Survey Research - 2017

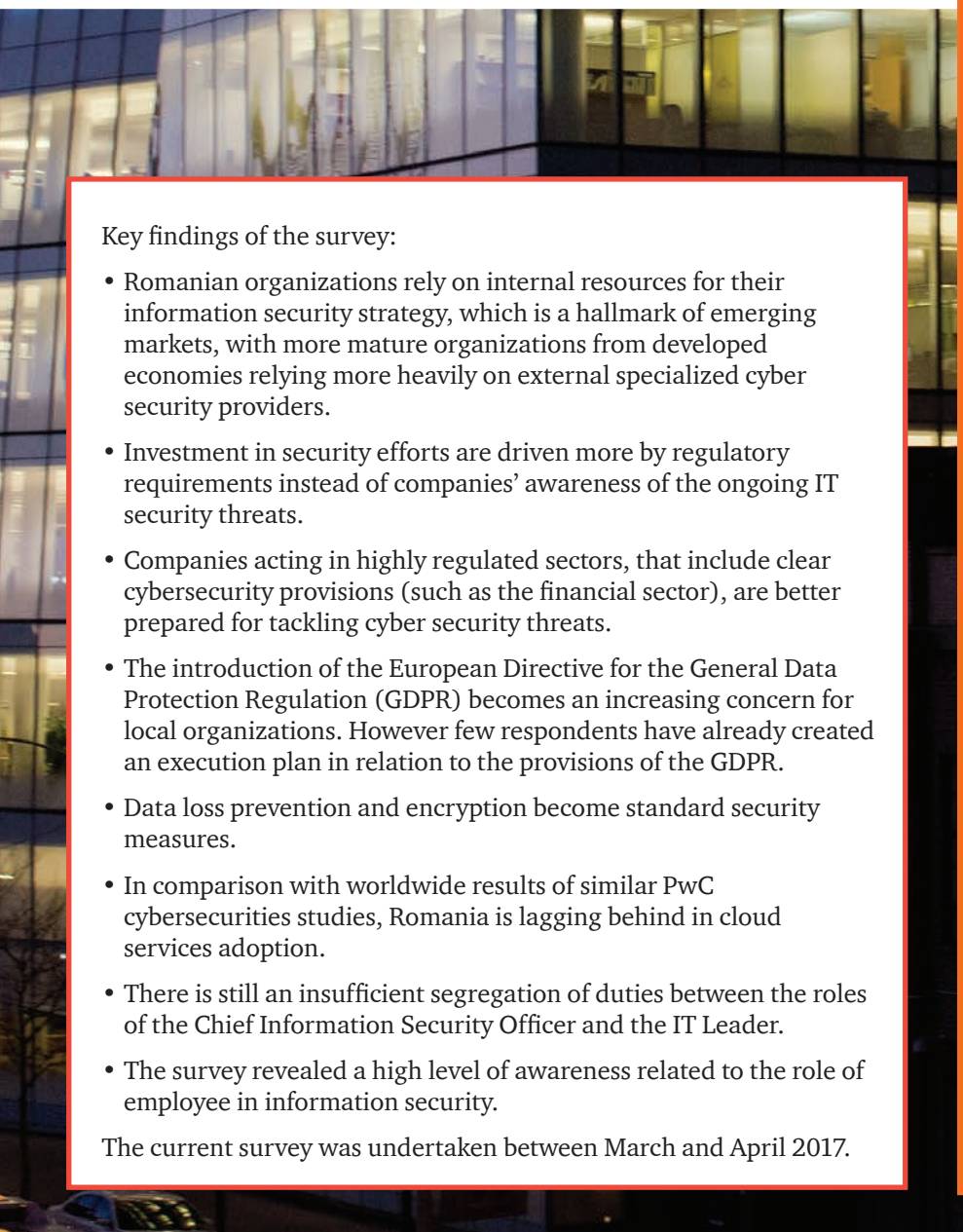
Security Trends

Security in the Digital Age

pwc

Microsoft

Contents



Key findings of the survey:

- Romanian organizations rely on internal resources for their information security strategy, which is a hallmark of emerging markets, with more mature organizations from developed economies relying more heavily on external specialized cyber security providers.
- Investment in security efforts are driven more by regulatory requirements instead of companies' awareness of the ongoing IT security threats.
- Companies acting in highly regulated sectors, that include clear cybersecurity provisions (such as the financial sector), are better prepared for tackling cyber security threats.
- The introduction of the European Directive for the General Data Protection Regulation (GDPR) becomes an increasing concern for local organizations. However few respondents have already created an execution plan in relation to the provisions of the GDPR.
- Data loss prevention and encryption become standard security measures.
- In comparison with worldwide results of similar PwC cybersecurities studies, Romania is lagging behind in cloud services adoption.
- There is still an insufficient segregation of duties between the roles of the Chief Information Security Officer and the IT Leader.
- The survey revealed a high level of awareness related to the role of employee in information security.

The current survey was undertaken between March and April 2017.

Key recommendations for organisations:

- **Have adequately scaled resources (people supported by technology and tested processes) responsible for reporting to an information security officer CISO (chief information security officer). The CISO should report directly to the Board of Directors or to one of the Board Members;**
- **Perform regular security assessments including information security strategy and vulnerability assessments, by using independent external providers;**
- **Invest in employees training and awareness programmes related to information security. It is a critical success factor in every security programs;**
- **Robust business continuity planning and exercising - ensuring that individual user systems and key servers can be restored rapidly from backups, and that the frequency of backups aligns to the timeframe of data your organisation is prepared to lose in the event of any system being rendered unusable;**
- **Crisis and incident response planning and exercising - ensuring that there are formal procedures in which employees and those responsible for the management of high priority incidents are well versed to streamline the organisation's reaction to ransomware events and its ability to restore service to employees and customers;**
- **Strong security hygiene policies and user awareness - preventing ransomware entering your IT environment through the most common delivery vector, phishing, by enforcing strong controls at your email gateways, and developing vigilant employees through robust awareness campaigns;**
- **Rigorous patch and vulnerability management and a robust vulnerability management programme will help reduce the likelihood of exploitation;**
- **A close assessment of the cloud computing services should be undertaken to identify the benefits of cloud services for security, privacy and compliance.**

Introduction

In a business world that is more and more reliant on digital technology, and where data has become the backbone of innovation, the way we safeguard our information systems is vital for the organization as a whole, and an issue that should be on the agenda of all departments within a company, including the CEOs'. This survey, undertaken by PwC and Microsoft, highlights the current situation and the challenges the Romanian companies are facing in terms of ensuring their cybersecurity.

The data was collected in March and April and the study was in the phase of layout finetuning when the WannaCrypt occurred. It was not just a simple coincidence that our companies were preparing this study. It was actually an attempt to signal the importance of cybersecurity with factual data, an approach we considered more prone to being taken seriously by higher management up to the level of CEO. The recent ransomware attack has proven this to a scale we did not anticipate though.

Putting aside its statistical relevance, the survey represents and in-depth evaluation of the current state of affairs in this domain and includes the answers of some of the most prestigious companies active on the Romanian market, from several industrial sectors.

What are the key findings of this survey?

First, there is the striking insight that 40% of Romanian companies do not have any strategy for ensuring their cybersecurity, while 7% don't even see the need to create one. That is quite alarming. Yet we suspect this may have changed now versus March and April, when we collected the data.

In the same time, a huge majority of participants are focusing their cybersecurity efforts on educating their employees in order to identify and tackle the cyber threats as well as on securing the board support to allocate resources and attention to these issues.

Taking into consideration that information technology is no longer the exclusive domain of the IT departments, that there are whole industries that rely on technology to secure their growth and transformation, specialization becomes an imperative, and complex issues such as cybersecurity cannot be managed just by the IT departments, but require a whole new specialized function within any organization. Still, the survey finds that there are plenty of Romanian companies that do not have such a specialized business function.

Yet, it is possible that, with the coming into force of the new EU Directive for personal data protection (the now famous GDPR), in May 2018, some of these companies, in their compliance process, may want to rethink their whole approach to ensuring cyber security. In fact, most of our respondents have stated that they are concerned about the impact that this EU legislation will have on their companies.

Generally speaking, the law does not precede the need, but rather comes as a response to a particular problem that individuals, companies or the states face. As such, this EU Directive tries to tackle the cybersecurity issues through more strict regulations. Looked through this perspectives, the GPDR Directive comes to fill a gap in the current data protection practices.

As business partners of companies from various economic sectors and different sizes, we can confirm that cybersecurity can no longer be a "luxury good" of the largest companies. Moreover, the recent attacks have provided a painful proof. Large or small, companies need to concern themselves with how they protect the security of their most important assets – their data.

We live in a world where technology is present at every step of the way. And we all feel its presence. It is natural to want to feel secure and protected in this journey, we as individuals, as well as our companies. And technology does have solutions to answer to this need. The way we put technology to work for us in making our lives and our companies safer should be on top of our priorities.

