ORACLE

intel

Secure and Manage Hybrid Cloud

Your Platform for compliance and security.

Insights from an independent global survey of 730 senior IT professionals demonstrating a clear link between cloud, compliance and security.

Longitude | THOUGHT LEADERSHIP SPECIALISTS

Cloud and Security: Better Together

What is the most compelling argument for migrating an organization's technology to a cloud platform? With the number of cyberattacks and data protection breaches increasing exponentially, the need to improve security could be the biggest driver of all for migration.

Cloud can be a decisive enabler of security—and the security it offers can ease adoption.

That message may surprise some people. There has long been a perception that cloud migration introduces a new source of cyber risk, or exposes organizations to additional vulnerabilities. However, survey analysis by Longitude Research flatly contradicts this idea. It reveals that advanced cloud-based technologies not only help to thwart attacks, but can also anticipate problems before they occur.

Indeed, the research reveals that it is the companies with the highest degree of cloud maturity that have the most confidence in their security capabilities. And much of this confidence stems from their partnerships with cloud providers.

"Cloud computing is about economies of scale," explains Daniele Catteddu, managing director EMEA at the Cloud Security Alliance. "Security in the cloud is no different. No matter the size of financial institution or healthcare organization, it can't match the budget and specialist skills of the big cloud players."

> "If the vendor is treating the service in the right way, it's probably more secure than running it internally in your own data center."
>
> Conny Björling
> Head of Enterprise Architecture
> Skanska

Conny Björling, Skanska's head of enterprise architecture, questions why many people think they are more secure running their own platforms than going to a cloud vendor. "If the vendor is treating the service in the right way, it's probably more secure than running it internally in your own data center," he says.

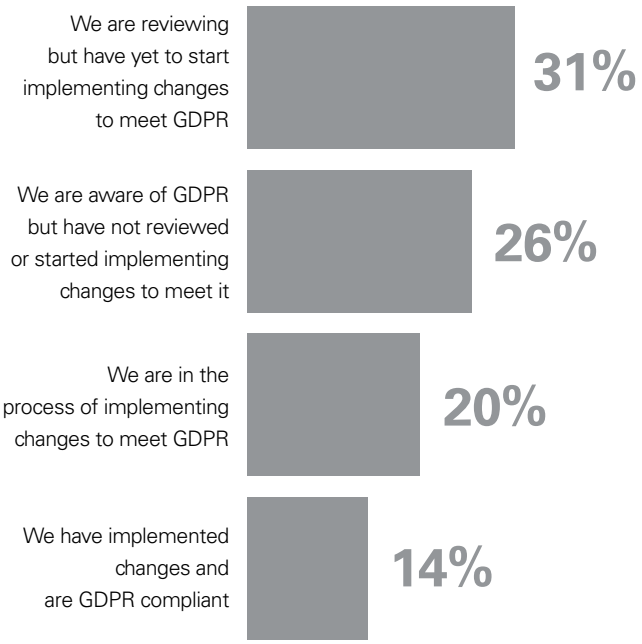
The Regulation Imperative

All companies are being pushed by regulatory change to make big decisions regarding their IT and data security. Most recently, the European Union's General Data Protection Regulation (GDPR) came into force in May 2018, and many enterprises were unprepared. More than a quarter (26 percent) of businesses in the survey said they had not reviewed or started implementing the changes required to comply with GDPR, with only months to go.

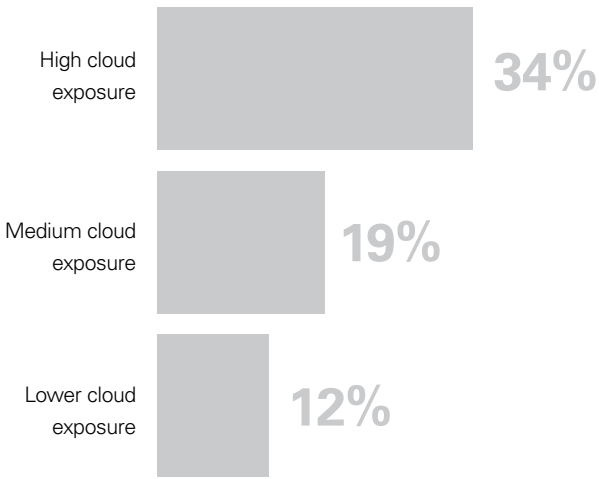
Cloud computing platforms provide a way to remedy this problem, with the survey showing a striking correlation between cloud maturity and GDPR compliance—the most cloud-mature organizations are significantly more likely to have made good progress preparing for GDPR.

