vs 13%). This could be for a number of reasons, including differing compliance regimes, threat landscapes and media coverage of security breaches.

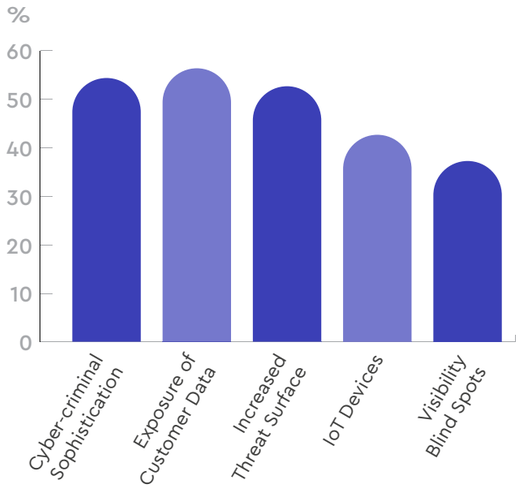
Certainly, looking at the overall findings by industry, there appears to be a trend whereby respondents from heavily regulated industries are more likely to be very or extremely concerned by the security risk posed by cloud; industries such as healthcare (55%), financial services (47%) and pharma (46%).

Please rate your level of security concern regarding cloud adoption



security of IoT devices was the number one concern for respondents from CNI companies (57%), an industry where such devices are used prolifically for monitoring purposes, and where any security breach could potentially be catastrophic.

What are your company's main concerns regarding cloud adoption?



Given the high adoption rates of cloud services, it seems these security concerns are not acting as an insurmountable barrier to cloud deployments. And nor should they. Being concerned about the security credentials of a technology is part of the job description for security professionals.

So, what is keeping our security professionals awake at night? Considering the increasingly punitive fines for the loss of customers' private data, it is little surprise that this ranked as the foremost concern; cited by 56% of respondents. This was only slightly ahead of one of the biggest security challenges of our times: the increasing sophistication of cyber criminals (54%) and, particularly relevant for multi cloud environments, the increased threat surface (52%).

IoT devices are also considered a key area for concern (53%); dispersed, connected sensors that extend the attack surface greatly. This is a critical issue to tackle as IoT devices are increasingly becoming central to new digital business models and customer experiences. If these services are to achieve all they can, securing IoT access points into the enterprise will be critical. Tellingly, the

One of the most interesting findings of this research is that the gap between the perceived risk of cloud services compared to on-premise services appears to be closing. This is important because security has often been cited as a key barrier to cloud adoption. When asked about the relative risk of security breaches in cloud environments compared to on-premise, one third (37%) said that they thought it to be higher. The good news is that 61% thought the risk to be the same, or lower. This speaks to a growth in confidence in the security of cloud services and an understanding of how the cloud can be secured.

However, this view of the risks of the cloud vary from industry to industry. Respondents from utilities (69%), healthcare (55%) and government (50%) were much more likely than the average to believe that cloud is a riskier proposition to on-premise. This in all likelihood reflects the fact that these sectors have experienced damaging, high profile breaches in the past and the nature of their fields means that they have a particularly low appetite for risk. It's little wonder that security professionals from these industries would be more cautious than most. The figures back this

theory up: respondents from companies that have suffered a breach in the past 12 months are more likely to believe that the cloud is a higher risk than on-premise than those that had not (52% vs. 25%).

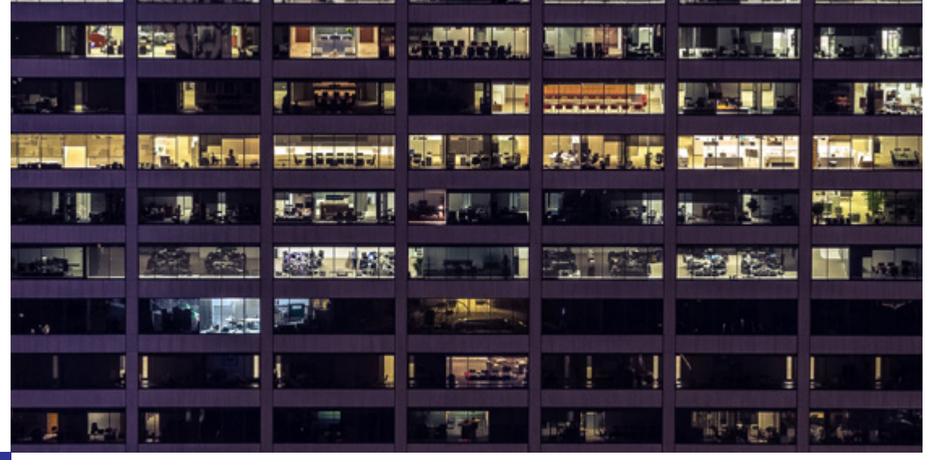
Overall, it appears that the perception of risk shrinks with exposure to cloud services. SaaS is the most mature of cloud services and the one with the greatest market penetration. It is therefore significant that fewer respondents thought SaaS to be a higher risk than on-premise alternatives (28%). Two thirds, meanwhile, believe the risk to be the same or lower. Seemingly, as cloud gains traction, the perception of risk falls.