Ionuț Simion
Country Managing Partner
PwC Romania

Gabriela Matei
General Manager
Microsoft Romania

Challenges associated with the protection of infrastructure

More than 70% of respondents considered the following factors as an **Important** or **Very Important** challenge for digital security:

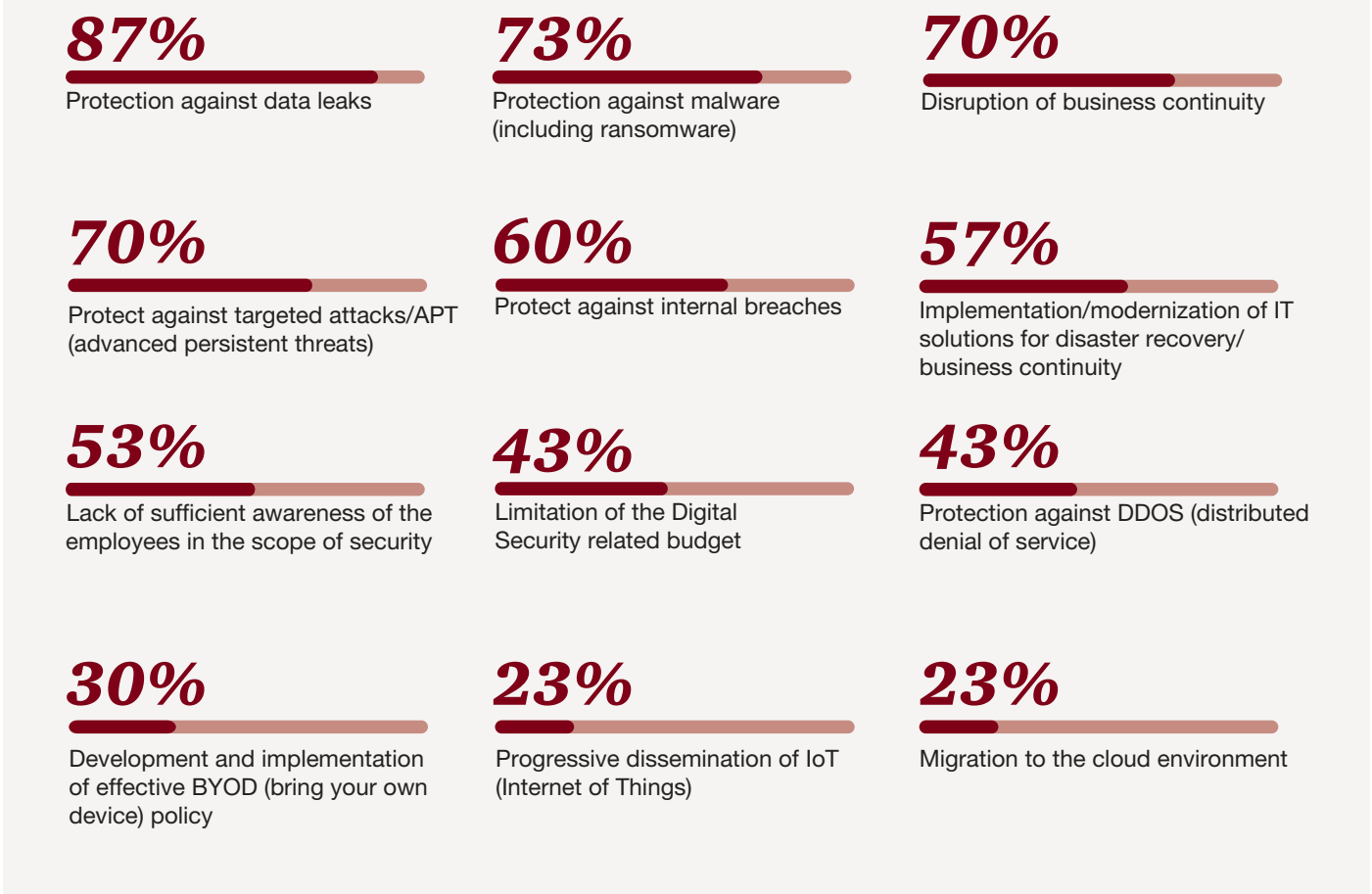
- Protection against data leaks
- Protection against malware (including ransomware)
- Disruption of business continuity
- Protection against targeted attacks/ APT (advanced persistent threats)

Approximately a quarter of respondents considered the followings factors as an **Important** or **Very Important** challenge for digital security:

- Progressive dissemination of IoT (Internet of Things)
- Development and implementation of effective BYOD (bring your own device) policy
- Migration to the cloud environment

Besides the traditional challenges of protecting against data leaks or internal breaches, keeping the infrastructure running and the employees security aware, while managing a limited security budget, the respondents have new challenges like protecting against new types of malware (ransomware) and targeted attacks. The arrival of IoT, cloud migration or BYOD policy are considered challenges by only a smaller fraction of respondents.

Which of the following factors currently constitutes the biggest challenge for digital security in your organization?



Almost 80% of respondents considered that increasing awareness (including training) of the employees regarding threats combined with increasing awareness and support of the management board are critical factors to improve digital security.

Almost 75% of respondents considered the following factors as **Important** or **Very Important** to improve digital security:

- Enforcement of regulatory requirements in the area of digital security
- Comprehensive migration to newer, safer software versions (this applies to server software, business applications, customers)
- Development of comprehensive strategy for managing cybersecurity
- Putting greater emphasis on early detection of threats

More than two thirds of respondents considered hiring additional employees in the area of digital security also an **Important** or **Very Important** factor to improve digital security.

Surprisingly, only half of respondents considered increasing the security budget a way to improve digital security. This may reflect the experience of managing security on shoestring budgets.

Less than 25% of respondents considered the followings factors as **Important** or **Very Important** to improve digital security:

- Entrusting security management to the external provider
- Transition to cloud computing
- Possibility of outsourcing the selected processes related to digital security

What are CSOs counting on

83%
Increasing awareness (including training) of the employees regarding threats

80%
Increasing awareness and support of the management board in the scope of digital security

77%
Enforcement of regulatory requirements in the area of digital security

73%
Comprehensive migration to newer, safer software versions (this applies to server software, business applications, customers)

73%
Putting greater emphasis on early detection of threats

73%
Development of comprehensive strategy for managing cybersecurity

67%
Hiring additional employees in the area of digital security

57%
Exchange of security information with other entities in the sector or industry

47%
Increasing digital security related budget

53%
Avoid using unauthorized cloud computing solutions

43%
New model of security management

43%
Possibility of more frequent use of the support of external companies that provide specialized services in the area of digital security

