



Is cybersecurity about more than protection?

Global Information Security Survey
2018-19 results
Benchmark APG



The better the question. The better the answer. The better the world works.



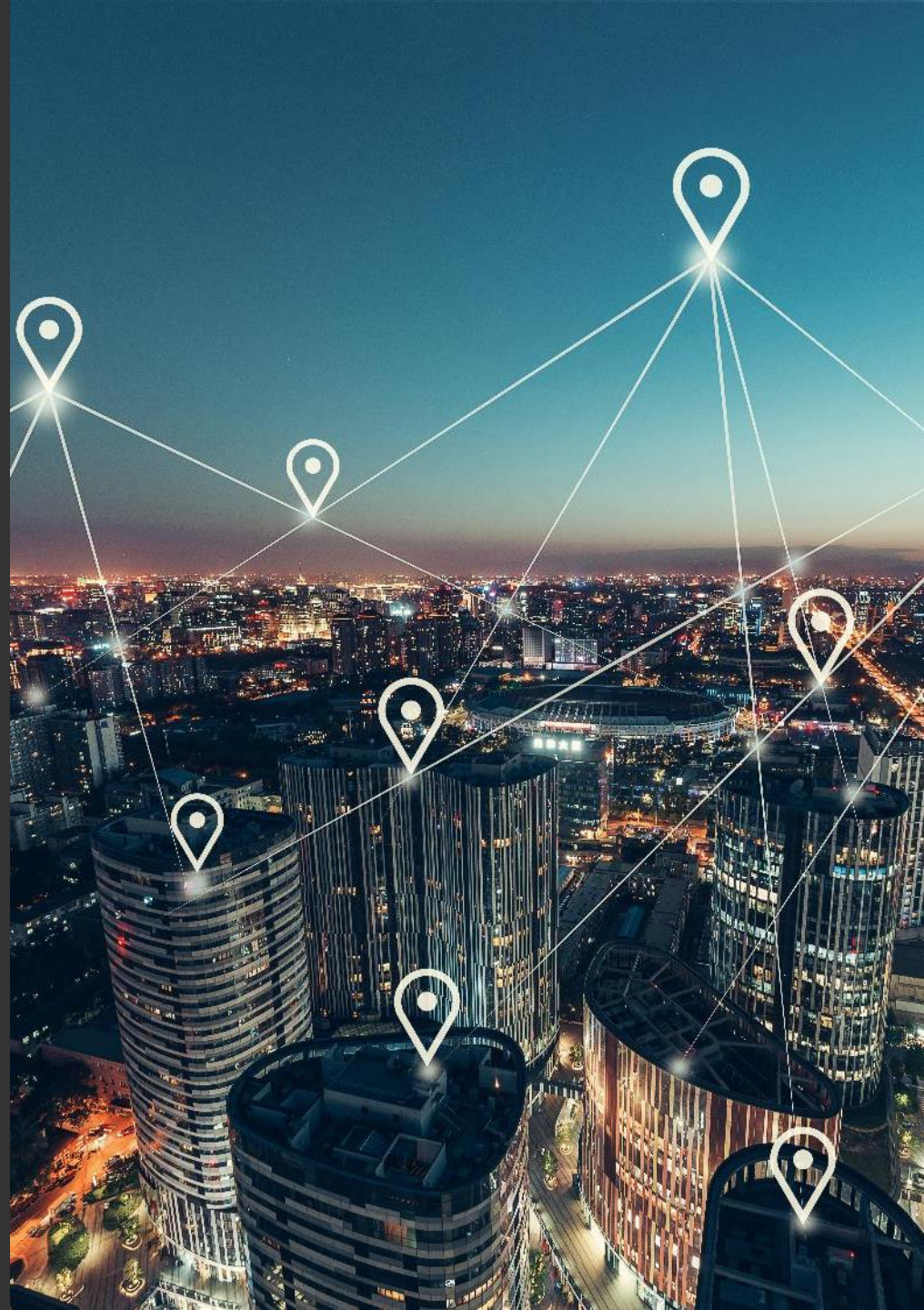
Building a better
working world

Agenda

Overview and the future for cybersecurity	3
Main conclusions	7
Financial Services results – A. Protect the enterprise	11
Financial Services results – B. Optimise Cybersecurity	17
Financial Services results – C. Enable Growth	23



Overview and the future for cybersecurity



EY Global Information Security Survey 2018–19

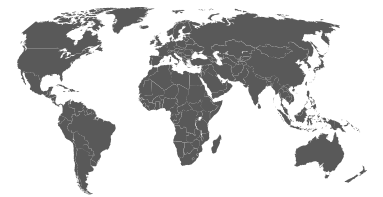


1,400

C-suite leaders and senior information security and IT executives/managers participated to the survey

60 countries

Responses were collected from over 60 countries representing all industry sectors



27%

Financial Services represents 27% of respondents

Insights from the survey will reveal your standing compared with the global results across sectors and for your specific sector cluster

Cybersecurity continues to rise up the boards' agenda, but the survey results suggest that organisations need to do more as attacks continue to grow

After a year in which organisations have been rocked by a series of large-scale cybersecurity breaches and ongoing recriminations over state-sponsored interventions, this years EY Global Information Security Survey shows that organisations are spending more on cybersecurity, devoting increasing resources to improve their defences, and working harder to embed security-by-design.

The survey also suggests that organisations need to do more:

- ▶ More than three-quarters of organisations do not yet have a sufficient budget to provide the levels of cybersecurity and resilience they want
- ▶ Protections are patchy, relatively few organisations are prioritizing advanced capabilities, and cybersecurity too often remains siloed or isolated
- ▶ The frequency and scale of the security breaches all around the world show that too few organisations have implemented even basic security
- ▶ Organisations must, at the same time they still seek to catch up, move forward, fine-tuning existing defences to optimise security and support their growth
- ▶ Cybersecurity needs to be a key enabler of growth, as the digital transformation agenda forces organisations to embrace emerging technologies and new business models
- ▶ Our research suggests that financial services businesses have recognized that tension: protection is high (although continuous reflection and maintenance is necessary) and work on optimizing cybersecurity is underway

It's not easy ... do you recognize this?

