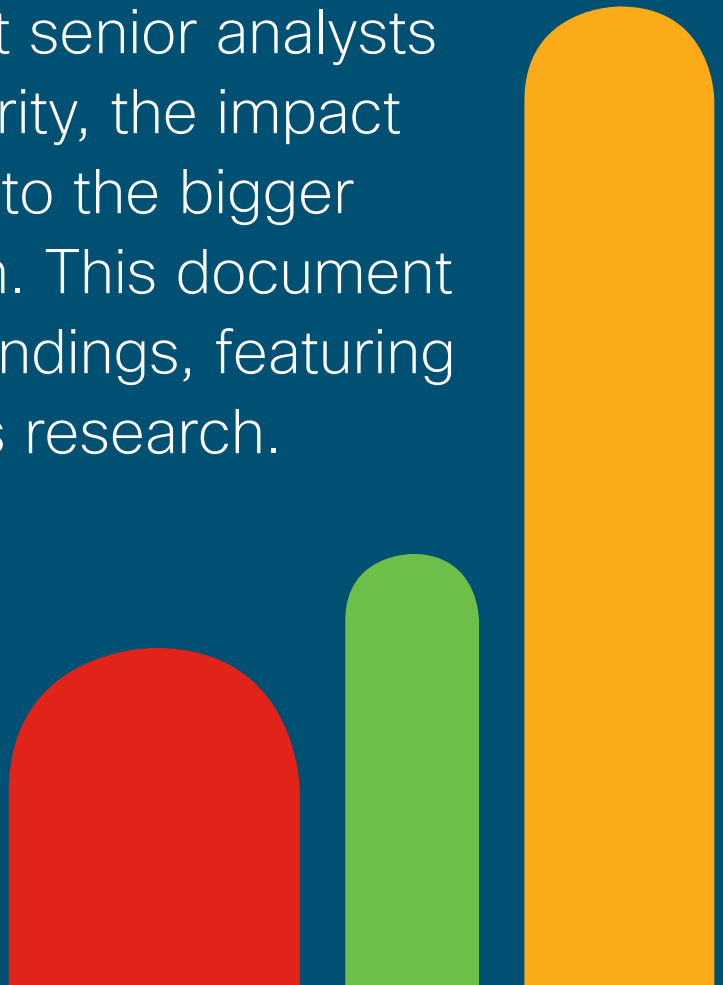
From security and compliance to digital trust

How IT leaders are approaching security in the age of digital transformation

Ovum
TMT intelligence | Informa

With analysis from Ovum

For those with security and compliance in their job titles, we're in a tumultuous time. We sat down with two of Ovum's most senior analysts to discuss trends in cybersecurity, the impact of GDPR and how all this fits into the bigger picture of digital transformation. This document summarises some of the key findings, featuring exclusive content from Ovum's research.



Meet the contributors

Spencer Izard
Chief Analyst, Enterprise Advisory, Ovum

Tim Jennings
Chief Research Officer, Ovum

Phil Goff
Manager, Systems Engineering, Cisco Security

Paul Docherty
Senior Director, Cisco Security Advisory Services

Security is tied to digital transformation

"Creating digital capability" is the top technology priority for businesses today. In Ovum's latest EMEAR survey of more than 2,200 decision-makers, nearly a quarter said digital was their #1 priority (see Figure 1). No shock there.

But IT leaders also recognise that going digital has huge interdependencies. Like the need to modernise core legacy systems, named as a top-three priority by nearly 60% of leaders. And, critically, the need to protect the digital business by managing security, identity and privacy – a top-three priority for more than half of organisations.

71% said that cybersecurity and data privacy are the most important technology requirements to support a digital strategy (Ovum survey on digital transformation, 2017)