In other words, organizations with more exposure to the cloud are on the front foot. They are taking action in order to comply with the new regulation. Equally, those firms that have a developed cloud strategy are also ahead of the game on GDPR compliance. Not only are cloud-mature firms more active in their quest to be GDPR compliant, but the cloud is helping them secure compliance.

Preparation for GDPR



GDPR progression by level of cloud maturity



Continuous Compliance

Compliance with GDPR—or any other regulation—is not a one-off exercise. It requires ongoing attention to ensure continuous compliance—particularly given the increasing amounts of data flowing into organizations, and the proliferation of data classification and discovery methods.

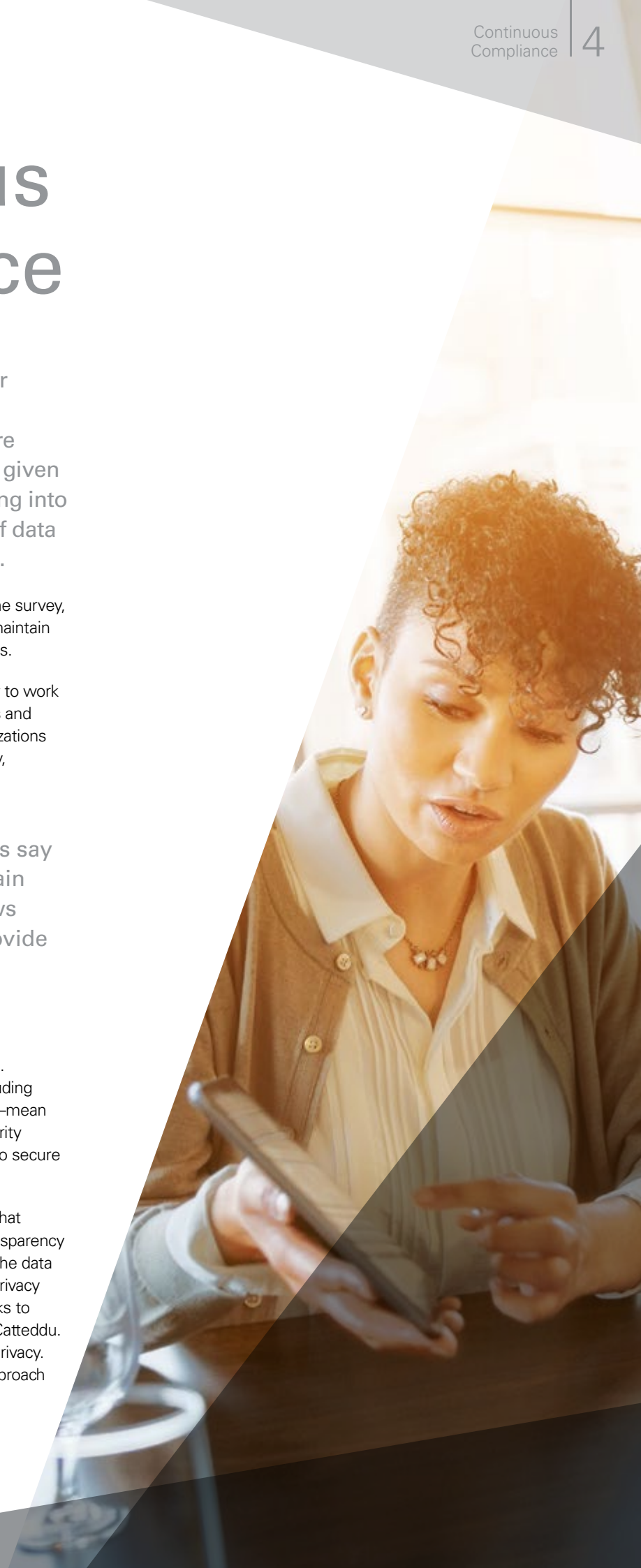
However, continuous compliance is challenging. In the survey, 43 percent of organizations say it is very difficult to maintain compliance with government and industry regulations.