6.4 billion

The number of fake emails sent worldwide – every day¹

1,464

The number of government officials in one state using "Password123" as their password²

50%

The number of local authorities in England relying on unsupported server software³

2 million

The number of stolen identities used to make fake comments during a US inquiry into net neutrality⁴

1,946,181,599

The total number of records containing personal and other sensitive data compromised between January 2017 and March 2018⁵

US\$729,000

The amount lost by a businessman in a scam combining "catphishing" and "whaling"⁶

550 million

The number of phishing emails sent out by a single campaign during the first quarter of 2018⁷

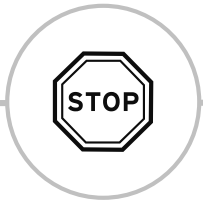
US\$3.62m

The average cost of a data breach last year⁸

Organisations need to progress on three fronts: Protect the enterprise, optimise cybersecurity and enable growth

EY considers that in order to cope with the demanding cybersecurity environment and be able to progress, organisations will have to focus on working at three main fronts

The challenge is for organisations to progress on three fronts:



A. Protect the enterprise

Focus on identifying assets and building lines in defence



B. Optimise cybersecurity

Focus on stopping low-value activities, increasing efficiency, and reinvesting the funds in emerging and innovative technologies to enhance existing protection



C. Enable growth

Focus on implementing security-by-design as a key success factor for the digital transformation that most organisations are going through

These three imperatives must be pursued simultaneously in order to create a sustainable development plan for the information security function of your organisation



Main conclusions: Financial Sector results

Main conclusions: financial services sector

The financial services sector is at the heart of the battle against cyber attacks. Not only does it represent a hugely lucrative target for criminals, but it is also increasingly dependent on data. The sector must keep that data secure at all costs – even as it adapts to initiatives such as open banking, which requires organizations to share data externally with trusted parties.

- Current status. Only 6% of financial services companies say their information security function currently meets their organization's needs, but 65% have plans to make the required improvements. But there's a problem: 31% warn that skill shortages are a potential stumbling block.
- Investment priorities. Organizations in this sector are most concerned about the immaturity of their information security processes in the areas of architecture (cited as non-existent or very immature by 18%), metrics and reporting (18%), and asset management (17%).
- In-house or outsourced. Nearly 6 in 10 financial services organizations (59%) have a security operations centre. They are more likely to run its functions in-house than outsourcing them: only penetration testing (79%) and forensics (52%) are outsourced by a majority.
- Reporting. While only 16% of financial services companies say that their reporting of information security meets their needs, that puts them ahead of other sectors.



Financial Services results – A. Protect the enterprise

To protect the enterprise organisations have to get the basics right and steadily improve, focusing on four vital components

On a global level, many organisations do not have a clear picture of what and where their most critical information and assets are - nor do they have adequate safeguards to protect these assets.

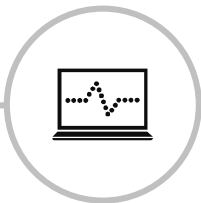
That is why it is important for most organizations to continue to zero in on the very basics of cybersecurity. Organisations should first identify the key data and intellectual property (the “crown jewels”), then review the cybersecurity capabilities, access-management processes and other defences, and finally upgrade the shield that protects the company.

In this section, we will look at four vital components of protecting the enterprise:



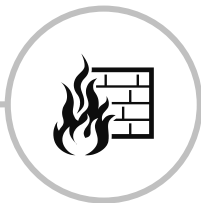
Governance

To what extent is cybersecurity an integral part of the organisation’s strategy and is there enough funding for the necessary investment in defence?



What is at stake?

What do organisations fear the most, and how do they regard the biggest threats they are facing?



Protection

The maturity of the cybersecurity of an organisation and the most common vulnerabilities are key.



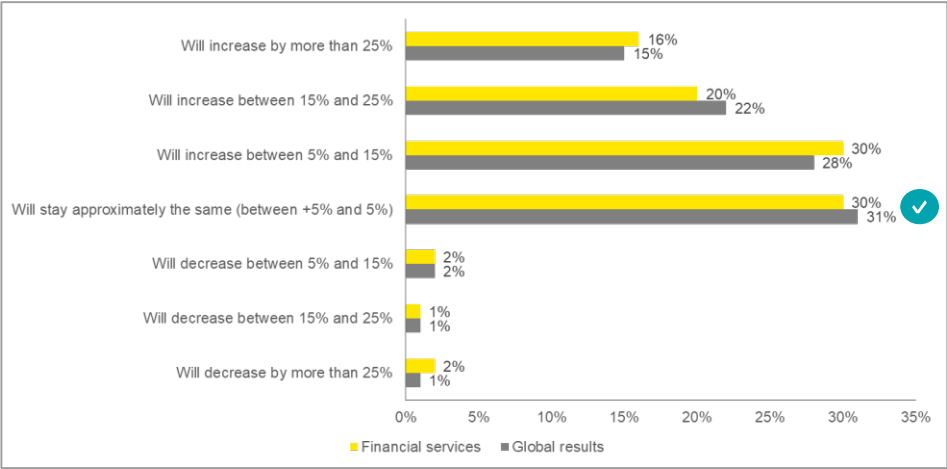
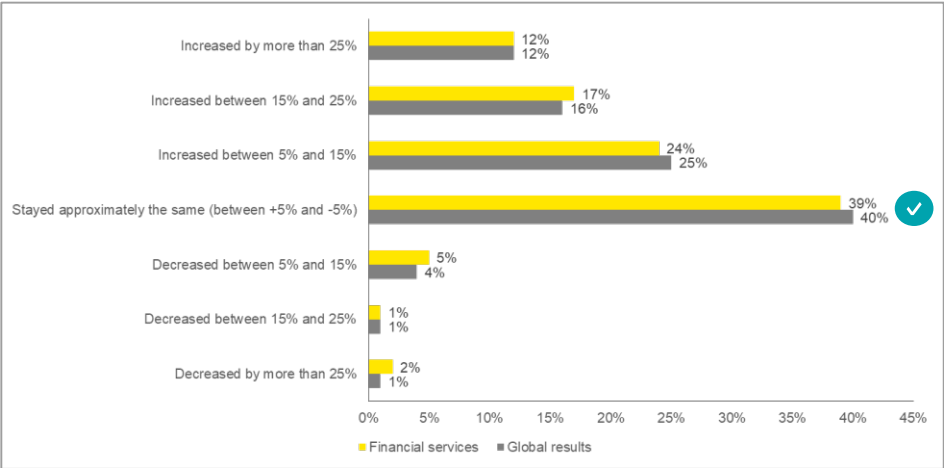
Breaches

How breaches are identified and the way in which organisations respond are critical issues.

Governance: Is cybersecurity a part of the strategy and is it in the budget?