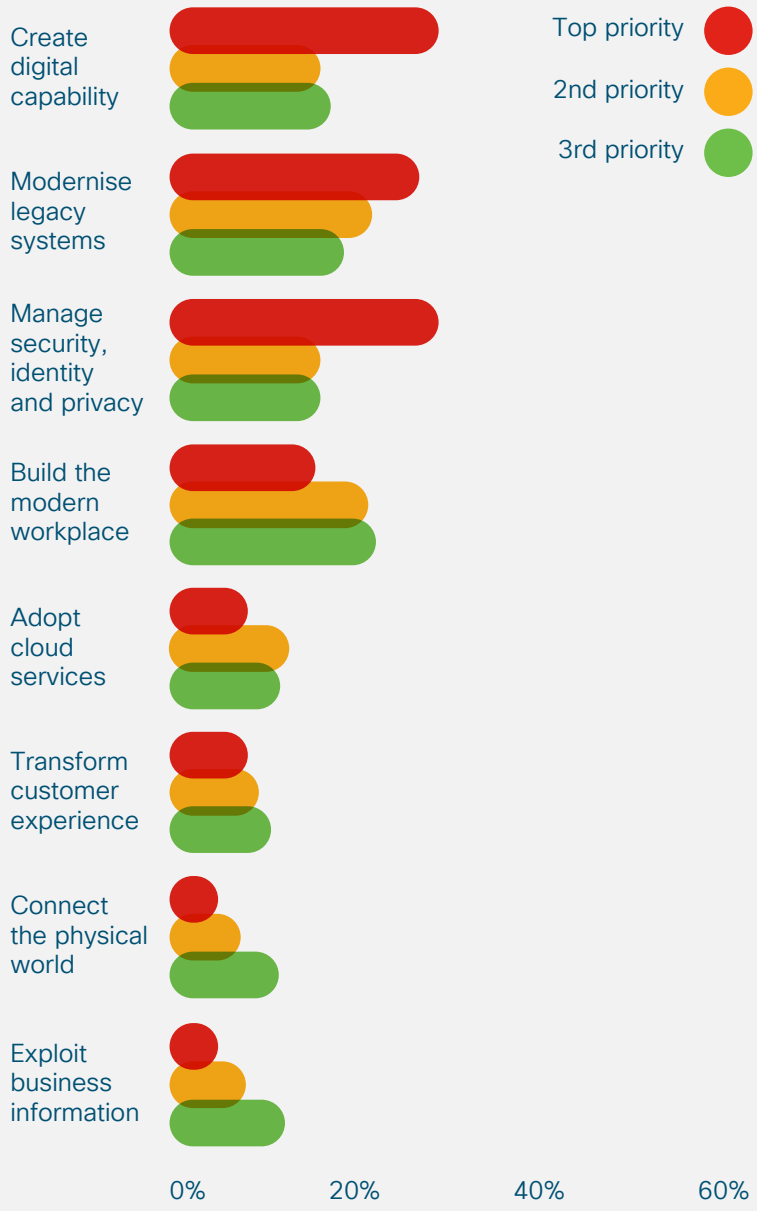


Figure 1: Top technology priorities for EMEAR organisations, N=2,290

That's because while digital initiatives come in many forms, they're essentially about data: data relating to customers, that enables better experiences; data relating to operations, to deliver more agile, automated processes. And this data is often sensitive and therefore governed by regulation and a target for attack.

Ovum's research supports the idea that, thanks to digital initiatives, sensitive data is being gathered, stored, moved and used in more places than ever before (See Figure 2), increasing the attack surface and multiplying the complexity of data governance strategies.

And at the same time, the intensity of attacks on this data has ramped up, with the majority of organisations reporting an increase in the volume of attacks they're monitoring (see Figure 3).

Read our Cybersecurity reports for hard data on the state of the threat landscape today.

60% of respondents said the volume of data breaches has increased, comparing to 1% saying it decreased