The good news is that cloud platforms provide a way to work toward continuous compliance, with usage protocols and configurations that can be arranged to ensure organizations stay within the rules—and adjusted, when necessary, quickly and easily.

> 43 percent of organizations say it is very difficult to maintain compliance. The good news is that cloud platforms provide a way to work toward continuous compliance.

The best time to start this process is ahead of GDPR. The potential consequences of a GDPR failure—including fines of up to four percent of global annual turnover—mean that chief information officers, chief information security officers, and data protection officers should be able to secure the resources and budget they need.

"In extreme synthesis, what the GDPR is saying is that organizations need to enforce accountability and transparency principles. They need to be responsible stewards of the data in which they are entrusted, and apply security and privacy measures that are good enough to cope with the risks to which personal data are exposed," explains Daniele Catteddu. "The regulators aren't asking for perfect security or privacy. Rather, they are asking to implement a risk-based approach and appropriate level of protection of personal data."



Systems and Data Management

The survey shows that cloud-mature organizations and those that have moved enterprise data to the cloud have found it to be a more secure environment. But what about their machine data—the data generated by systems that provide intelligence about routine operations?

For example, an Oracle Database alert log contains information about startups and shutdowns, changes in system parameters, errors encountered, and other important information. Operating systems and applications also generate a multitude of log files that are updated automatically. Other operational data includes system and application configurations, and user interactions such as application response times and transaction traces.

This data is often both important and valuable. For example, IT operations teams use log files to diagnose issues and troubleshoot problems.

It makes sense to migrate machine data and the applications and security around it to the cloud, for a variety of reasons. First, since logs are voluminous and organizations require significant computing power to efficiently explore them, cloud is the best way to store this data so that it can be analyzed for operational and security reasons.

Second, while log data has been in use for some time, user experience and application configuration data is harder to collect and analyze, due to a need to change application code. However, next-generation systems management solutions have solved this issue, and are able to apply cloud-based machine learning to the entire dataset across logs and other data sources.

The benefit is that organizations can connect user activity to application activity and transactions—right down to the infrastructures that support them. Ultimately, this results in faster root-cause analysis and troubleshooting of both operational and security anomalies. Machine learning can also help organizations make better forecasts about operational performance and availability, or security vulnerabilities and future threats.

Why should organizations move to the cloud?

Storing machine data in an on-premises solution requires enterprises to compromise on what they collect and analyze, because of the volumes of information collected. Few organizations have the capacity to store everything on premises. But with greater capacity in the cloud, organizations can store more data—which means their machine learning process will generate more meaningful insights.

The possibilities are limitless, and the use cases are wide-ranging. For example, organizations can collect user experience data, as well as internal and external security monitoring data. Knowing who is accessing the data in real time, and then spotting patterns and anomalies, can help companies head off security issues before they cause difficulties.

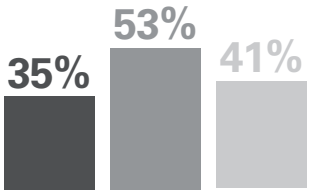
This automated monitoring of systems and data is a sensible use of resources. In the research, a lower proportion of firms that are highly exposed to the cloud say time and money spent on tracking systems of record is negatively impacting the organization than those firms with less cloud exposure (32 percent compared with 38 percent).

Equally, a higher proportion of firms with medium levels of cloud exposure agree with many negative attitudes to security. This may be because they have yet to migrate more critical data, such as machine data, which would give them greater visibility.

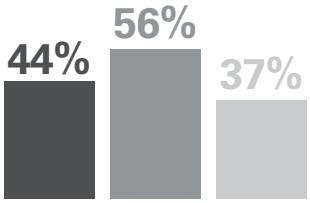
Firms that are integrating several cloud and on-premises solutions will also need to put in place additional monitoring to secure the application programming interfaces (APIs) between them.