23%
Entrusting security management to the external provider

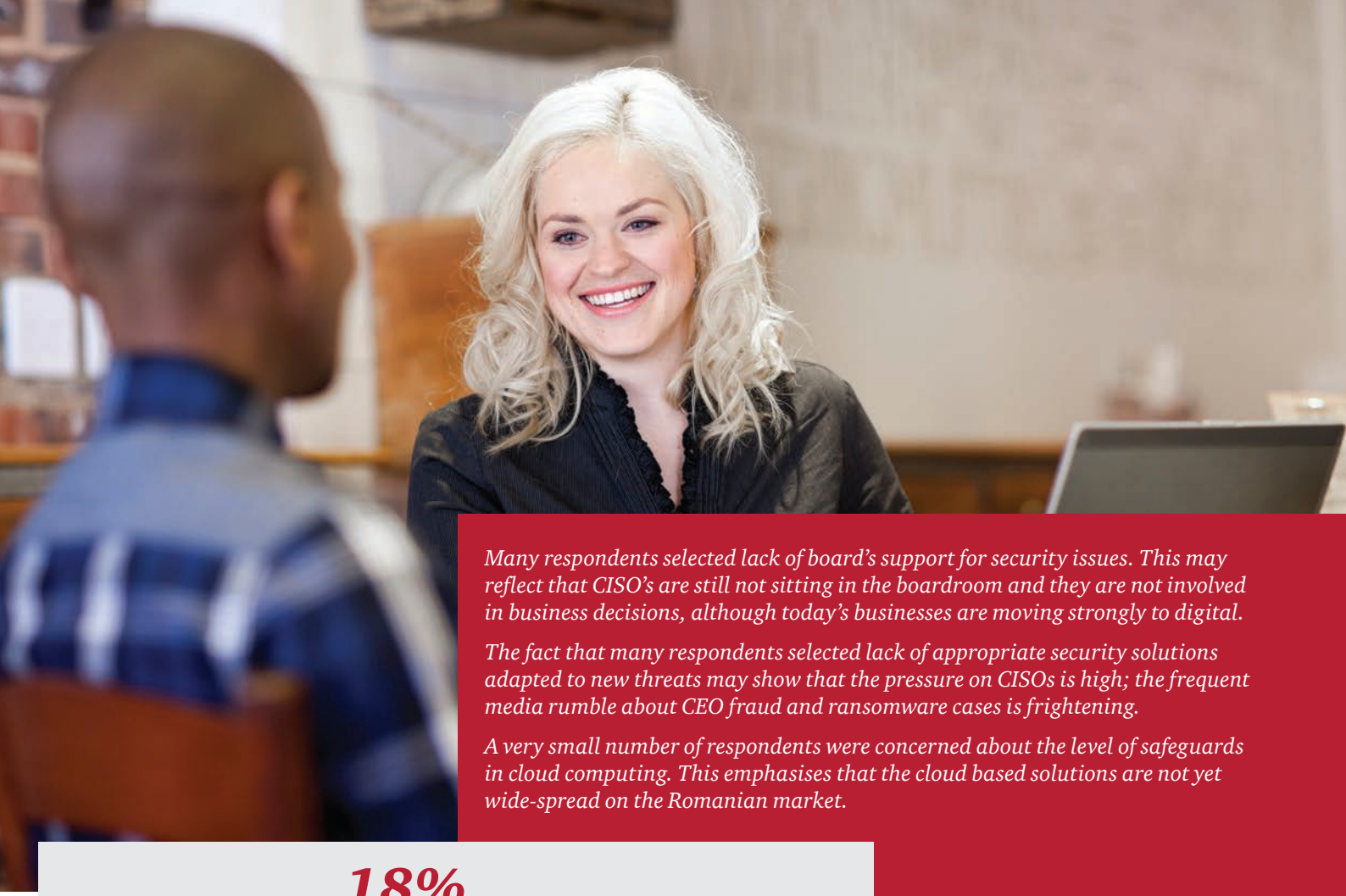
20%
Transition to cloud computing

20%
Possibility of outsourcing the selected processes related to digital security

Vast majority of respondents considered the enforcement of regulatory requirements a major driver to improve digital security. This may reflect the compliance requirements they are faced with.

The need to hire additional security staff and to exchange security information with others were also considered by the large majority of respondents very important to improve digital security. This may reflect the current understaffed state of security in most of organizations and the hope that the experience of others may help.

Outsourcing security processes or utilization of cloud computing to improve digital security were also not very popular choices. This may reflect the insufficient awareness of local CISOs about the advantages of cloud services.



Many respondents selected lack of board's support for security issues. This may reflect that CISO's are still not sitting in the boardroom and they are not involved in business decisions, although today's businesses are moving strongly to digital.

The fact that many respondents selected lack of appropriate security solutions adapted to new threats may show that the pressure on CISOs is high; the frequent media rumble about CEO fraud and ransomware cases is frightening.

A very small number of respondents were concerned about the level of safeguards in cloud computing. This emphasises that the cloud based solutions are not yet wide-spread on the Romanian market.

The eleven fears of a CSO

18%
End users who do not follow security rules

13%
Lack of appropriate security solutions adapted to new threats

12%
Lack of awareness and support from the management board for actions in the area of digital security

10%
Lack of awareness regarding the threats from the side of business divisions

10%
Lack of the possibility to effectively identify security breaches

8%
Lack of coherent strategy of action in the area of digital security

9%
Mobile devices and lack of appropriate safeguards

7%
Gaps in the security of digital solutions used

5%
Insufficient protection of test and development environments

6%
End users who use social media carelessly

2%
Lack of appropriate level of safeguards in the cloud computing

The most sensitive points in current data protection systems:

- End users who do not follow security rules;
- Lack of appropriate security solutions adapted to new threats;
- Lack of awareness and support from the management board for actions in the area of digital security.

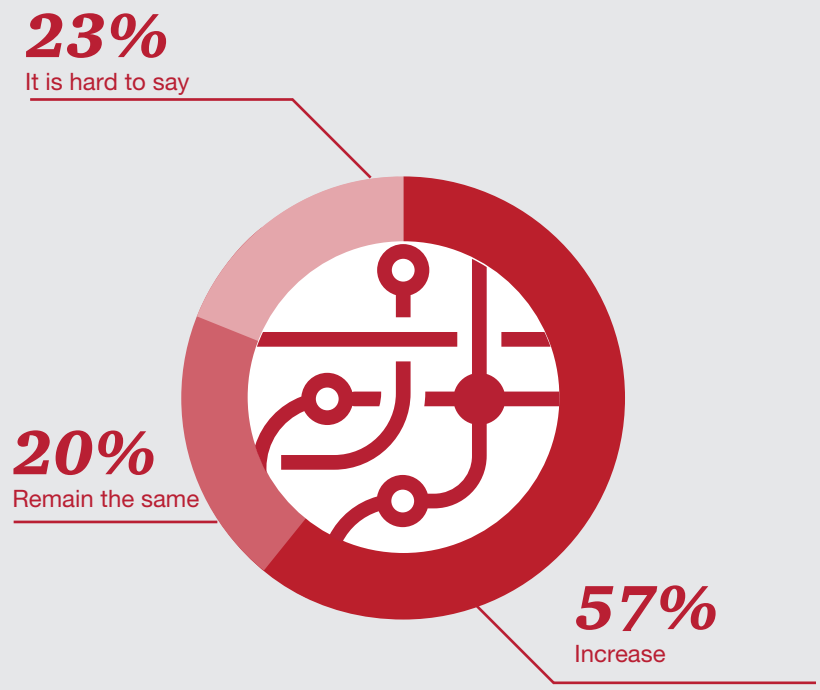
Bottom three least sensitive points in current data protection systems:

- End users who use social media carelessly;
- Insufficient protection of test and development environments;
- Lack of appropriate level of safeguards in the cloud computing.

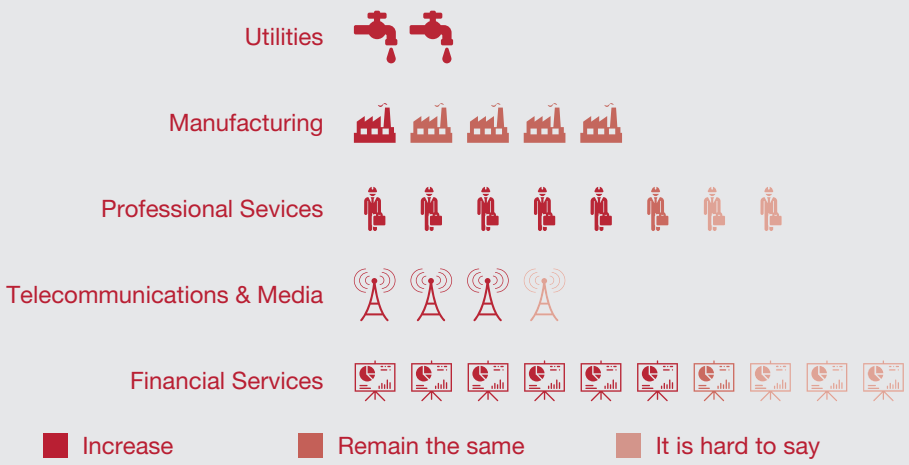
Almost two thirds of respondents think that their organization's expenditure related to digital security will increase in the next 12 months. This may be related to the overall positive business outlook of the country, with Romanian being the fastest growing economy in Europe.

On the other hand, the analysis of the expenditure per business verticals shows that, even in the financial services area, 30% of respondents were not sure about the future outlook of the expenditure on digital security.

In the next 12 months, your organisation's expenditure related to digital security, will:



Expenditure on digital security per business verticals



Management of security

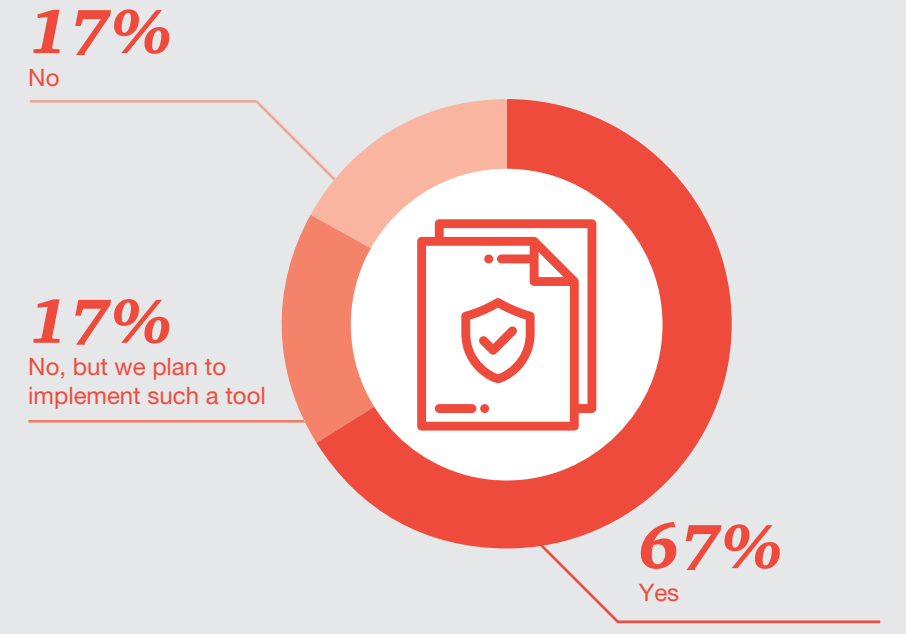
Most of respondents would invest in data backup / recovery process, improving access management to systems and data leak prevention solutions. This may show that respondents prefer to invest in areas that have a quick and major impact on their security risk posture, access and data protection.