54% of organisations in the financial sector make the protection of the organisation an integral part of their strategy and execution plans. Compared to the Global results where more than the half do not make the protection of the organisation an integral part of their strategy.

Organisations in the financial services sector with an increase in the total cybersecurity budget



53%

Have seen an increase in their budget this year

66%

Forecast an increase in their budget next year

34%

Say that <2% of their total IT headcount work only cybersecurity.

✓ You

Your answer: 2-5% work solely in cybersecurity

What is at stake: What are the biggest fears and threats?

43% of the financial services organisations consider customer information, customers' password and board member information to be the top three most valuable information that organisations would like to protect. Cyber attacks to steal financial information, phishing and malware are the highest ranked threats.

Top 10 most valuable information to cyber criminals

19% - Customer information	✓
15% - Customers' passwords	✓
12% - Board member information	
12% - Financial information	✓
12% - Corporate strategic plans	✓
9% - M&A information	
6% - R&D information	
4% - Patented IP	✓
4% - Non-patented IP	
4% - Supplier and vendor passwords	

Top 10 biggest cyber threats to organisations

20% - Cyber attacks (to steal financial information)	
20% - Phishing	
18% - Malware	✓
14% - Fraud	
11% - Cyber attacks (to disrupt)	✓
6% - Internal attacks	
5% - Cyber attacks (to steal IP)	
4% - Spam	
2% - Natural disasters	
1% - Espionage	

- More organisations are beginning to recognize the broad nature of the threat. One thing that has changed for the better over the past 12 months is a growing realisation that security is also about maintaining the continuity of business operations – and not only about the security of data and privacy
- Increased focus on, and real experience with, big cyber attacks in all sectors are likely reasons for the changes in awareness



You

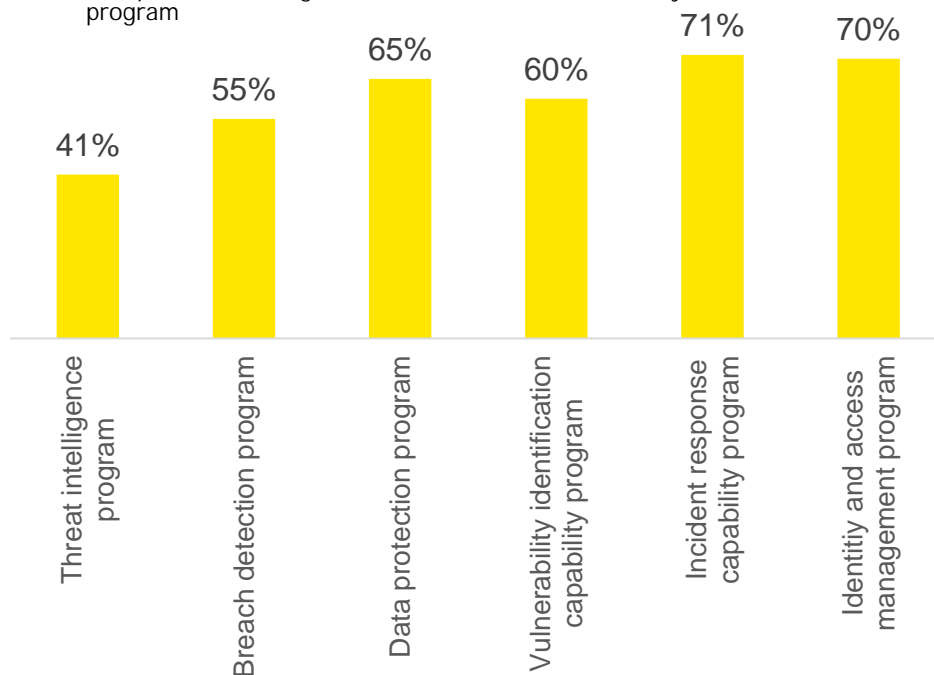
Protection: What are the vulnerabilities and how mature is the cybersecurity in the organisation

60% say that that careless or unaware employees and outdated information security controls are the vulnerability that have most increased organisations risk exposure over the past 12 months. At the same time many organisations have proper cybersecurity programs in place that addresses the different vulnerabilities.



Financial organisations that have a program or have an informal program in different cybersecurity areas:

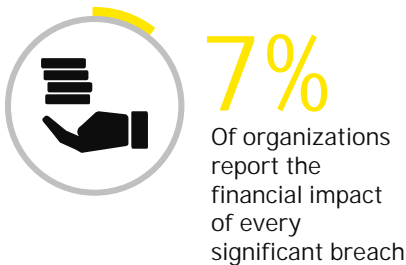
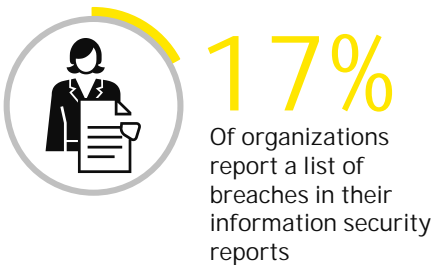
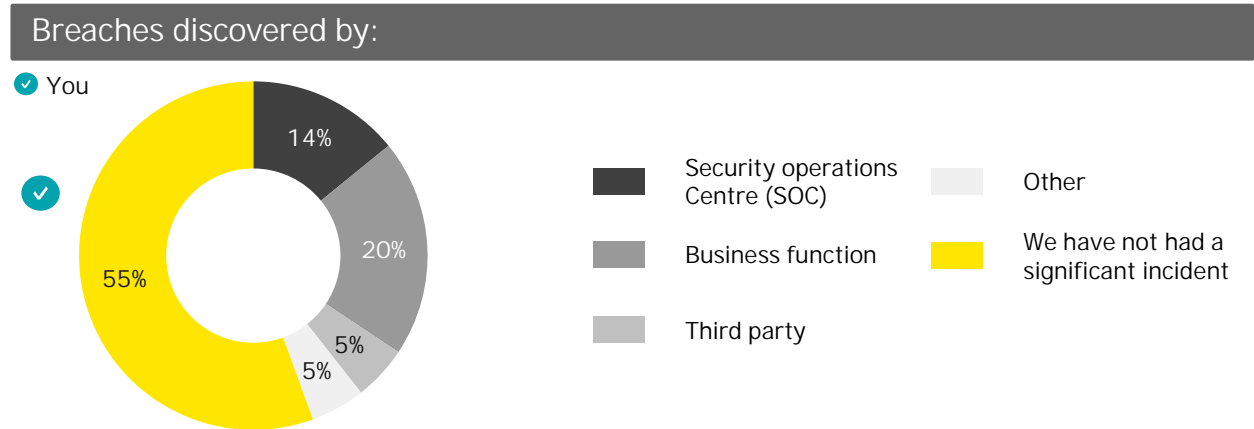
✓ You. In the majority of the programs you have a formal but obsolete program. Except threat intelligence and breach detection there you have an informal program