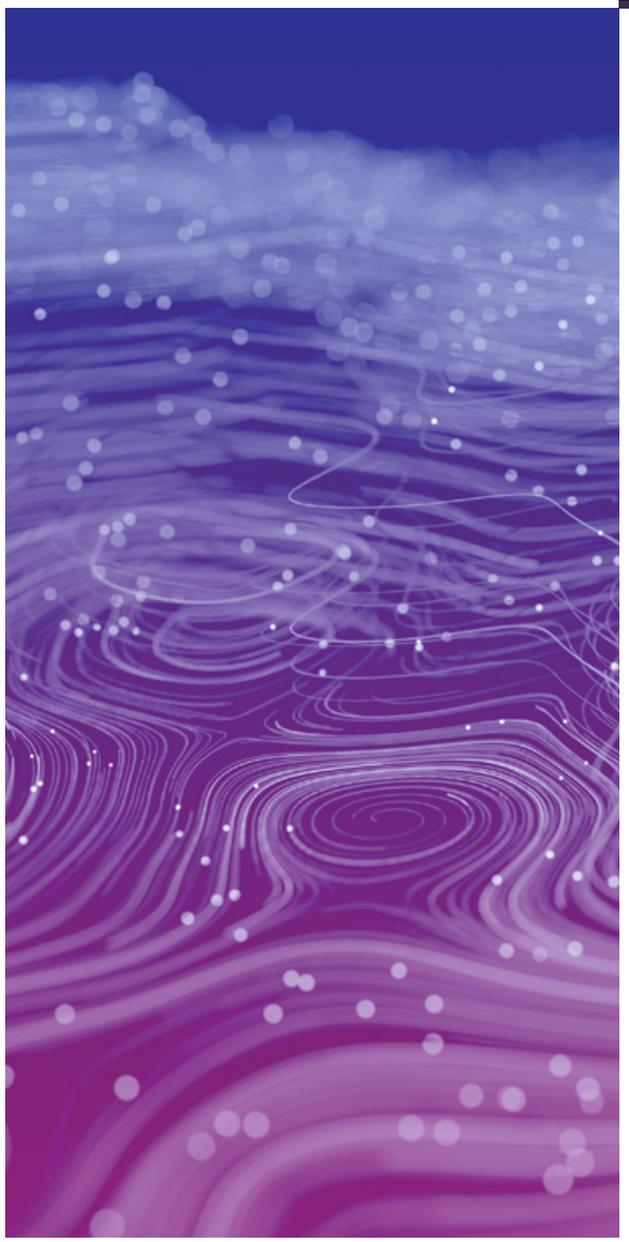
Securing through the cloud

The cloud is not only, or even primarily, a security challenge for businesses; it is also a security enabler. The cloud gives organizations access to outsourced security services and managed security services to enhance their overall security posture. Indeed, the ability of the cloud to rapidly deliver new services that integrate easily into organizations' existing systems is a key value driver.