APIs have IP addresses of their own that can be accessed externally and compromised in a cyberattack, so it is important to monitor API usage in order to detect unusual activity. This will ensure that organizations have greater visibility and tracking ability across their entire IT environment, keeping them more secure.

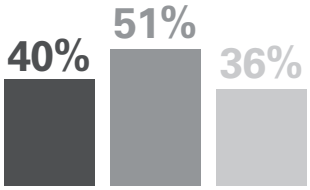
Attitudes toward security



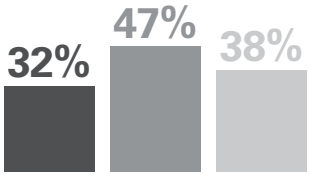
Existing security tools do not meet cloud and on-premises security requirements



Our current tools do not give complete visibility across the entire IT environment



It is very difficult for our organization to maintain compliance with government and industry regulations



Time and money spent on tracking systems of record is negatively impacting the organization

High cloud exposure

Medium cloud exposure

Lower cloud exposure

Security at the Forefront

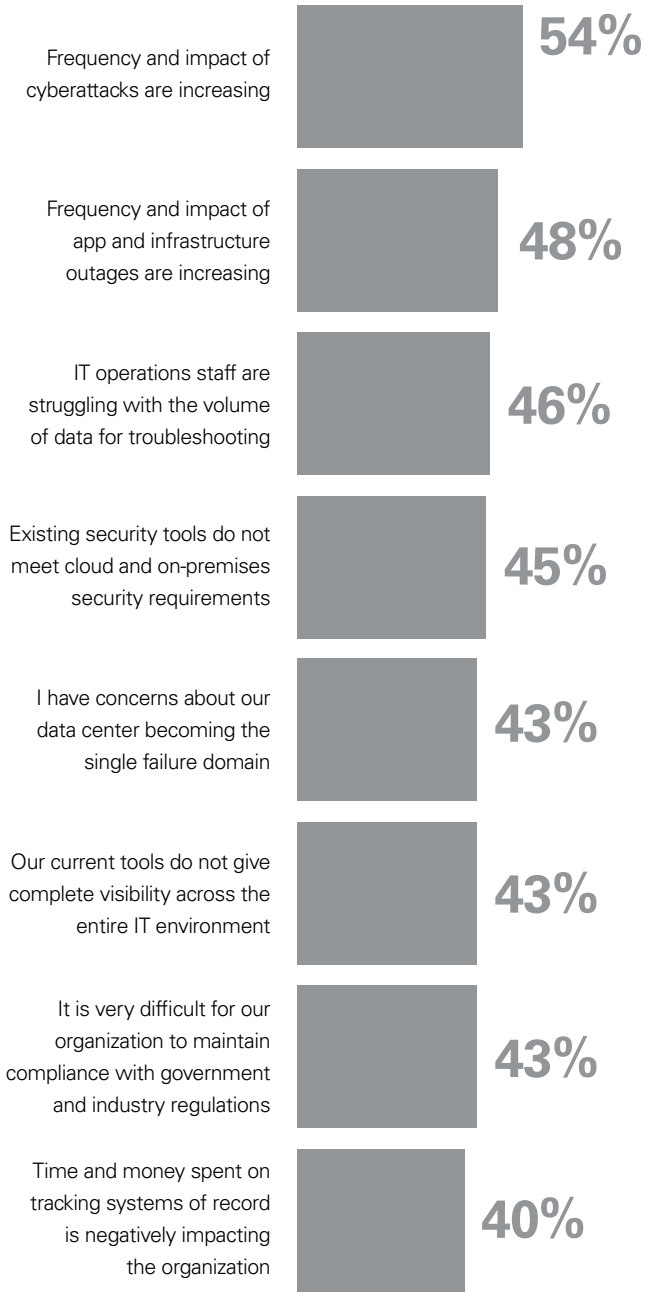
In years gone by, organizations invested in a panoply of security products, but cloud migration offers an opportunity to embrace more holistic, secure cloud access security broker (CASB) solutions.