Only few of the respondents would invest in security monitoring & incident response technologies or mobile device management solutions. This is likely due to the fact that respondents are still willing to invest based on an old fashion pattern.

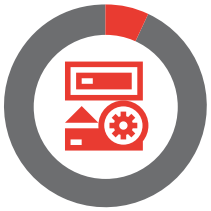
More than two thirds of respondents use a Data Loss Prevention (DLP) solution and this points out that DLP became a common security measure, similar with antivirus solutions.

On the other hand, almost one fifth of respondents are not using a DLP solution. A possible explanation may be the lack of an information classification policy.

Does your organization use tools to protect against data leaks (DLP – data loss prevention)?



Which investments from the area of digital security are prioritized in your company?



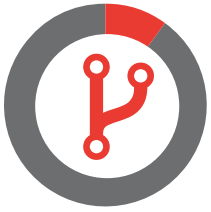
20%
Improving the backup and data recovery process

19%
Managing access to systems

16%
Implementation of the solutions that prevent data leaks

13%
Implementation of advanced tools for detecting malware

11%
Implementation of a program to raise awareness regarding security threats

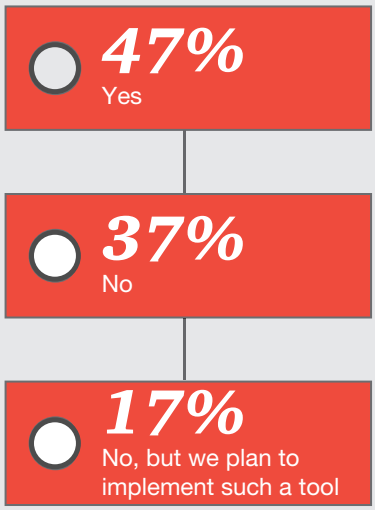


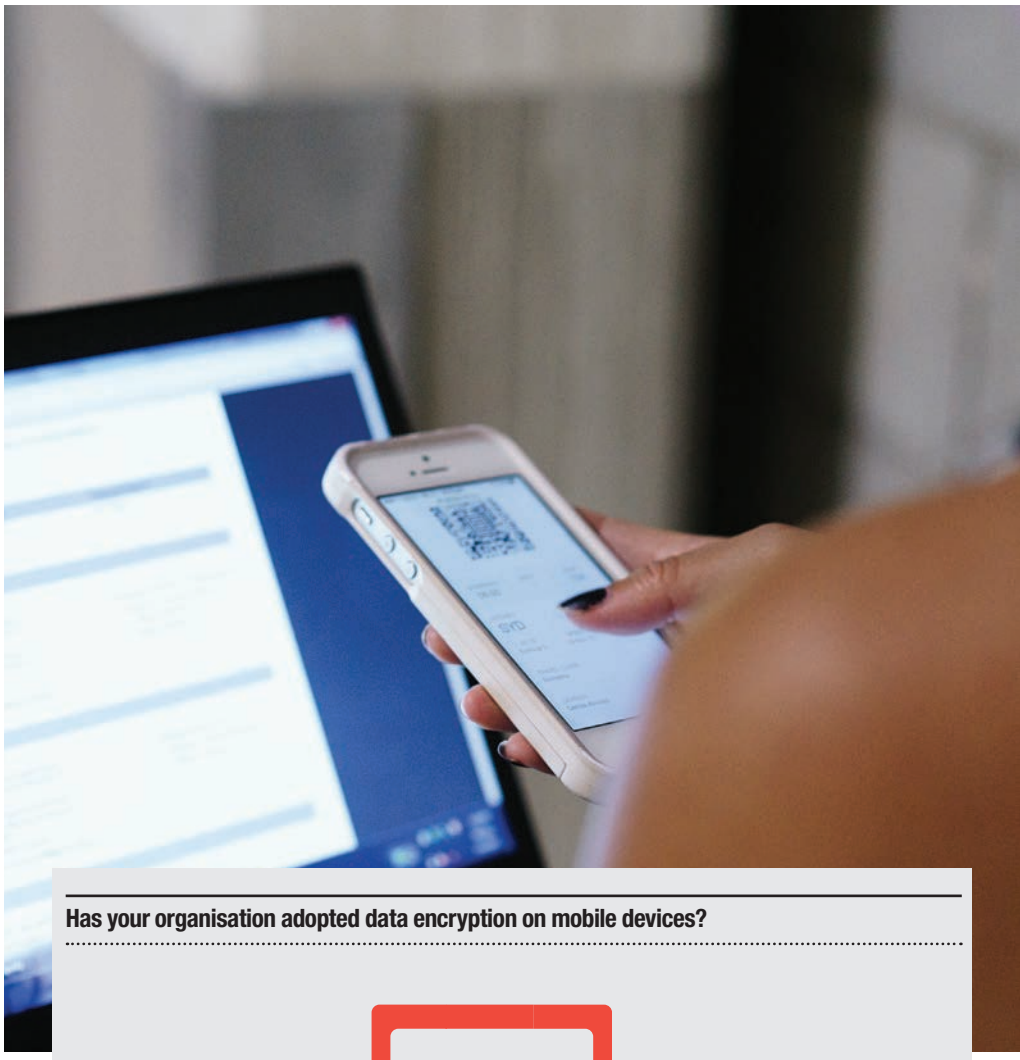
11%
Reorganisation of the processes of security monitoring and responding to incidents associated with security

9%
Implementation/ medernization of the tools that automate the management of mobile devices

Almost two thirds of respondents have implemented or are planning to implement solutions to manage access across the entire ecosystem (Identity and Access Management solution). This pinpoints that IAM began to show its value for organizations and more implementations are expected.

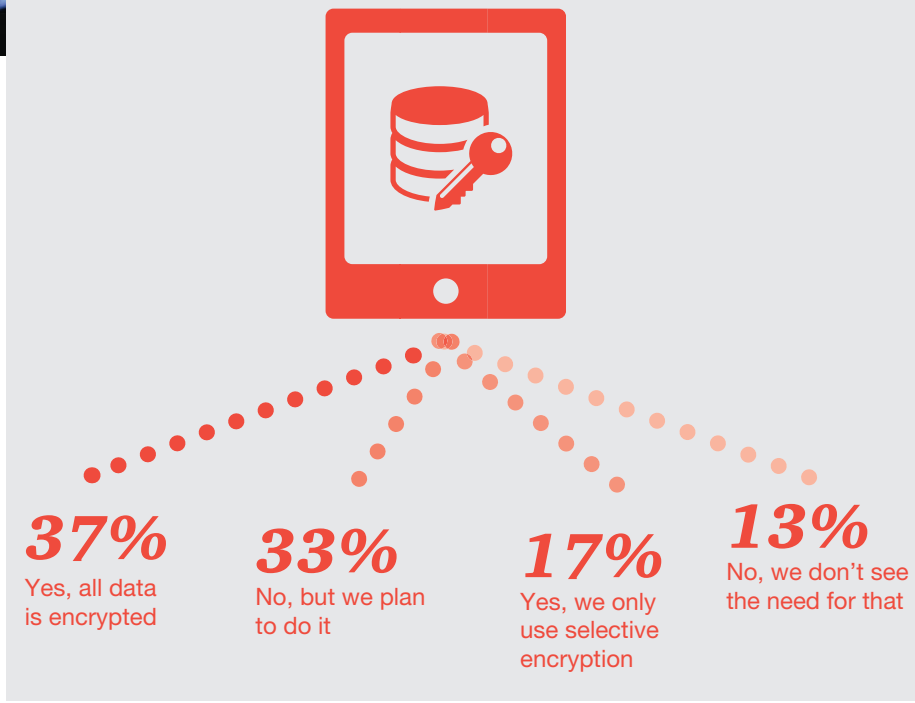
Does the organisation include a team dedicated to respond to security incidents?





More than one third of respondents have implemented full data encryption for mobile devices, while 33% of respondents are planning to implement this protection measure. This shows that organizations began to realize that data should be protected also on the mobile devices, which are the new security perimeter of the ITC infrastructure.

Has your organisation adopted data encryption on mobile devices?



Almost two thirds of respondents have a dedicated incident response team and none of the respondents are using an external provider for this task. This may indicate several thing:

- That organizations are satisfied with the results of their internal incident response teams;
- That they do not trust external providers of this service;
- Or that they do not know the existing offers for Managed Security Services.

On the other hand, one third of the surveyed organizations do not have a dedicated security incident response team and this is rather surprising.