- Financial services organisations share the trend of general global responses concerning the vulnerabilities that most increased risk exposure over the past 12 months
- Internal factors make most of the top vulnerabilities with careless employees and outdated security controls on top followed by unauthorized access
- Emerging technologies related vulnerabilities rank lower. However, the financial sector should be aware of these, as the sector is looking to these technologies as a way of coping/leading disruption
- Numbers suggest that organisations in the financial sector are relatively more mature in comparison to the other sectors related to their cybersecurity related programs, as many do have formal programs in place either up-to-date or obsolete.

Breaches: How are breaches identified and how do organisations respond?

55% say they have not had a significant cybersecurity incident in the past 12 months. While this may be perceived by some as a reasonable number, no news may actually be bad news. Many organisations only become aware of a breach, if at all, a long time after it has happened



 Your report contains information on how/when to notify, list of breaches, number of attacks, the overall threat level of your organization, areas for improvement. You have also answered that you are unlikely to increase your cybersecurity budget after a serious breach

- Many organizations are unclear about whether they are successfully identifying breaches and incidents. Among organizations that have been hit by an incident over the past year, 14% say the compromise was discovered by their security centre
- The main reason is that SOC's are still too technical and lack business orientation, which makes them less effective in addressing business needs
- Organizations concede that they would be unlikely to step up their cybersecurity practices or spend more money unless they suffered some sort of breach or incident that caused significant negative impacts



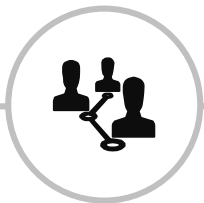
Financial Services results - B. Optimise cybersecurity



To optimise cybersecurity organisations have to move beyond basic cybersecurity while getting the basis right by focusing on four components

Organizations are strengthening their cybersecurity essentials, however they are also rethinking their cybersecurity framework and architecture to support the business more effectively and efficiently. More focus is put on emerging technologies such as artificial intelligence, robotic process automation, and how they can be used to increase the security of key assets and data.

In this section, we will look at four vital components of optimizing cybersecurity:



The status today

To what extent is an organization's information security function currently able to meet its cybersecurity needs.



Investment priorities

Where is investment needed to update capabilities to the standard required?



In-house or outsourced

What is the best way to develop new cybersecurity capabilities and who should take the lead?



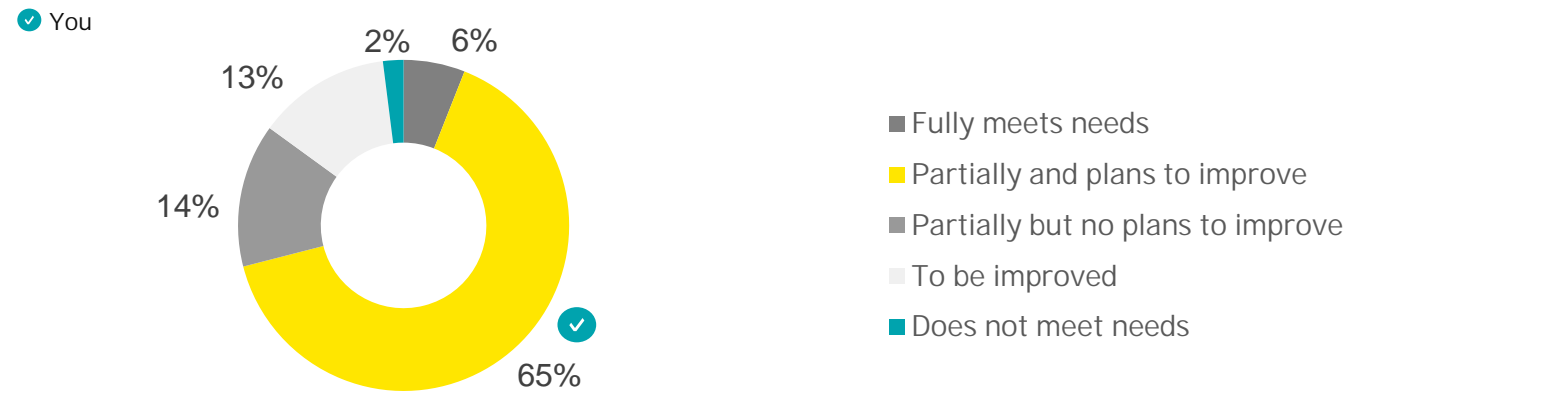
Reporting

How well is the organization able to evaluate its own capabilities and report back to key stakeholders?

Status today: Is the information security function currently meeting the organizations needs? How serious is the shortfall?

63% of organizations in the financial services sector say they are likely or very likely to detect a sophisticated breach. This is a higher number compared with aggregated Global results

How would you characterize the extent to which the information security function is meeting the needs of your organization?



6%

Of organizations in the financial sector have information security functions that fully meet their needs

31%


Of organizations in the financial sector consider lack of skilled resources to be a key challenge for information security.

Your answer: Management and governance issues

- Financial services organisations, following the trend of other global organisations, consider that lack of skilled resources, budget constraints, and insufficient tools are the main challenges organisations face
- Despite stating that budget is a main challenge, financial services organisations are spending more on cybersecurity technologies than in previous years comparing with aggregated Global results
- If the increase in spending on these technologies and the implementation of adequate tools continues, organisational needs may in the future be met to a larger extent


Investment priorities: Where are the gaps and where are resources most urgently needed?

50% of the organizations in the financial sector say they do not perform sufficient forensics after a cybersecurity breach. This decreases their ability to learn from past breaches and therefore their ability to incorporate effective protection against future attacks.