According to technology research company Gartner, "the continued and growing significance of SaaS [software-as-a-service], combined with persistent concerns about security, privacy and compliance, continues to increase the urgency for control and visibility of cloud services."[1]

There is no single security threat; the threats are coming from every direction. The challenge for organizations is therefore to develop their resilience.

"CASBs provide information security professionals with a single point of control over multiple cloud service concurrently, for any user or device," adds Gartner.

Attitudes towards cybersecurity

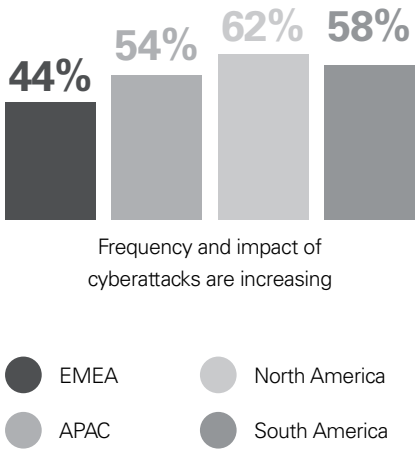


[1]https://www.gartner.com/newsroom/id/3744917

Security concerns are more acute in North America.

Almost two-thirds (62 percent) of North American respondents consider the frequency and impact of cyberattacks to be increasing, compared with 44 percent of respondents in the EMEA region.

Organizations from North America are also more likely to have the greatest concerns over outages, and are more likely to worry that their tools do not provide visibility across the entire IT environment.



With cyber hacking the top concern of respondents in North America and the EMEA region, organizations need to develop both prevention and detection capabilities. This is only possible with the latest cloud solutions, powered by machine learning and big data analytics.

A more proactive stance will enable organizations to predict when alerts might happen, look for anomalies, and find new types of detection. Those with a single view of their environment across their infrastructure, apps, and users will have the ability to respond in minutes rather than days.

This is not to overlook respondents' second most pressing concern: infrastructure outages. While organizations worry about security, they also need greater visibility of operational performance.

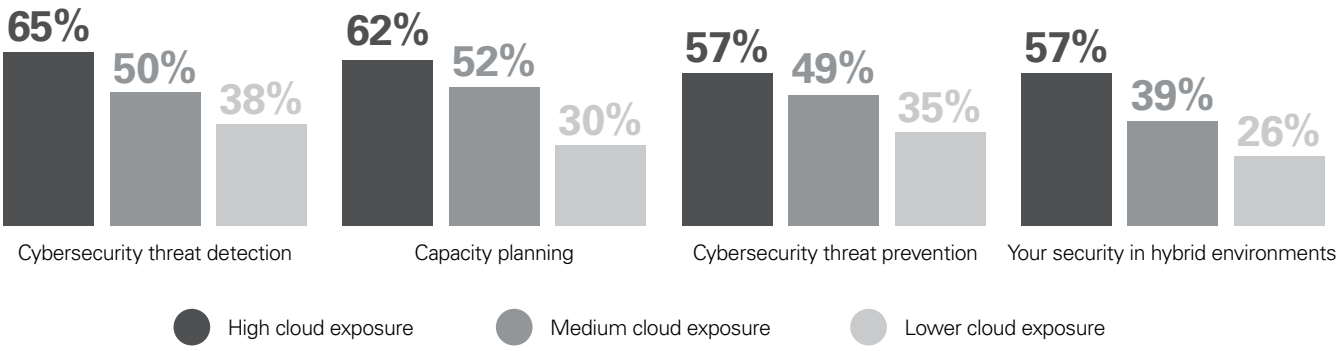
In fact, the same tools that detect and deter cyberattacks can also be used to monitor application performance. Cloud services can provide monitoring and detailed analytics of applications across different environments, which gives organizations early warning of deteriorating application performance.

The two issues may often be linked, of course. Daniele Catteddu points out that cloud can also help with one of the most common cyber threats: denial of service attacks, which can cripple performance. "With cloud computing, you can scale up your resources and make sure you're still available and in business. We should be careful though, because the same scale, elasticity and resource pooling that can be used to protect us could be used to harm us," he says.