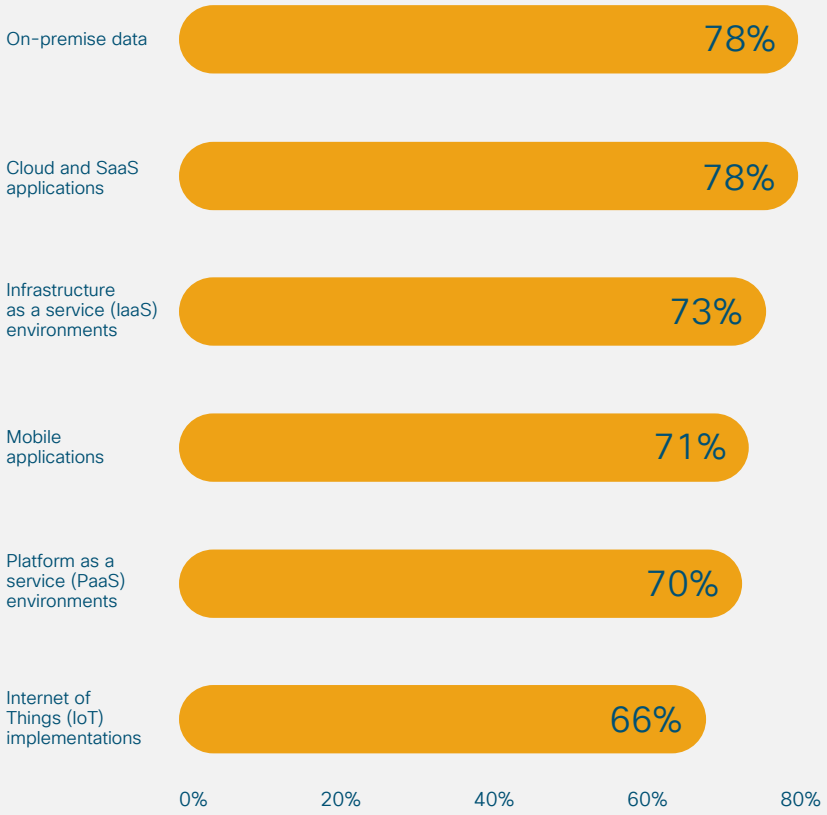


Figure 2: Where will your regulated and sensitive data be held in 2018? Source: Ovum Data Sovereignty Survey

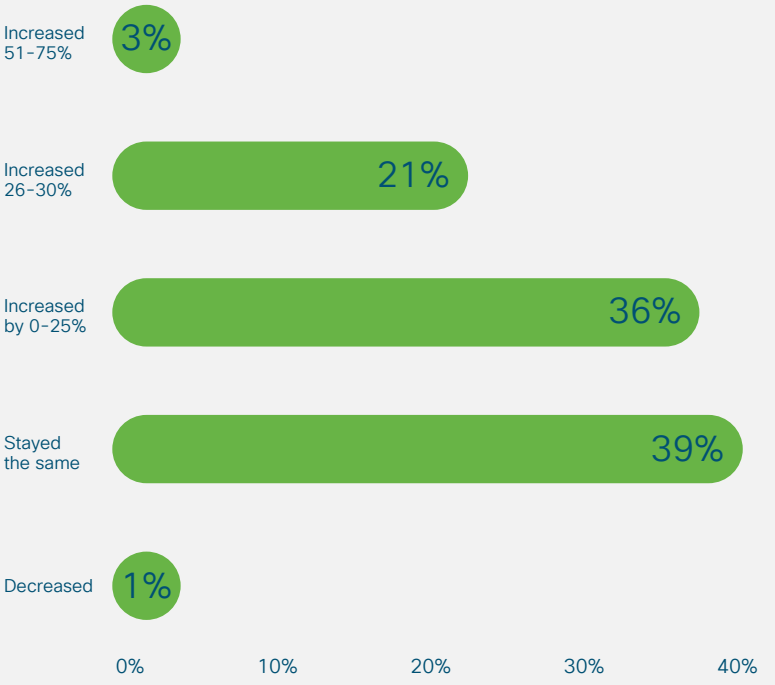


Figure 3: How has the volume of attempted data breaches changed in the past year? Source: Ovum Cyber Sovereignty Survey 2017, N=350

Security and compliance has a reputation problem

Digital trust has value

IT leaders recognise the potential to position security, and its related disciplines of privacy and compliance, as a value-add to the business.

In Ovum's 2017 survey on digital transformation, 93% of respondents said they believe their digital strategy can create value by improving digital trust.

Digital trust means being able to show customers, ecosystem partners and business stakeholders that risks are well understood and effectively managed, so they can get on with doing business with confidence. This kind of trust is essential when exploring new customer experiences, products and services, and business models, where the exchange of value (and data) between players is new and unfamiliar.

Security as afterthought

But today security isn't always viewed as a critical enabler for innovation that should be prioritised.

In our experience talking with customers, and in the experience of the analysts from Ovum, security is often bolted on late in a project, only to be cut again as too expensive as initiatives advance.

Although security spending has never been higher, basic operational best practices like patching and decommissioning old systems are neglected, leaving vulnerabilities lurking across the infrastructure.

Many budget-holders still believe deep down that if they put the right perimeter security in place – basically, firewalls – they won't suffer a breach, meaning other security techniques like segmentation and monitoring are neglected. As a result, it can take months to detect a breach.

When security investments are made, they're done so tactically and reactively: a specific need is spotted, and a point product is purchased to answer that need, leading to fragmentation and complexity across the toolset over time. In Ovum's 2017 Cyber-Security Survey, only 50% of respondents agreed that "we look to invest in new solutions before we experience the threats they can help us with".