38%

Of organizations in the financial sector have cyber insurance that meet their needs




Your answer: You do not have cyber insurance and are actively looking for appropriate cover

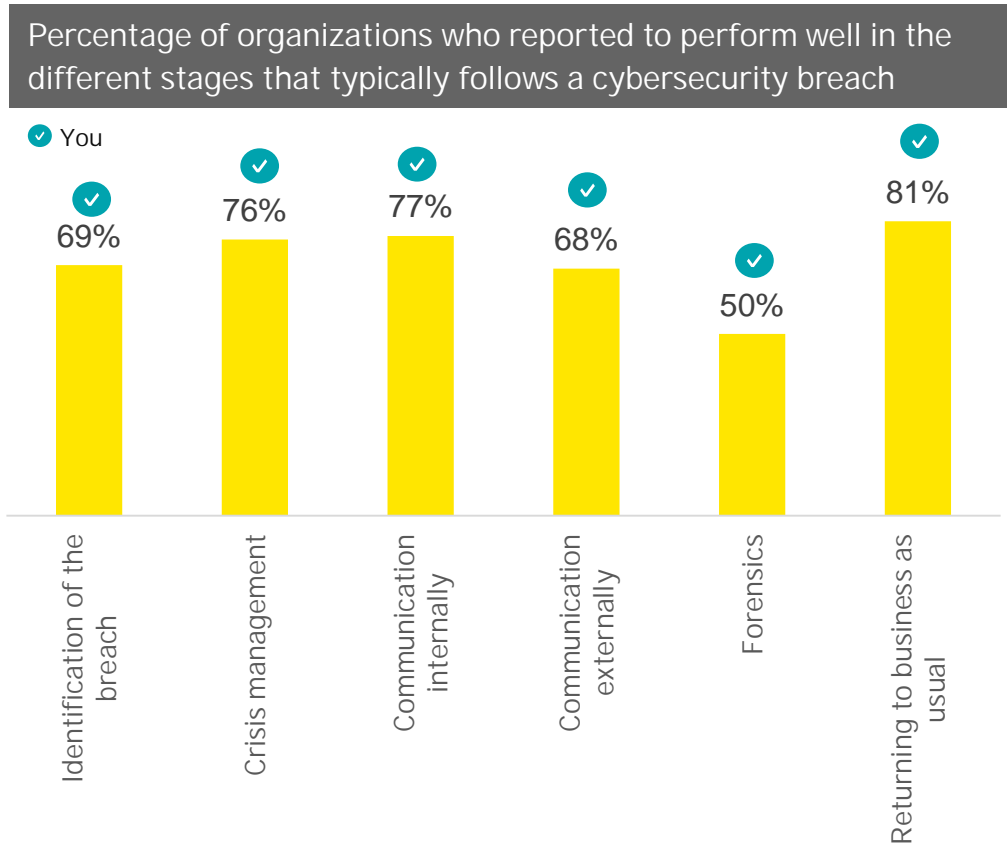


<10%

Of organizations in the financial sector believe they are mature on their cybersecurity processes



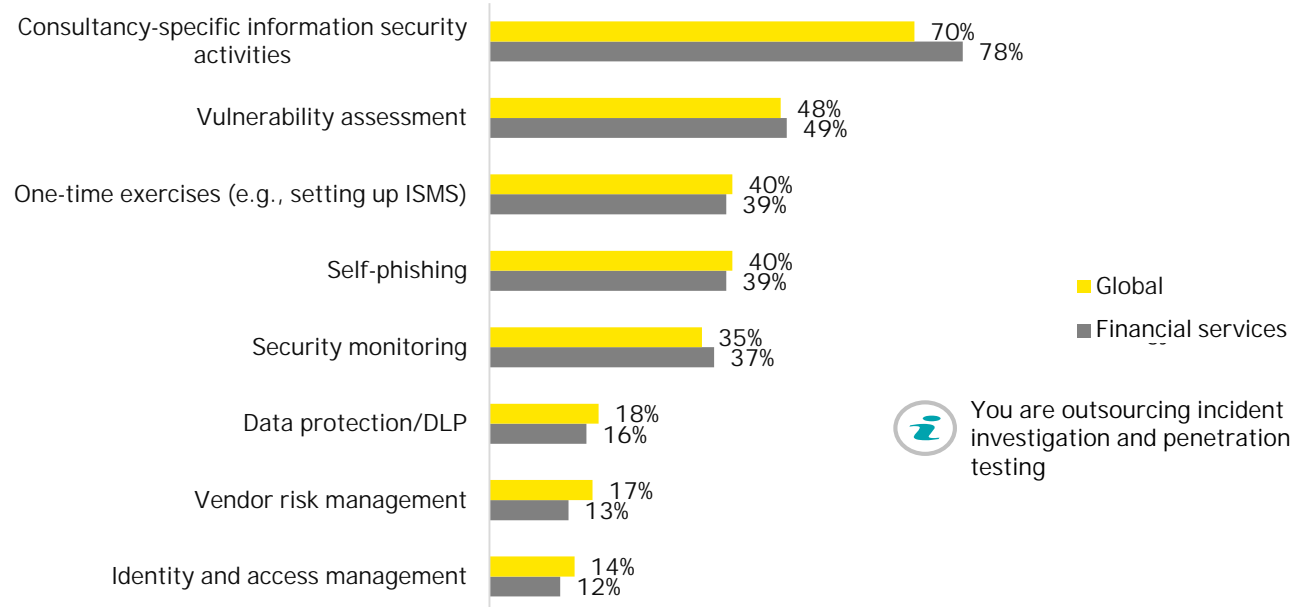
Your answer: On average you stated that maturity is on 3 in a scale of 1 to 5




- A higher percentage of organizations in the financial sector say they are able to return to business as usual compared to other sectors
- The inability to identify breaches, and the reduced learning from identified breaches, may in the long run affect organizations' ability to return to business as usual
- Few organisations believe they have a cyber insurance that meet their needs.
- A cyber insurance could be particularly interesting as less than 10% of organisations believe to have mature cybersecurity processes
- Given this, investments which increase the ability to identify cybersecurity breaches, to perform better forensics, to increase the maturity of processes and to ensure an adequate insurance should be prioritized

In-house or Outsourced: What are organizations doing themselves, and what do they outsource?