All respondents considered the following factors as an **Important** or **Very Important** criteria when choosing an IT solution:

When choosing IT solutions, the organisation focuses on:

93%
Quality of service

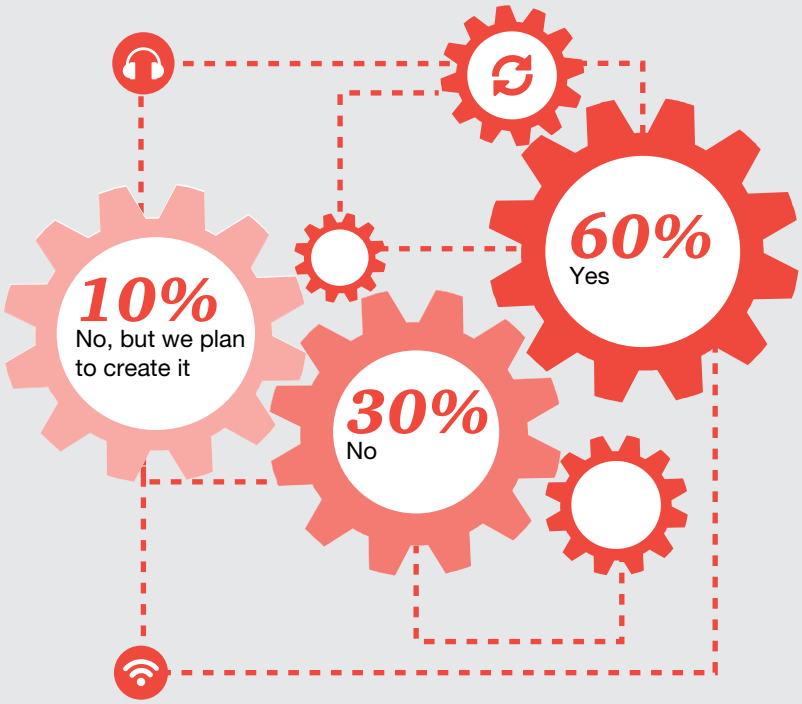
83%
Security of offered solutions

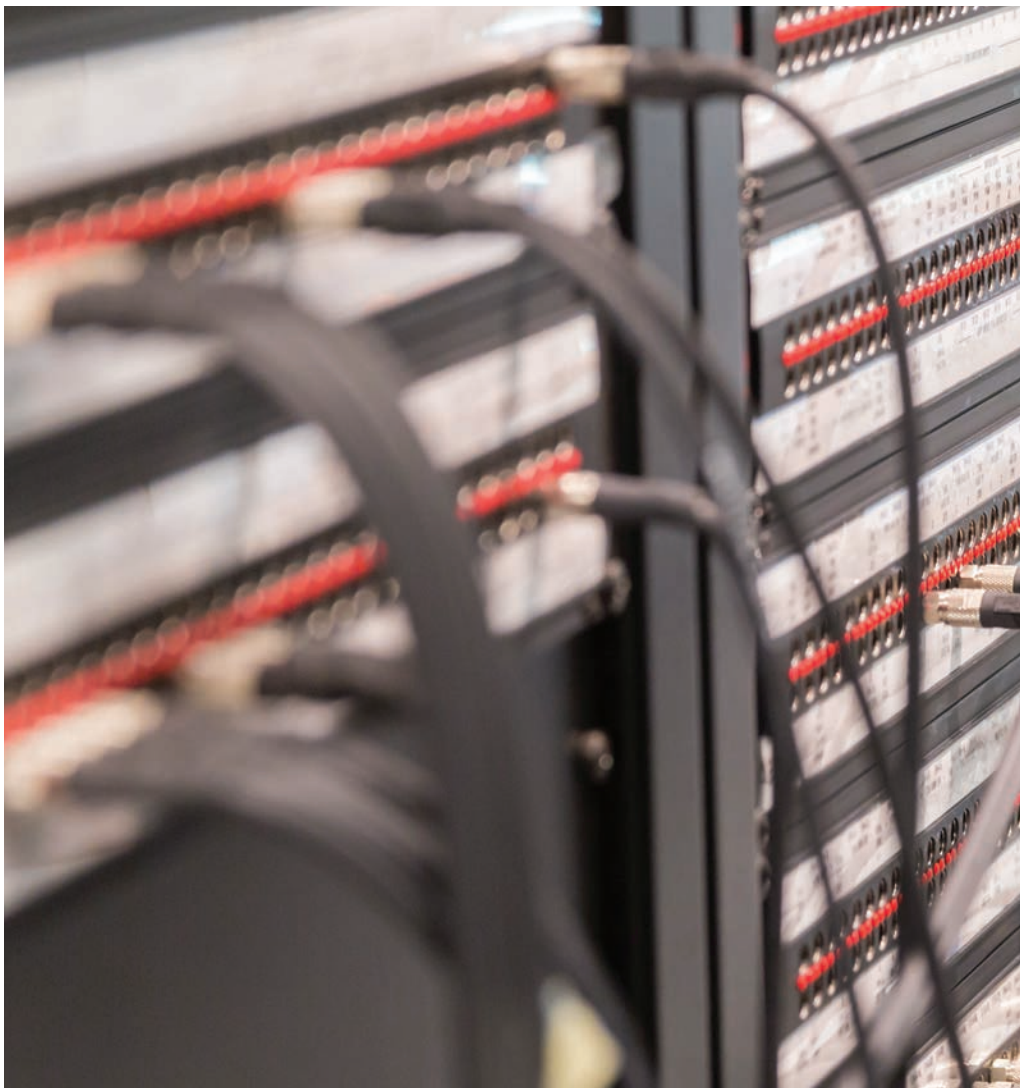
77%
Reputation of the provider - a provider that we have already worked with or that has a good reference

73%
Price-quality ratio

57%
Regular software upgrades

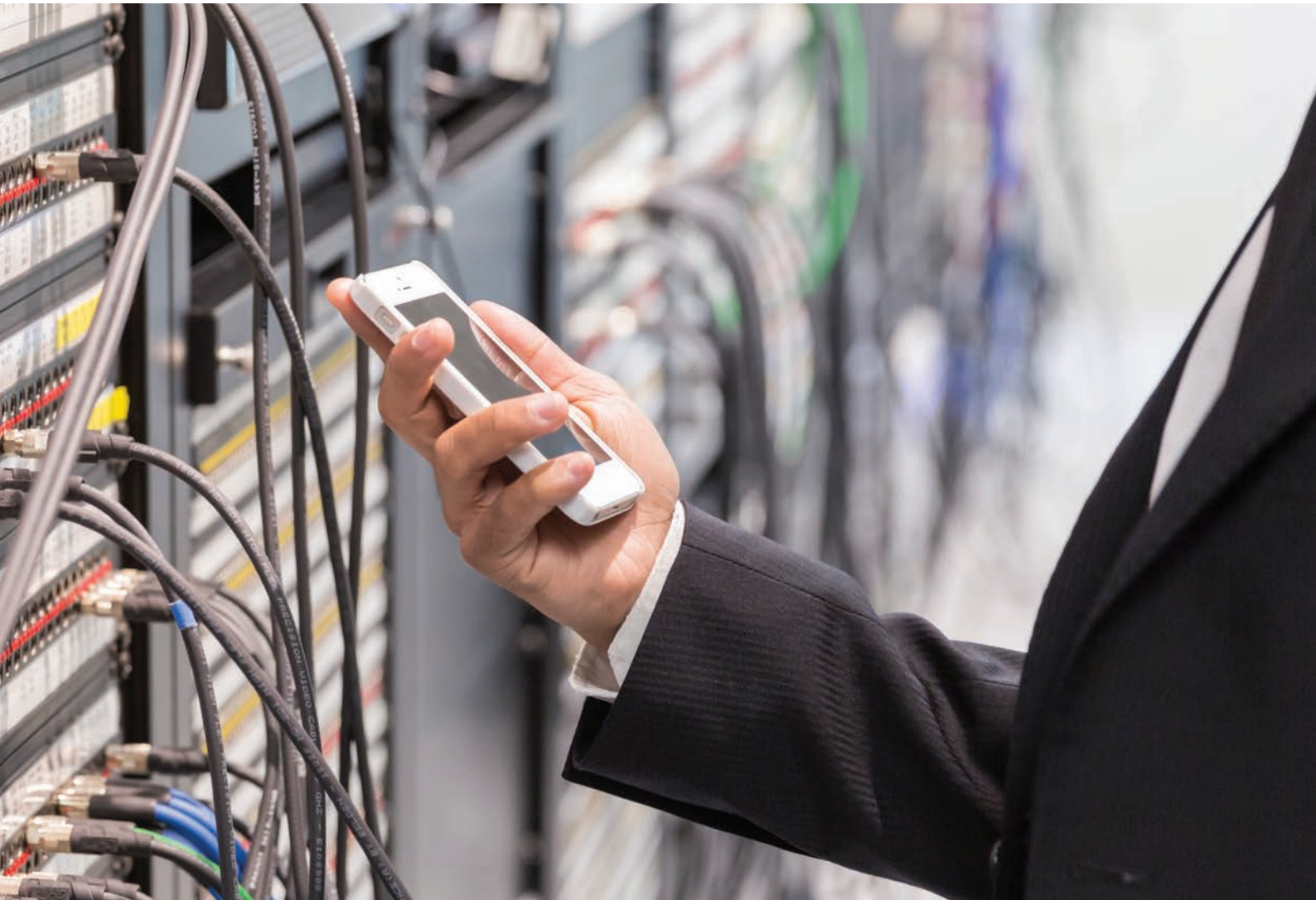
Does the organisation include a team dedicated to respond to security incidents?