> "With cloud computing, you can scale up your resources and make sure you're still available and in business."
>
> Daniele Catteddu
> Managing Director EMEA
> Cloud Security Alliance.

The aggregate impact is both improved performance and greater security. Indeed, the study shows a clear correlation between organizations giving themselves high ratings on security and those that are the most cloud-mature.

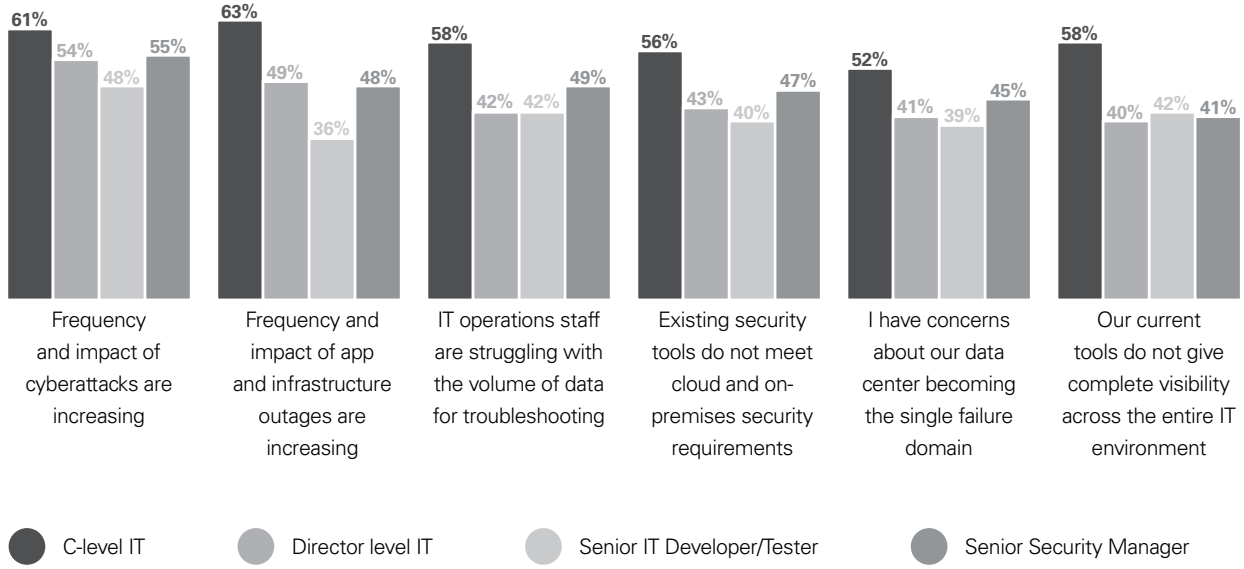
Self-rated security management (good/very good)



A strategic imperative.

With security and management concerns so widespread, the survey reveals the issues that are of greatest concern to C-level IT executives.

Cybersecurity and systems management concerns by role



The research finds that higher proportions of C-level executives share each of the concerns than their less senior IT colleagues, which suggests that they are taking these areas seriously. The broad spread of their concerns, meanwhile, underlines the need for a holistic strategic response.

Conclusion: Future-proofing

Companies have become comfortable about migrating their infrastructure to the cloud, but the stigma of perceived insecurity persists in places. Gartner has predicted that cloud security will be one of the five key cybersecurity trends both this year and next.[2]

The research provides reassurance for those who worry about security in the cloud. In fact, organizations with greater cloud maturity tend to be more compliant with new regulations and feel better prepared in terms of cybersecurity than organizations that are less exposed. And while they recognize the need to continue improving the security of data stored in the cloud, mature cloud adopters are upbeat about prevention and detection.

There is, in other words, a clear link between cloud, compliance, and security. Migration can therefore play a key role in helping organizations improve their resilience.

For further information, visit: oracle.com/goto/yourplatform

Try Oracle Cloud today

ORACLE®
Cloud Platform

[2]http://www.gartner.com/smarterwithgartner/5-trends-in-cybersecurity-for-2017-and-2018/
Source: Cloud Insights survey, Longitude Research, August 2017