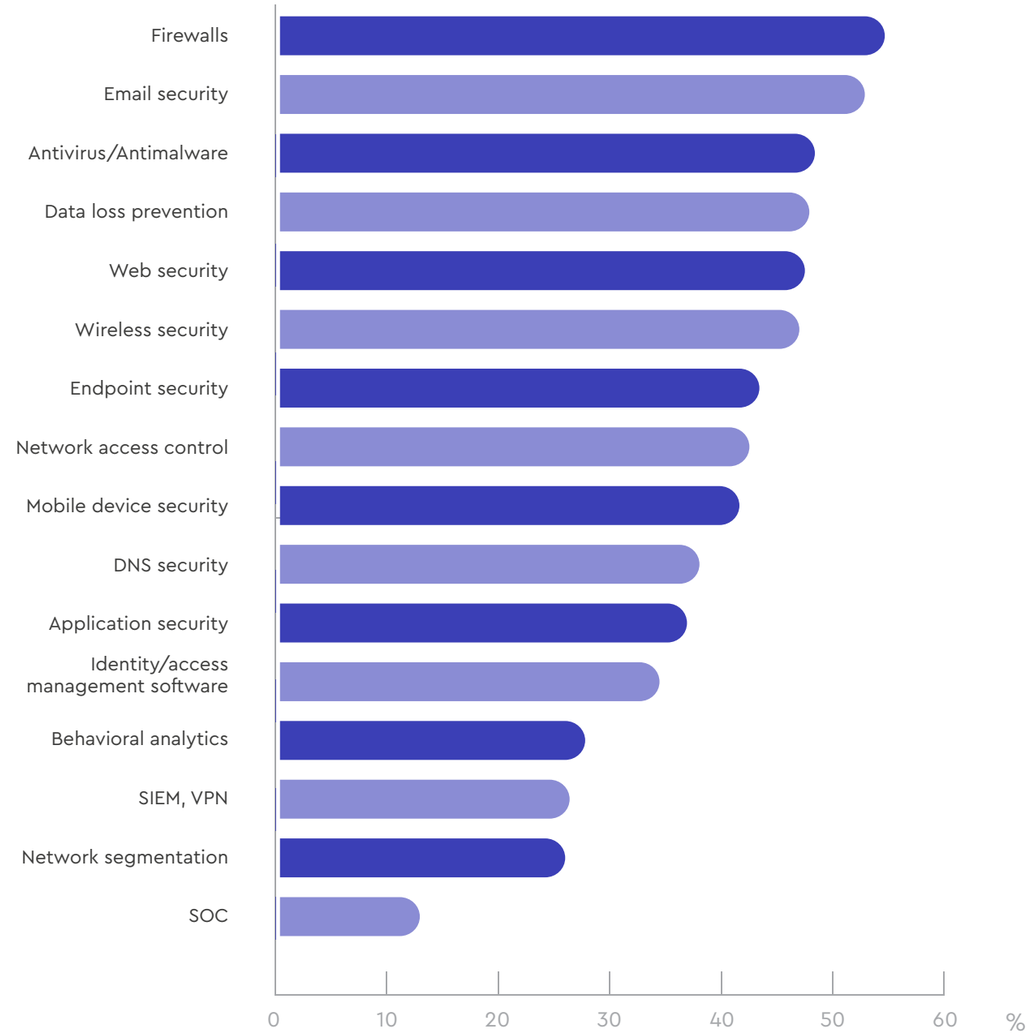
Our research suggests that the ability of the cloud to drive security benefits isn't lost on organizations; 92% of our respondents reported that their companies are engaged in, or planning to adopt, cloud-based security solutions.

These organizations are using a wide variety of cloud-based security tools to help protect their business, such as firewalls (55%), email security (52%), antivirus/antimalware (48%) and data loss prevention (48%). The cloud is therefore being used as the delivery mechanism of choice for a very broad array of security approaches, underlining the new trust businesses have in the technology.



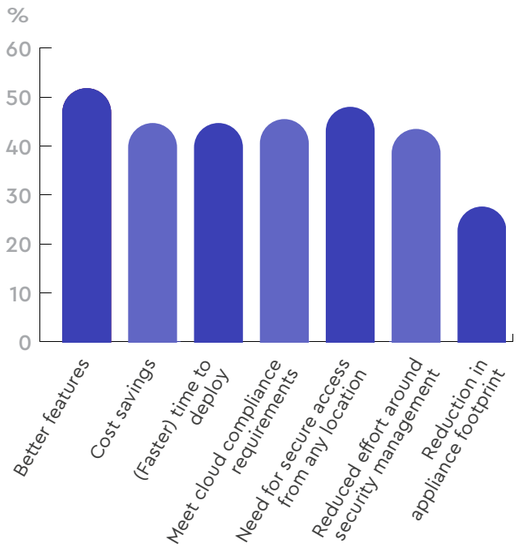


What forms of cloud security protection are in use at your organization?



Our research suggests that there is some variance in the tools used by organizations and the sectors within which they operate. For example, cloud-based DNS security enjoys very high take up in sectors such as legal (75%), retail (53%) and hospitality (50%). Meanwhile, Identity and Access Management gets more traction in finance (47%), critical national infrastructure (43%) and automotive (43%) than in other industries. This variance likely reflects a difference in the most common types of threat facing various sectors as well as security best practice for each industry.

What are the main drivers for considering cloud-based security solutions?



These considerations link to a central question: what is driving uptake of cloud-based security tools? According to our respondents, the inherent cost (45%) and agility (45%) benefits of the cloud are important, but so too are enhancements to the technology that have made it enterprise grade. Indeed, for the majority (52%), the improved features of the current generation of cloud-based security tools are driving adoption. This reason was closely followed by the need for secure access from any location (48%); a significant finding that once again shows shifting perceptions around the cloud: from security challenge to security enabler.