We noted that security of the offered solution is almost as important as the quality of the provided services. Also, the reputation of the provider is followed closely by the price-quality ratio. This may show that security became an important factor, compared to the regular selection criteria.

More than half of respondents use a centralized solution that enforces security policies on mobile devices, while almost a quarter of respondents plan to implement such a solution. This indicates that Mobile Device Management (MDM) became a standard security measure, similar with the antivirus.



13% of respondents do not allow employees to use their own mobile devices in the company, while over one third of respondents have a Bring Your Own Device security policy or intend to implement one.

Is there a security policy that specifies the rules for employees regarding the use of their own mobile devices in the company?

37%
Yes, there is

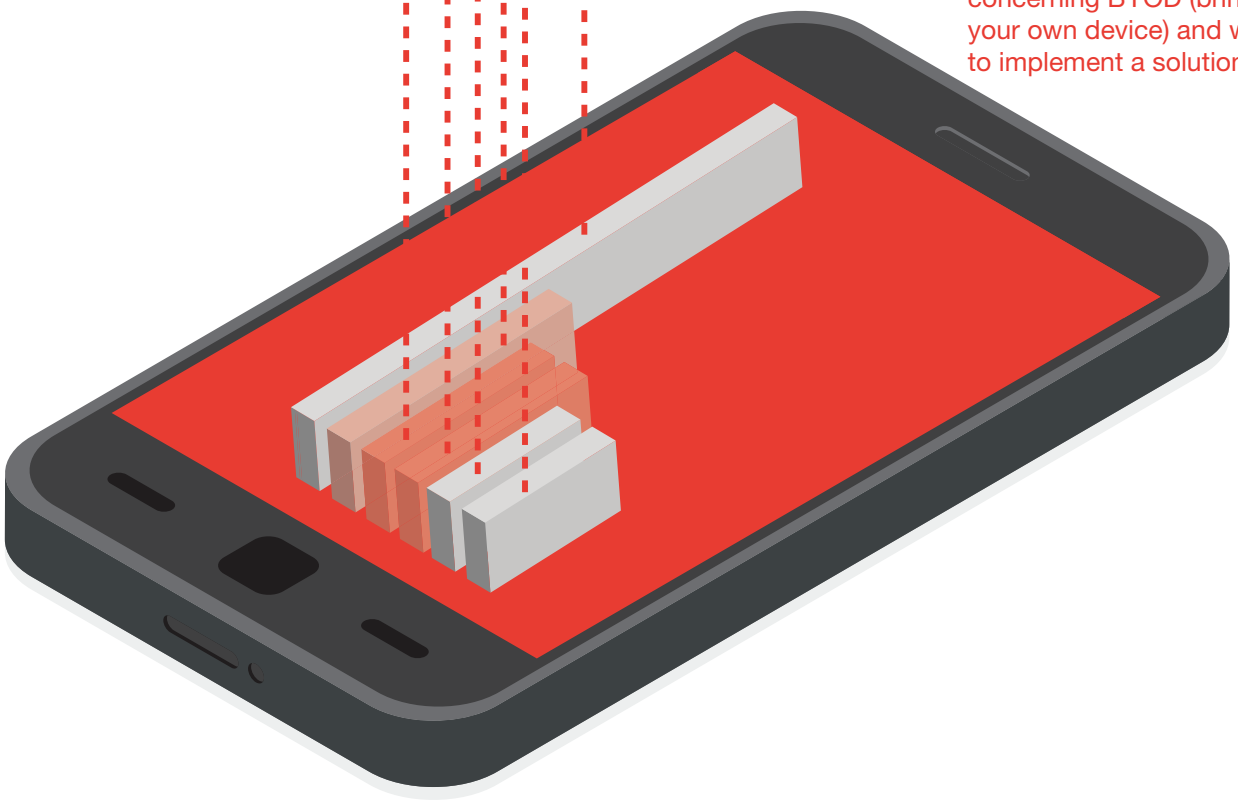
17%
No, but we plan to implement such a policy within the next year

13%
Employees cannot use their own mobile devices in the company

13%
No, these has not been necessary to date

10%
No, but wa have standards and procedures

10%
There is an outline of rules concerning BYOD (bring your own device) and we plan to implement a solution



More than two thirds of respondents assess security vulnerabilities periodically and most of them use external penetration testing providers. Almost 40% of the respondents use internal penetration testing teams. Only 30% of respondents use automated solutions for vulnerability assessments and only 17% executes code review with an external provider.

How does your organization assess security vulnerabilities?

67%
Vulnerability assessment carried out periodically

60%
Penetration tests carried out by an external company

40%
Penetration tests carried out by an internal team

30%
Automated solutions

17%
Code review carried out by an external company

17%
Code review carried out by an internal team

10%
We do not assess it

Trends associated with the protection of infrastructure

Respondents' approach to cloud computing is cautious and the use of public cloud services is reduced:

- 21% do not anticipate **any** cloud project implementations;
- 26% use some **public** cloud services;
- 26% already implemented solutions based on **private** cloud;
- 9% plan to migrate certain systems to the **private** cloud;
- 7% plan to migrate certain systems to the **public** cloud.

However, the large number of participants in GSISS survey form North America and from Asia Pacific are well known as early cloud adopters.

How does your organization approach cloud computing?

26%
We use some services available in the public cloud

26%
We hve already impemented solutions based on private cloud

21%
Currently, we do not anticipate implementation of any cloud projects

12%
We have already implemented solutions based on hybrid cloud

9%
We plan to migrate certain parts of systems to the private cloud

7%
We plan to migrate certain parts of systems to the public cloud

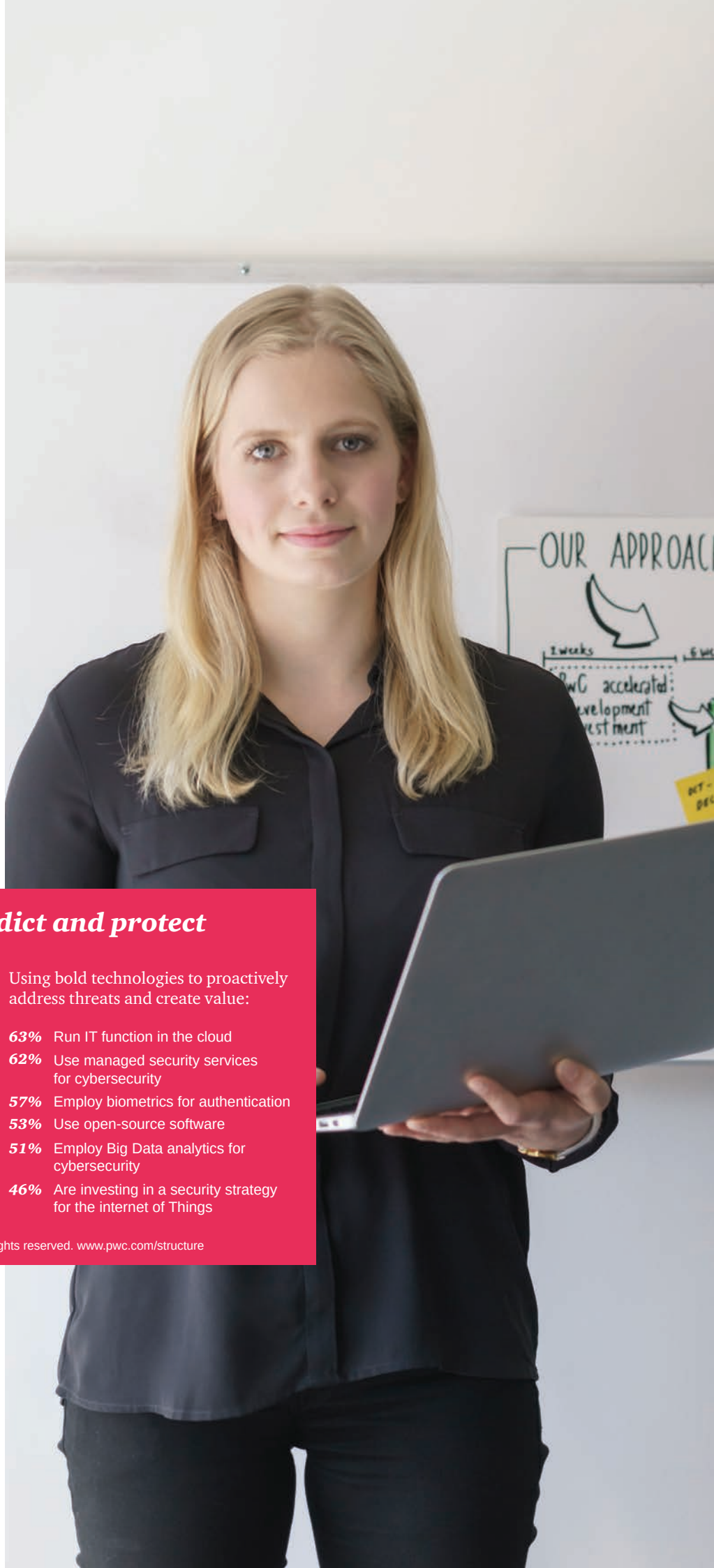
22%

Respondents' trust in cloud providers' ability to protect data is also reduced:

- 40% of respondents believe that the organization is able to protect data more effectively than cloud providers;
- 43% of respondents believe that cloud providers are able to protect data more effectively than the organization;
- 13% of respondents have no idea about the security mechanisms offered by cloud providers.