Percentage of Global and Financial services organisations who state to be outsourcing information security tasks




 You are outsourcing incident investigation and penetration testing



59%


Of organizations in the financial sector have a security operation center (SOC)

 You have a SOC



78%


Of organizations in the financial sector perform incident investigation in-house

 You have it outsourced



79%

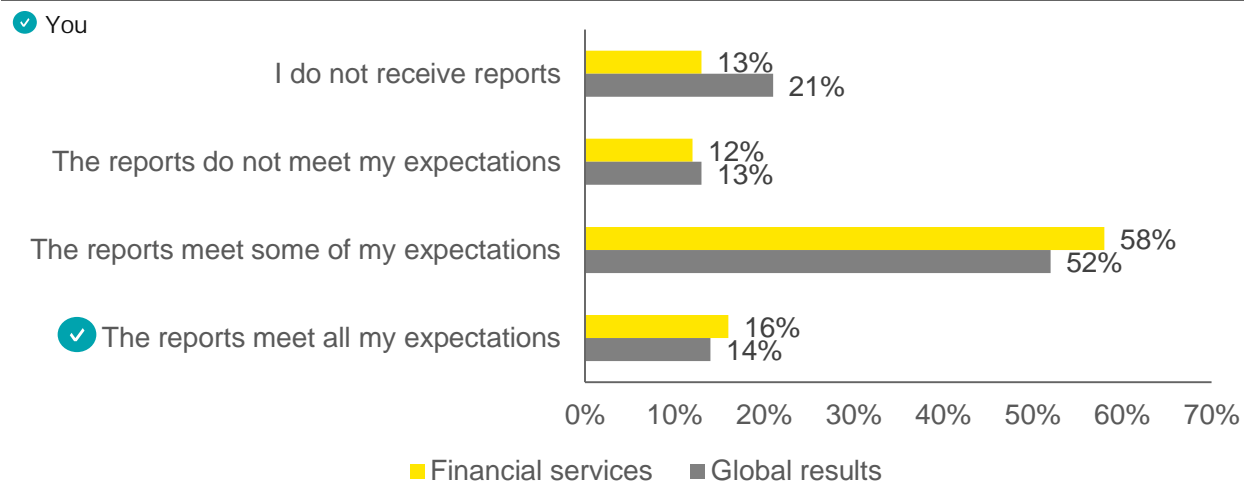
Of organizations in the financial sector outsource penetration testing

 You also outsource

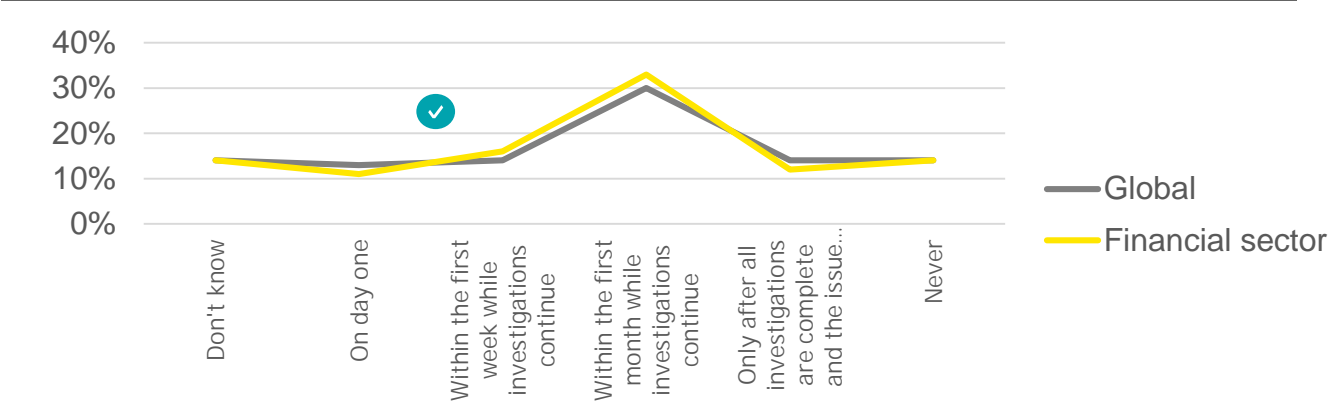
- Financial services organisations resort much less to outsourcing than the rest of the global organisations. Activities typically outsourced, such as Vendor risk management, Identity and Access Management and Data protection/DLP are actually the activities that financial services organisations outsource less
- More than half of organisations in the financial sector have a Security Operations Centre (SOC). The use of SOC's may increase an organization's ability to more effectively and efficiently identify and handle potential security breaches
- Incident investigation is performed mainly in-house. Taking into account the performance results, organisations should ensure that this tasks are performed by a dedicated internal team, with sufficient knowledge, leveraging best practices from 3rd parties, if necessary

Reporting: Is the organization gathering information on cybersecurity capabilities and incidents? How is this being reported to stakeholders?


How effective are your organizations information security reports?



When are significant cybersecurity breaches communicated?



- The financial sector has the highest percentage of organisations who say that their reports do meet some or all their expectations
- Cross-sector findings tend to show that reports focusing on information about breaches, and areas for improvement, meet expectations to a higher degree
- External reporting is taking too long if reported at all
- Reports that meet expectations to a higher degree, lead to better decision making, namely at the executive level, as information is conveyed in an adequate manner and decision makers become better informed

A person in a dark jacket and pants stands with their back to the camera on a wooden pier, looking out at the Shanghai skyline. The Oriental Pearl Tower is prominent on the left, and the Shanghai Tower is on the right. The sky is a pale blue with light clouds. A semi-transparent white banner is at the bottom, and a yellow square is in the bottom right corner.

Financial Services results - C. Enable growth

Organisations will need an innovative cybersecurity strategy that should take into account four key elements in order to enable growth

Organizations are more convinced that looking after cyber risk and building in cybersecurity from the start are imperative to success in the digital era. The focus should now also be on how cybersecurity can support and enable enterprise growth. The aim should be integrating and embedding security within business processes from the start and build a more secure working environment for all.

To achieve these goals, organizations will need an innovative cybersecurity strategy rather than responding in a piecemeal and reactive way.

In this section, we will look at four vital components of making cybersecurity part of the growth strategy:



Strategic oversight

To what extent do boards charged with pursuing digital transformation appreciate the need to build cybersecurity into their growth strategies?



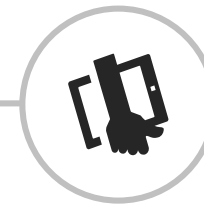
Leadership

Who are digital organizations asking to take the lead on cybersecurity, and how is accountability delivered?



Digitalisation

As organizations make greater use of digital technologies, how much does this increase cybersecurity vulnerabilities?