All of this is symptomatic of a perspective in the business that delivering IT projects is hard enough, and slow enough, already, without the security team coming in and causing more delays and costs.

In Ovum's research, 66% said it's highly important to address compliance and regulation in order to be successful in digital transformation.

GDPR and the march of compliance

Compliance requirements are often viewed in the same way as security: a series of arduous, costly hoops to jump through in order to get a rubber stamp and be able to get on with business, instead of as an opportunity to get ahead and build digital trust.

GDPR is a case in point. Many organisations we've spoken to, even large financial services organisations, are taking a "wait and see" approach: they're making some progress at getting ready, but are relying on their existing privacy measures and waiting to see how enforcement will be addressed before they take any decisive action.

Others, particularly smaller organisations, have misconceptions about what GDPR compliance entails or even whether it applies to them. A UK government survey published in August 2017 found that only 6% of the top FTSE 350 companies considered themselves already compliant with the regulations.

It's not that IT leaders disagree with compliance in principle or see that there's no value in it. In Ovum's research, 66% said it's highly important to address compliance and regulation in order to be successful in digital transformation.

The challenge is that across the board (and particularly in highly regulated industries like financial services) there's scepticism about compliance as a result of the sheer volume of regulations coming in to effect, and IT teams are prioritising ruthlessly.

Several we spoke to said it's not realistic to be fully compliant with the whole universe of applicable regulations, and at some point the penalties for non-compliance seem less punitive than the cost of achieving compliance.

Check out our GDPR microsite for top resources.

Time for a structured approach to securing digital

If IT leaders are to be seen as a partner to the business and an enabler of innovation – and if they're to effectively protect their digital organisations and ensure compliance – this state of affairs has to change.

So what's the way forward?

Formalising the relationship between digital and security, Ovum has blueprinted six essential foundations of a digital strategy: a comprehensive security architecture is one of them (See Figure 4).

Such a security architecture, or platform, has two fundamental principles:

1. **It's holistic and comprehensive,** designed to give complete visibility to the business right across their infrastructure. This means an end to point purchases and instead a focus on integration of security technologies, and gathering of data from other infrastructure elements, like the network. Security is not a discipline in isolation.
2. **It focuses on sensing and responding** to security events, not building a "hard perimeter". It's a fact of life that breaches are inevitable; security efforts should focus on spotting them quickly, containing them, and mitigating them. Again, the network will be critical here.

Build digital platform
Define a digital platform architecture that supports rapid, automated provisioning of new initiatives

Simplify operations
Simplify and optimize technology operations; make the transition to 'cloud-native' development processes, making maximum use of automation

Manage security risk
Define a comprehensive security architecture designed to rapidly respond to cyber threats, and provide visibility to the business

Unlock data insights
Consider data from the infrastructure and network as a first-class source for insights into business activity

Enhance digital skills
Empower staff to communicate and collaborate seamlessly across any type of business activity, including customer-facing interactions

Partner for success
Seek partners who can support your long-term digital vision and contribute to the overall delivery of digital transformation programs.

Figure 4: Six foundations for a digital strategy

So how do you build an architecture like this? It's undeniably a long journey, and although it's easy to point the finger at limited budgets or legacy systems as the biggest barrier, the reality is that organisational and cultural factors are often the hardest challenges to overcome. So it's as much about cultural and organisational change as about technology. After all, the vast majority of vulnerabilities would be eliminated if businesses followed basic software patching practices, and security training for all employees would help tackle the 95% of breaches that involve human error. We all need to boost our digital skillset.

Bridging the talent gap

Ovum is clear that few organisations will be able to complete this journey alone. The sheer number of security tools, and specialist skills required to integrate them into a coherent security architecture, is proving a challenge to many enterprises.

Third party providers not only have the new technologies needed to secure the digital business, but the in-demand skills, headcount and experience of helping other organisations.

Today, Ovum's research found that only 37% of organisations say they "work with external experts to help us maintain a strong and secure position" (see Figure 5).

But Ovum tracks the number of managed services contracts for security, an indicator of how organisations are choosing to rely on third parties. The number is trending up significantly, as Figure 6 shows.

60% said that external services and partners are core to delivering their digital transformation strategy (Ovum survey on digital transformation, 2017)

Check out our report, Insights at the Speed of Change, to find out more about how businesses are evolving their approaches to security and their relationships with third-party providers.