This finding is not aligned with findings of GSISS 2017 and cloud providers should promote better their responses to the "CSA Consensus Assessments Initiative Questionnaire" and security certifications on the Romanian market.

In contrast, GSISS 2017 found that 62% of respondents are using Managed Security Services for cybersecurity.



New possibilities to predict and protect

62%
Use managed security services for cybersecurity

Using bold technologies to proactively address threats and create value:

- ***63%*** Run IT function in the cloud
- ***62%*** Use managed security services for cybersecurity
- ***57%*** Employ biometrics for authentication
- ***53%*** Use open-source software
- ***51%*** Employ Big Data analytics for cybersecurity
- ***46%*** Are investing in a security strategy for the internet of Things

According to half of respondents, the main advantages of cloud solutions are their cost-effective implementation of backup and disaster recovery solutions and shifting the costs of infrastructure operations – including security - to the cloud service provider. One of the respondents answered that there are *"Only costs benefits so far, doubts with regards to security and data protection".*

In contrast GSISS 2017 identified powerful synergies in the cloud based approach to cybersecurity:

"Cloud-based cybersecurity not only helps deter intruders but it also monitors those who do get in—including legitimate employees, third-party partners and customers—to learn from their behavior. When cloud-based cybersecurity is integrated with functions like marketing, customer service and logistics, the system can track activities of everyone who interacts with their business ecosystem. This enables businesses to assess customer behavior and ultimately improve the experience."

39% of respondents considered that the perceived lack of control over the processing and security of data moved in the public cloud is the main obstacle to wider market adoption of public cloud services.

This finding is not aligned with findings of GSISS 2017 and cloud providers should promote better their responses to the "CSA Consensus Assessments Initiative Questionnaire" and security certifications on the Romanian market, together with their data security and operational procedures.

A quarter of respondents agreed that the concerns about the availability of data is another obstacle. This concern was enforced by the recent availability incidents of two major cloud service providers.

The issue of compliance with laws and industry regulations was the third factor considered an obstacle.

Over two thirds of respondents considered that the awareness of threats has increased in the business divisions. We hope this trend will continue further.

On the other hand, only 19% of respondents confirmed that security is a topic in the reports to management board.

The good news is that only 7% of respondents considered that business still perceives security as an obstacle.

What are the advantages of using cloud solutions?

35%
Cost-effective implementation of back-up data centers and disaster recovery solutions

23%
Shifting the costs of infrastructrure security to the service provider

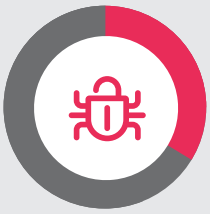
18%
Greater resistance of the cloud infrastructure to load spikes

13%
Easier management of the virtualized environment

8%
Higher resistance of the cloud to failures

2%
Other

Which factors in your opinion constitute an obstacle to wider market adoption of the public cloud services?



39%
Belief that there is a lack of control over the processing and security of data

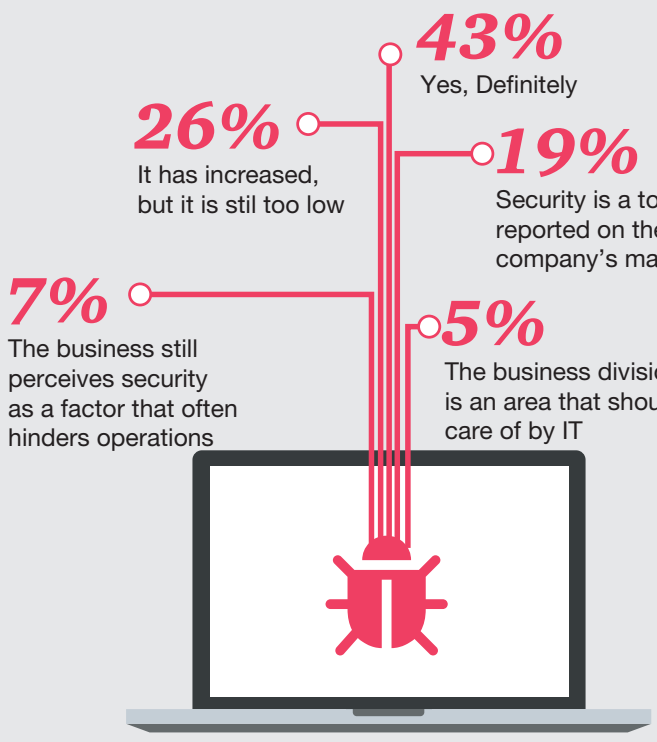
23%
Concerns about the availability of data, when it is needed

22%
Issue of compliance with laws and industry regulations

8%
Lack of trust in regard to the potential provider

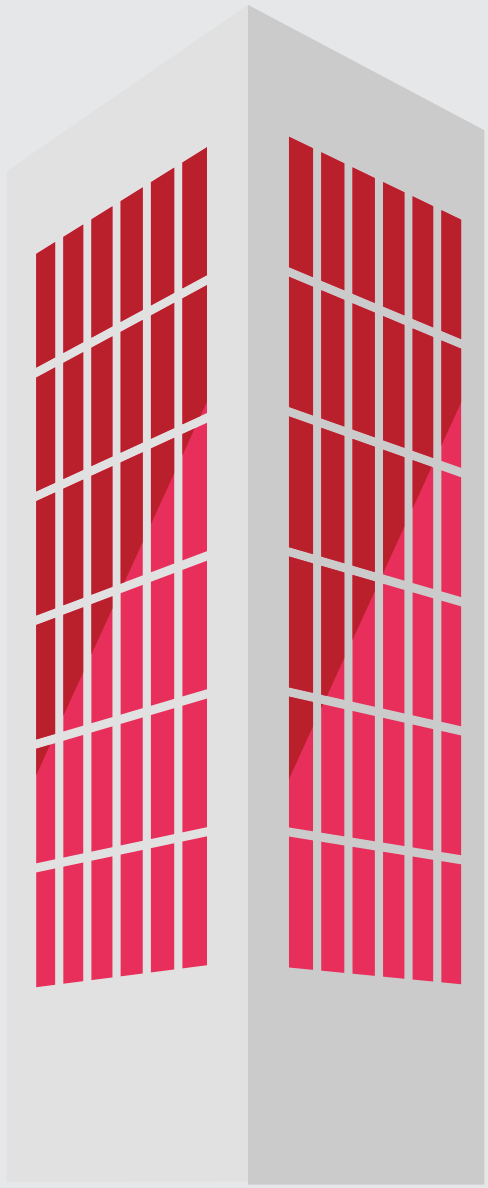
8%
Other

Has the awareness of threats increased in business divisions of your company over the last year?



Cyber security strategies

Does your organisation have a formally approved strategy for cyber security?



33%
We plan to create such a strategy

30%
Yes, such a strategy has been defined

20%
Yes, such a strategy has been defined and implemented

10%
Yes, such a strategy has been defined, implemented and optimised

7%
The company has no such strategy and it has no plans to create it

All respondents are concerned about cyber security strategy, but only few of them have implemented it.

More than half of the respondents have a formally **defined** cyber security strategy and almost 20% of them have implemented the strategy. Another one third of respondents plan to create a cyber security strategy.

On the other hand, only 10% of respondents reported that their strategy is not just implemented, but is also optimized. This may show that the cyber security initiatives are relatively new or that the participating organizations do not optimize their strategy to respond better to business requirements and evolving threats.

43% of the respondents have developed their cyber security strategy without external support. 30% of respondents used support from an external provider to develop the strategy.

Almost two thirds of the respondents have their cyber security strategy constantly aligned with the business strategy. Only 10% have their cyber security strategy developed independently from the business strategy, while a quarter of respondents declared they do not have a formal business strategy.

Almost two thirds of respondents have their security management process **compliant** with a relevant standard, while 23% of respondents have also certified it. A surprisingly high number of 23% of respondents considered compliance with a relevant security management standard is not needed.