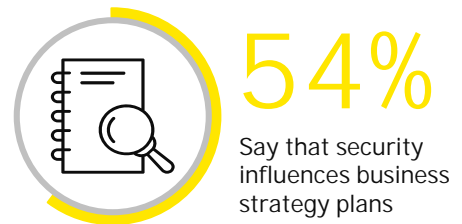


Emerging technologies

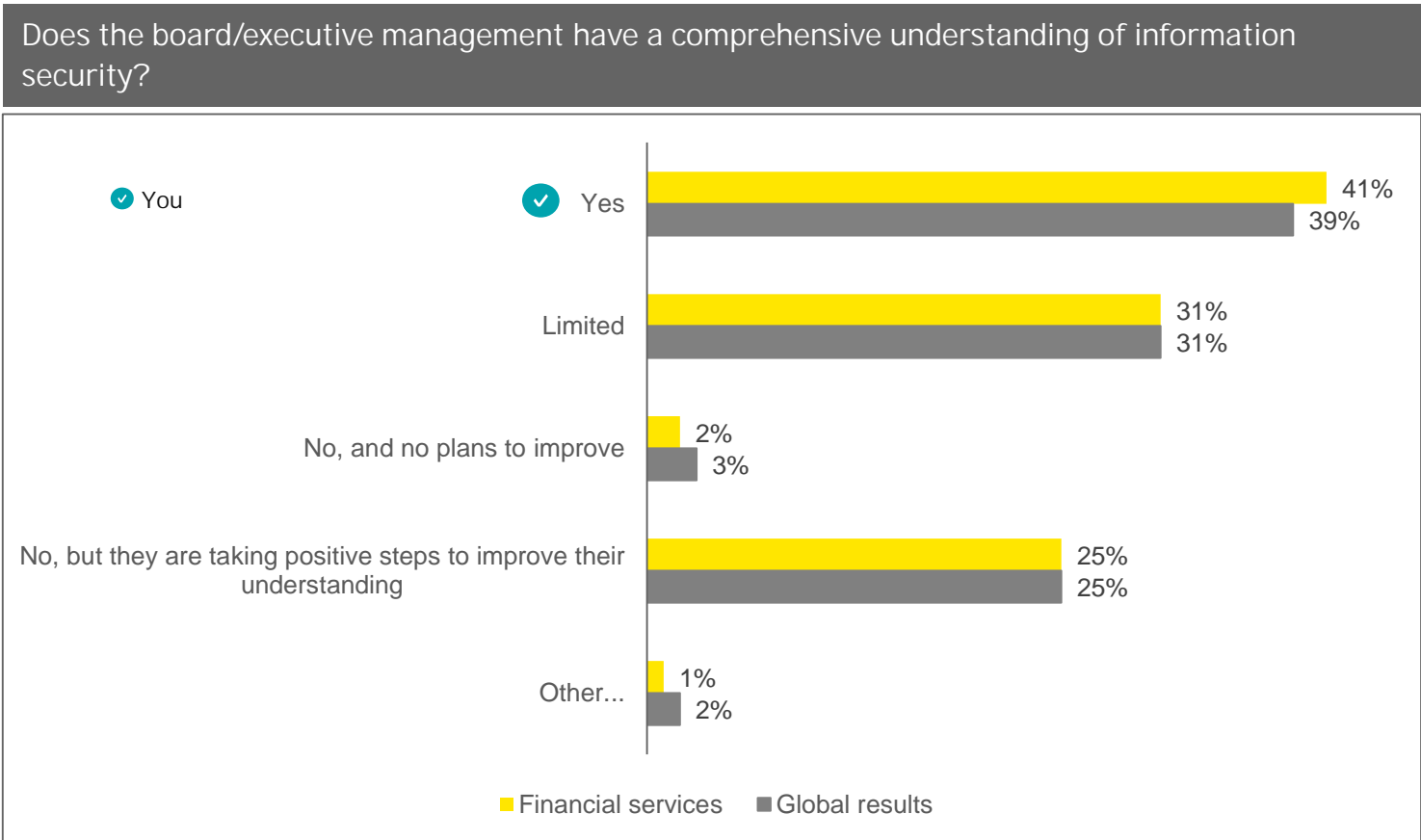
Where are organizations increasing investment in cybersecurity in order to build security-by-design?

Strategic oversight: Do the organisations have structures that make cybersecurity a key element of the board’s strategic planning?

66% of organizations in the financial sector say that their senior leadership has a comprehensive understanding of security or is taking positive steps to improve it. This is a higher number compared with aggregated global results



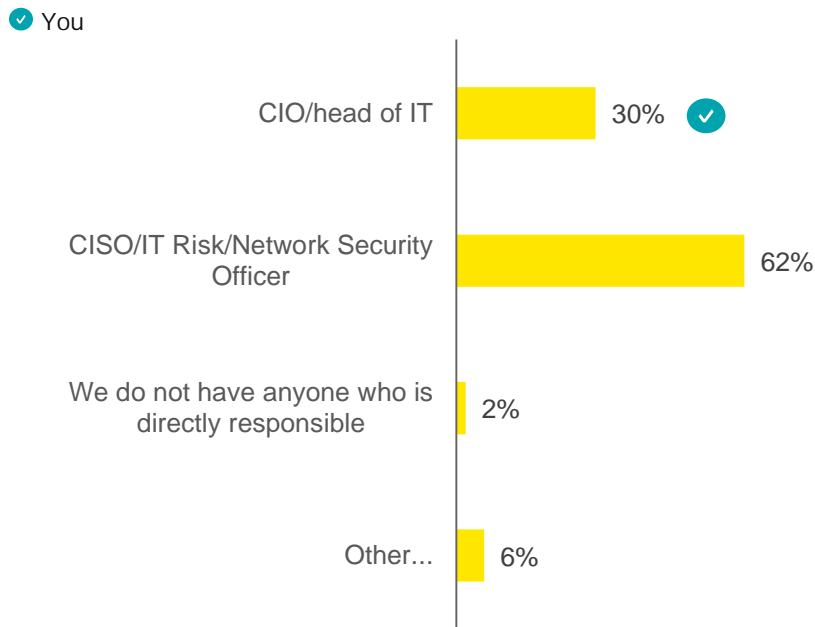
Your answer: Fully on a yearly basis



Leadership: Who is ultimately accountable for cyber security and are they able to drive leading practices across the organisation?

92% of the organisations in the financial sector have a CIO/head of IT or a CISO/ IT Risk / Network Security Officer who is responsible for the information security. Aligned with the global aggregated findings the financial sector have more direct responsibility at CISOs/ IT Risk / NSO and less at CIO/head of IT

Who is directly responsible for information security in your organization?