This isn't to say however, that there are no perceived drawbacks with cloud-based security tools. In fact, considering data privacy (49%), staff expertise and training (44%), the integrity of cloud security technologies (42%) and budget (42%), respondents cited a wide variety of potential barriers to deploying such tools in their organizations.

The good news is that all of these barriers are surmountable with the correct tools and the appropriate cloud partners. Where perhaps ten years ago these barriers would have been prohibitive to cloud adoption, today they are more like touchstones that firms are using to ensure their cloud investments deliver as required.

This careful consideration extends to the cloud service providers and vendors that organizations work with. As you would expect with any service providers, security professionals have a checklist of things they require from potential partners. When it comes to cloud-based security services, our research reveals the top considerations to be cost effectiveness (67%), seamless integration with existing systems, including on-premise (62%) and ease of deployment (58%). These all came out ahead of the availability of cloud-native tools (54%).

Respondents clearly want to consume cloud services, but they want them on their terms. For many, this means focusing on vendors that can provide cloud services that can be seamlessly integrated into their existing systems, no matter where they are in their cloud journeys.

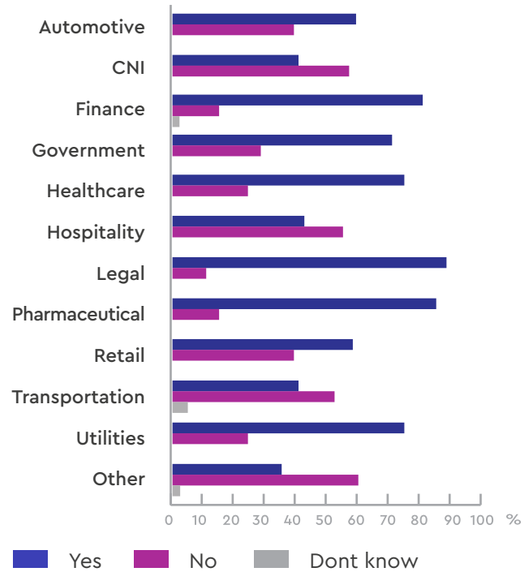
Cloud as a managed service

When the cloud first hit the mainstream, it was primarily used as a delivery mechanism for software. Enterprises accessed SaaS applications over the cloud instead of buying software licenses from vendors. As the cloud has matured however, so too has the development of managed services, where firms outsource wholesale the management of certain aspects of their enterprise, whether that's infrastructure, business processes or operations.

When it comes to cloud security operations, nearly two thirds of respondents (63%) said they already outsource to such managed service providers. When looking at the industry breakdowns, the outliers were CNI, hospitality and transport, where respondents were more likely to say they don't outsource some of their security operations (57%, 56% and 53%, respectively).

Outliers aside, most organizations are happy to outsource when it comes to security, and appear to believe the practice improves their security profile. Respondents that do outsource their security operations were much more likely to score the effectiveness of their security stack highly compared to those that don't (64% of 'outsourcers' scored themselves seven to ten out of ten compared to 35% of 'non-outsourcers'). What's more, these businesses are more likely to see cyber security as an increasing priority (65% vs. 34%).

Do you outsource any of your cloud security operations?



The cloud security budget boom

With the demand for cloud security tools and managed cloud security services on the rise, you would expect to see a corresponding increase in cloud budgets. And, in fact, this is exactly what our research shows. When asked how they see their cloud security budgets changing over the next 12 months, the majority (57%) of respondents reported that they expected it to increase. While 38% expect their budgets to remain the same, just 3% are predicting a drop off in budget.

Our respondents are positive about the future role of the cloud as part of the security mix. Confidence was apparent in all of the industries covered by our survey, with the exception of pharma and hospitality, where budgets are largely expected to decrease (62% and 56% respectively). There are a number of reasons why this could be, including tightening overall budgets in these industries, or something related to the maturity of their IT cloud security investments relative to other industries.

In organizations where cloud security budgets are increasing, respondents are more optimistic about the performance of their overall security stack. In fact, 58% of respondents from firms where cloud security budgets are increasing rated their security stack effectiveness between seven to ten on a scale of ten, compared to just 37% in businesses where budgets are remaining static and 3% where spend is decreasing. Indeed, where budgets are remaining static, respondents were most likely (50%) to score the effectiveness of their security stack a fairly average score of between four and six.

Of course, an increase in budget may not only reflect a security conscious leadership team. It could also be a response to a security breach. Our findings suggest that respondents are likely to believe their cloud security budgets are increasing if their business has been attacked in the past 12 months (62%).