The value of a security management process compliant with a relevant standard lays in the possibility to periodically conducting audits against the requirements of the standard, and constantly improving the security management process.

As expected, the most implemented management frameworks are ISO 9001 and ISO 27001. COBIT was reported as "Other" by 10% and ITIL had the same score. Only 5% of respondents have implemented ISO 22301 business continuity framework.

Most of the respondents participate in cooperation initiatives at sector level and share their experience to improve cybersecurity posture. Another popular method reported was the participation in conferences and meetings.

Only 16% of respondents participate in cross sector initiatives and this is a surprisingly small number. Today, when suppliers' and partners' security have the same importance as the organization's own security, participation in cross-sector security initiatives like National Computer Incident Response Center (CERT-RO), Romanian Association for Information Security Assurance (RAISA) and others is highly recommended.

Was the cyber security strategy created with the support of an external company?

43% No

30% We do not have such a strategy

27% Yes

Is your organization's cyber security strategy aligned with the business strategy?

63% Yes, it's constantly updated in cooperation with the business

10% No, it's developed independently

27% No, we don't have a formal business strategy

Does your organization participate in cooperation initiatives aimed to exchange experiences and to increase cybersecurity?

36% Yes, in sector initiatives

33% Yes, in conferences, meetings, discussions

16% Yes, in cross-sector initiatives

7% Only when state authotities require

7% No, never, security is an internal matter of the company

2% No, we dont't have time for this

What management frameworks have been implemented in the company?

31% ISO 9001

29% ISO 27001

14% None has been implemented so far

10% ITIL

10% Other (COBIT, CisSecOrg, Regulator)

5% ISO 22301

2% ISO 31000

Is the security management process compliant with a relevant standard?

40% Compliant, but not certified

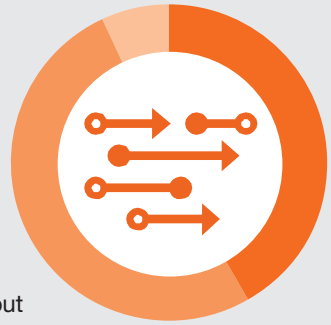
23% No, there's no such need

23% Compliant and certified

13% No, but we plan to implement this

Compliance strategy in the digital area

Do you have a strategy to achieve compliance with new rules and regulations in the digital area?



7%
Don't know

43%
Yes, dedicated compliance responsibilities are established and regulatory requirements are continously monitored

50%
Strategy not formalized but awarness exist

How concerned are you about the impact on your organization of new regulations such as EU General Data Protection Rules (GDPR)?

10%
Not Concerned

33%
Somewhat concerned

30%
Very Concerned

27%
Concerned

How much do you think the technology can help you with responding to the GDPR requirements?

33%
Technology can help, but it is not essential

67%
Technology is essential to responding to GDPR

43% of respondents have a strategy to achieve compliance with new rules and regulations in digital area. These organizations have established compliance responsibilities and are continuously monitoring regulatory requirements.

Half of respondents are aware about the new regulatory requirements, but do not have a formal strategy to achieve compliance.

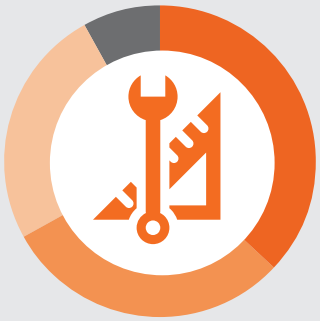
57% of respondents are concerned or very concerned about the EU General Data Protection Rules (GDPR) and another 33% of the respondents are somewhat concerned.

Regarding the role of technology in responding to GDPR requirements, more than half of the respondents considers technology essential, while the rest of respondents considers that technology can help, but is not essential.

The most popular technologies considered useful to ensure GDPR compliance were incident and event monitoring tools, data loss prevention tools and discovery tools.

Most of respondents are aware about all the key five requirements of GDPR. The best known were of course the administrative fines and the key dates for rule applicability, while the least known was the requirement to appoint a Data Protection Officer.

Which technologies do you primarily consider to ensuring GDPR compliance of your organization?



8%
Other tools

37%
Incidents and enets monitoring tools

25%
Discovery tools - to search for personal data

30%
Data loss prevetion tools

Are you aware about the new requirements in the GDPR rule?

83%
Administrative fines

77%
Notification require-ments in case of data breaches

77%
Key dates for rule applicability

63%
Reuirement - security by befault/design

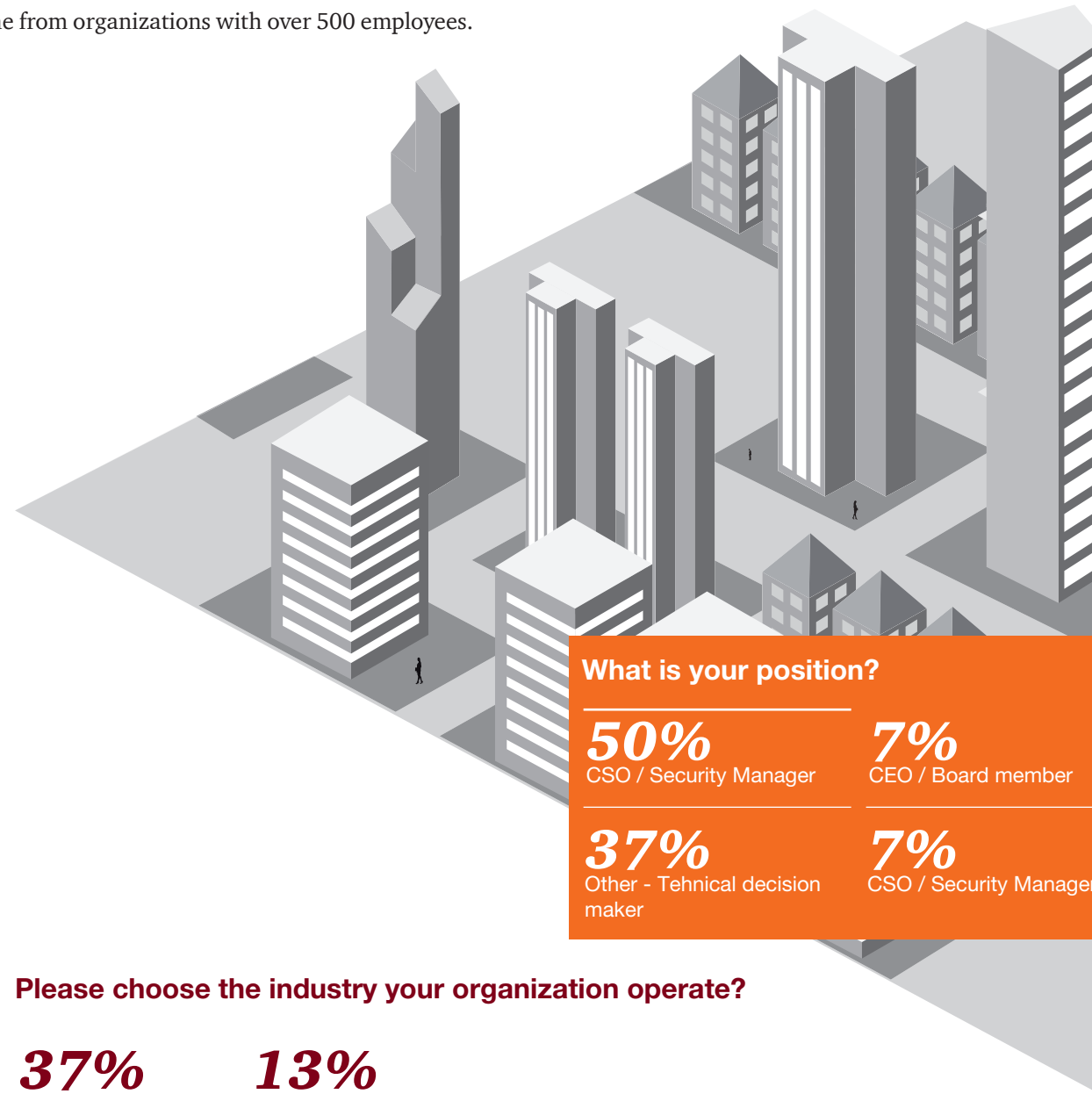
60%
Ise your organization required to appoint a data security officer?

About the study

The results discussed in this report are based on responses of 30 organizations. The survey was undertaken between March and April 2017.

The results can be used for comparing an organization's security status with the general status of the respondents.

76% of responses came from organizations with over 500 employees.



What is your position?

50% CSO / Security Manager

7% CEO / Board member

37% Other - Tehnical decision maker

7% CSO / Security Manager

Please choose the industry your organization operate?

37% Financial Sector

13% Telecommunications and media

27% Professional Services

7% Utilities

17% Manufacturing

The margin of error is less than 1%; numbers may not add to 100% due to rounding.
All figures and graphics in this report were sourced from survey results.

How big is the organization you represent

53%
over 1000 people

23%
501 - 1000 people

23%
1-500 people