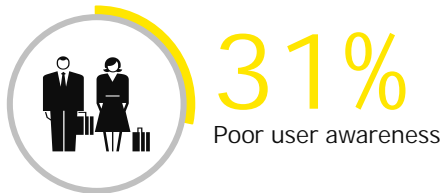



- In the financial sector the ultimate responsibility for information security is not yet held at the most senior levels of the company. In 30% of the organisations it is the chief information officer (CIO) that has this responsibility
- 38% of the direct responsibility for information security is held at the board/executive management. This may lead to decision making that does not take in consideration the entire perspective of the organisation
- As security becomes a key enabler of growth, it is important that information security is prioritized and included in the leading practices. This is also a crucial part in making sure that all people in the organisation see the importance of information security. Organisations in the financial sector should, therefore, consider having more involvement from the board in information security

Digitalisation: As organisations pursue transformation, how does it increase their risk profile? What threats do new technologies pose?

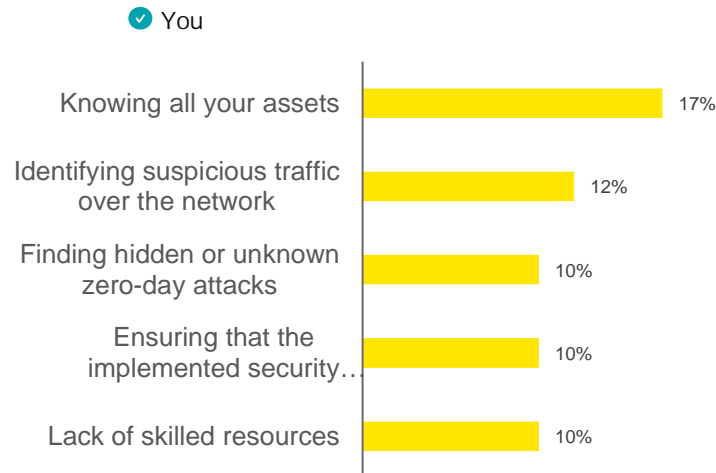
60% say that careless/unaware employees or outdated information security controls or architecture are the vulnerabilities that have most increased their risk exposure. However, in general there is a limited understanding of what threats new technology involve.


Risk associated with growing use of mobile devices



 Your answer: Loss of smart device, devices do not have the same software running on them and organized cyber criminals sell hardware with backdoors

Top 5 challenges: Internet of Things



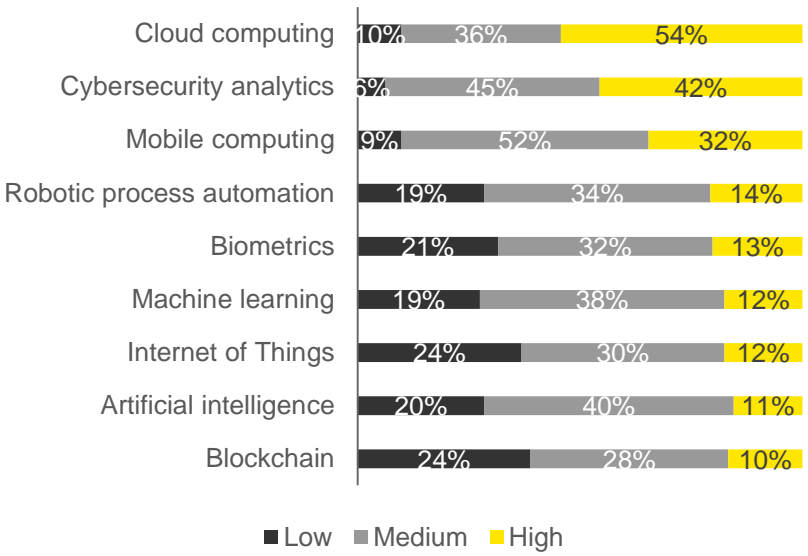
 Your answer: Other

- Organisations in the financial sector feel that their vulnerabilities come mainly from careless or unaware employees and from outdated information security controls or architecture. The same is found in global figures
- Globally, as well as in the financial sector, threat related to the use of smart phones, the Internet of Things and operational technology are not yet well understood. Only 2% of organisations in the financial sector say that the IoT is their highest vulnerability, and 7% say the same for smartphones
- It is important that organisations engage in Digital transformations in order to grow. However, these frequently imply the utilisation of emerging technologies, which security risks are yet not well known to organisations
- Financial services organisations should improve their understanding of how these technologies affect their risk profile, while at the same time also perceive the benefits that these can have for information security

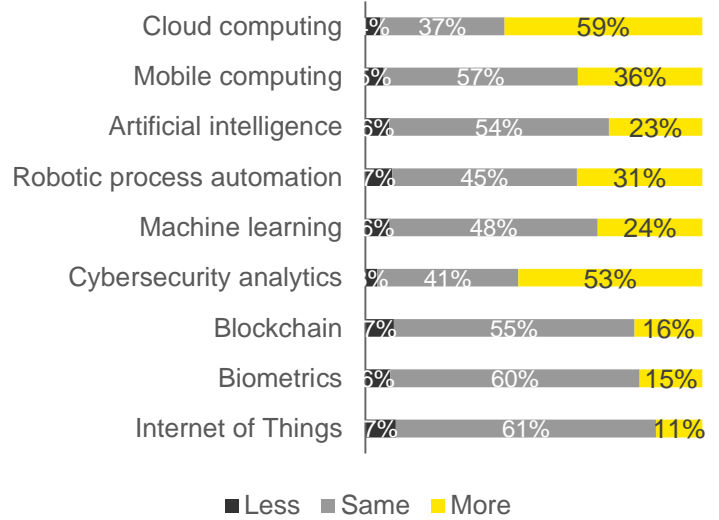
Emerging technologies: How to promote security-by-design and where to prioritise investments from a cybersecurity perspective?

59% are spending more on cloud computing compared to last year, being this the technology which most organisations in the financial sector defines as high for their cybersecurity

Priorities for cybersecurity investments this year




Spending compared to last year



■ Less ■ Same ■ More

- In general, the financial sector is planning to invest the same in new technologies compared to other sectors. When it comes to investment in cybersecurity analytics, the financial sector is investing 5% more than the average globally
- Other technology priorities are cloud, mobile computing and robotics
- As financial services organisations turn to digital opportunities, they must also invest on the cybersecurity side of things. They have to incorporate cybersecurity into the new architectures that they are constructing to take the opportunity to end their legacy systems that were not built around protection and resilience

 This year you are prioritizing investments and spending in Blockchain and Cyber analytics.



Thank you!