It's possible that organizations that have suffered an attack in the past are turning to the cloud to better manage future risk. Certainly, cyber security is more likely to be seen as an increasing priority in organizations where respondents also expect to see their budgets increase (65% compared to 31% of respondents from organizations where budgets are remaining flat). For most (63%) respondents from the latter type of business, no change is expected in the prioritisation of cyber security within their firms.

It's comforting that where security is seen as becoming increasingly business critical, that cloud security offerings are too becoming an important focus and consideration.

The future is in the cloud

There is no doubt that the cloud will continue to play a foundational role in enterprise IT systems today and in the future. The cloud allows businesses to move fast and pivot to new market opportunities rapidly and at a low cost. It drives innovation by enabling rapid prototyping and DevOps processes, and enables businesses to manage vast volumes of data and draw game-changing insights from it. The cloud has helped make digital disruption a reality and will continue to do so for the foreseeable future.

But the cloud is not without its challenges. As our research has shown, security concerns persist, and it is likely they will always be there. There does seem to be a shift, however, as cloud adoption rises and its ability to deliver additional security is considered. In Nominet's opinion, the security risks of cloud are lower than with on-premise systems. With managed cloud services, businesses benefit from services assured with the highest levels of security that are maintained by experts dedicated to combatting threats as they emerge.

The maturity of the cloud means that not only are businesses willing to use it for the delivery of operations and IT services, they are also embracing it for security tools and managed services. And as businesses look at how the cloud can help make them more secure, ease of integration is top of mind – whether that's with on-premise applications or other cloud services. What businesses want more than anything else are security solutions that can protect their data wherever it resides, and secure the systems their businesses use, whether in-house or via third parties.

This is exactly the right approach to take. The move to the cloud won't be an all-encompassing migration. Businesses will want to make the most of existing investments and only adopt cloud alternatives once these have reached the end of their product lifecycle. The pace of cloud adoption will also vary from one industry to the next, and even one business to the next, depending on business models, customer requirements and the competitive landscape.

Organizations today therefore need cloud security tools that are flexible enough to secure the enterprise as it is today, and as it will be tomorrow.

Methodology and executive analysis

Nominet commissioned a survey of 274 Chief Information Security Officers (CISOs), Chief Technology Officers (CTOs), Chief Information Officers (CIOs) and other professionals with responsibility for overseeing the cyber security of their organization.

Respondents were sourced from large organizations (with 2,500 employees or more) within the UK (117) and the US (157), spanning a range of industries and sectors including automotive, Critical National Infrastructure (CNI), finance, government, healthcare, hospitality, legal, life sciences, retail, transport and utilities.

About Nominet

Nominet is driven by a commitment to use technology to improve connectivity, security and inclusivity online. For over 20 years, Nominet has run the .UK internet infrastructure, developing an expertise in the Domain Name System (DNS) that now underpins sophisticated threat monitoring, detection, prevention and analytics that is used by governments and enterprises to mitigate cyber threats.

A profit with a purpose company, Nominet supports initiatives that contribute to a vibrant digital future and has donated over £47m to tech for good causes since 2008, benefitting more than 10 million people. The company has offices in Oxford and London in the UK and Washington DC in the US.

Nominet's Cyber Security Solution – NTX

NTX will reduce risk on your network and eliminate threats before they cause harm.

All networks rely on DNS traffic. It is a critical source of information to check for threats and monitor the health of a network, but often overlooked in the security stack. NTX analyzes network DNS traffic for both known and unknown threats. Embedding our patented algorithms means we eliminate threats from the network and identify zero-day activity not seen by traditional methods of detection. This narrows the window when malicious activity can compromise your network.

While best practice suggests that security should be considered at the planning stages of digital transformation initiatives, Nominet's NTX platform can be installed at any point in a project and deliver the same immediate protection to devices, systems, and data. This can be exceptionally useful in cases where it has not been possible to consider security at an earlier stage.

Eliminate network threats before they cause harm

Our continuous R&D efforts create powerful insights to predict, detect and block network threats.

Proven & trusted cyber security services

Protecting enterprise customers and chosen by UK Government.

Contextualize your network and know what good looks like

Understand normal network behaviors and identify any abnormal trends.

Threat hunting & forensics

Granular data capture to provide meaningful insight for the duration of your service.

Easy deployment & integration

With minimal touchpoints and rich APIs for your existing security investments.

NOMINET

NOMINET
CYBER
SECURITY

For more information on how Nominet can help secure your business, please contacts us on:
UK: +44 (0)1865 332 255 | USA: +1 202 821 4256 | info@nominetcyber.com | nominetcyber.com