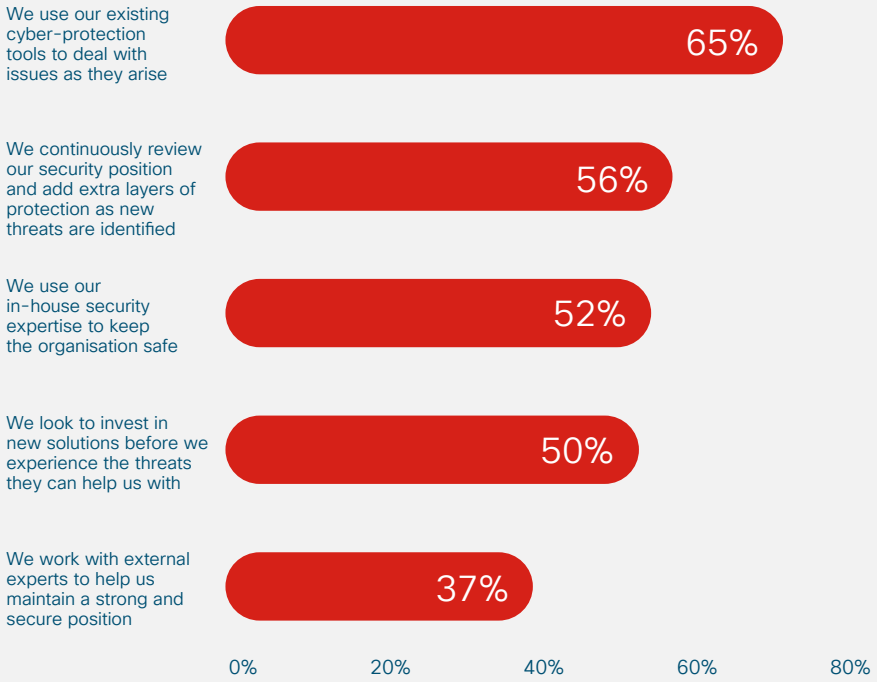


Figure 5: What approach do you take to developing cybersecurity readiness?
Source: Ovum Cyber Security Survey 2017, N=350

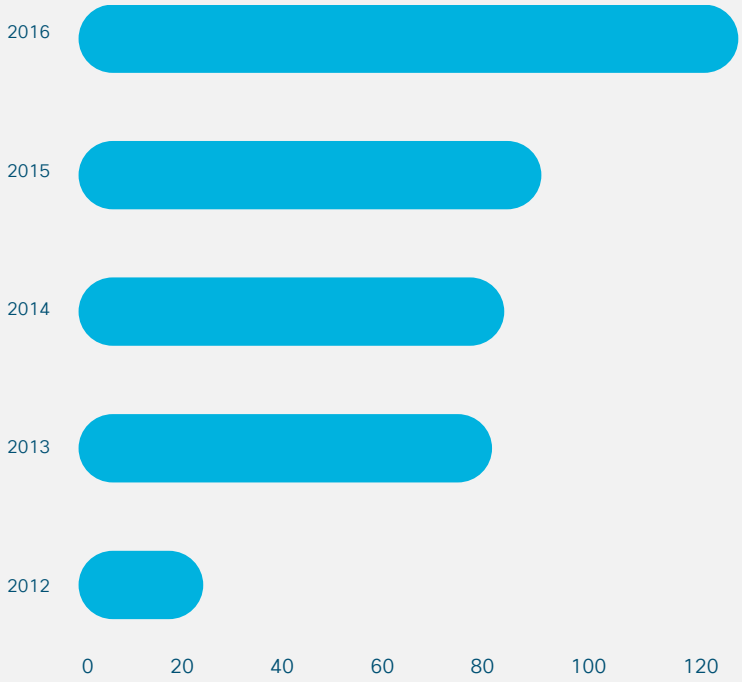


Figure 6: Number of managed security services contracts tracked by Ovum
Source: Ovum IT Services Contracts Analytics

Start today

If IT is going to make the transition from engine room to innovator, it needs to address security. The way it's managed today, security is not only a real and significant challenge to the health of the organisation, but a reputational barrier between IT and the lines of business. The goal must be to show the value of achieving digital trust, and the only way to achieve that is by lobbying for a truly holistic security architecture.

To find out more about how Cisco can help you more effectively secure your digital business and manage risk, **click here.**

Watch the video

Hear Spencer Izard, Tim Jennings and Phil Goff from Cisco discuss the changing threat landscape, GDPR, and new approaches to achieving not just security, but digital trust, in this video (6 mins).