REPORT

Next steps in cyber security

March 2015

Deloitte.

Efma

Contents

Executive summary

Deloitte and EFMA conducted a survey of 80 professionals across the financial services sector, 70 percent directly from banking institutions. 35 percent of respondents work in the IT department of their organisation, 25 percent of respondents being the head of the IT department. As a result of the survey, a series of conclusions was obtained regarding the importance and awareness of cyber security within the company and among its employees, and the way in which the company is addressing new threats.

Cyber security is a global concern for most of the respondents; both intermediate (IT and operation managers) and high-level (CEO), as they have seen the number of cyber attacks increase this year (according to 31 percent of respondents) or at least stayed the same as last year (38 percent).

Despite the global concerns about cyber security, 4 percent of the respondents have stated that there are no elements that make their company vulnerable to cyber risk, with some even saying that their institution doesn't have a specialised and dedicated professional group for the management of cyber security, and so there is no cyber risk management model with safety measures in place.

The traditional security framework should be evolved, committed to addressing new cyber threats, and also prioritising new detection and response capabilities.

It is also notable that 75 percent of respondents are not members of any cyber international security organisation, despite being international entities and acknowledging that cyber security must be addressed internationally.

Some of the respondents (approximately 20 percent) did not provide information regarding the budgeting of cyber security, but those who did provide this information stated that no more than 10 percent of the IT budget is committed to cyber security.

Among respondents, 39 percent report directly to the CEO and a 24 percent report to the executive committee. Furthermore, 9 percent of the respondents report to a cyber security committee.

The majority of the companies have spent more money on preventing cyber attacks than other security tasks such as detection or response and resiliency. Despite the measures taken against the risk elements, it is considered that the most worrying element is the human factor risk.

Most of the awareness campaigns are focused on the IT department (93 percent) but they have also started to be delivered to executive committees (61 percent) and back (49 percent) and front office employees (44 percent). 45 percent of the respondents stated that their CEO's awareness to cyber-risks is medium and should be considered higher.

Such awareness programmes are carried out by traditional tools implemented within companies surveyed, such as their corporate intranet (76 percent), training sessions (75 percent) and email campaigns (73 percent). As stated, human factors cause the greatest concern, and therefore traditional awareness programmes in most companies should be evolved to incorporate new approaches.

Regarding payment systems, our report finds that the majority of those surveyed are conscious of cyber security risks in relation to payments systems, with 64 percent of those surveyed stating that they have conducted a cyber-risk assessment of their payments systems in the last 12 months and 60 percent having implemented a separate security policy for online and/or mobile payments. Risk assessments should be conducted regularly in the context of a complex, sophisticated and rapidly evolving cyber security threat landscape, because the consequences of successful attacks can be significant, resulting in financial losses, regulatory censure and loss of reputation and customer confidence.

The European Central Bank Secure Pay forum recommendation for the adoption of strong customer authentication is based on the use of two or more of the following elements: knowledge, ownership and inherence, where inherence is suggested to be a biometric characteristic, such as a fingerprint (see 'Recommendations for the security of internet payments', published 31 January 2013).

Concerning the ECB recommendation, the survey results identify a wide adoption of two-factor authentication as a method of securing payments systems, a large majority (71 percent) having already implemented two-factor authentication. The majority (76 percent) of those who have not already done so intend to implement two-factor authentication within the next 12-24 months. Some organisations are actively investigating and pursuing disruptive approaches to authentication using biometric solutions, particularly in the online and mobile channels, whether through voice, facial or fingerprint recognition (for example the recent launch of Apple Pay with finger print authentication 'Touch ID'). In the payments market we are seeing adoption of biometrics being driven through the telephone channel, particularly in the UK and Australia.

Security methods, whether two-factor or biometric, are not sufficient by themselves. Effective security for online and mobile payments systems requires a multi-layered controls framework, supported by a mature governance framework. This requires both effective authentication controls and a suite of non-customer facing controls, for example threat intelligence, perceptive fraud detection monitoring capabilities as well as excellent response and operational capabilities.

The increasing threat of cyber security breaches and attacks should focus minds within financial services organisations. To start to effectively address this threat requires budgetary increases in both technical and human resources across the whole organisation, as well as a global increase of awareness campaigns not only for IT departments but also for business units and departments, starting with the executive board.

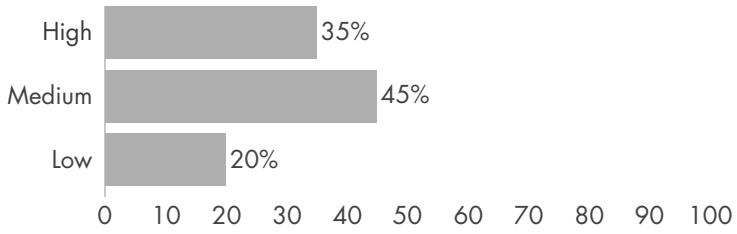
The surveys were conducted between April and June 2014. Our report incorporates quantitative and qualitative data based on this survey of European institutions.

The Deloitte and Efma questionnaire

Level of awareness

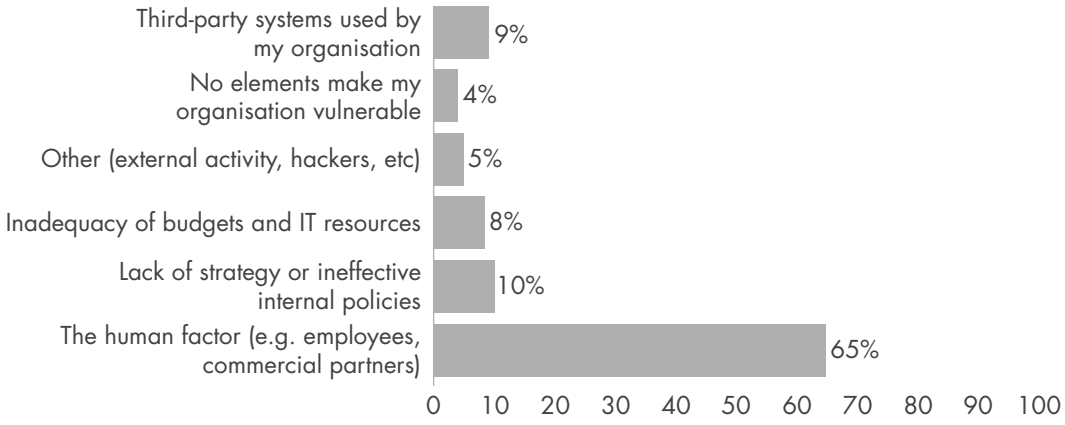
The data obtained show that there is concern about cyber attacks. In general terms, cyber security is considered with a medium/high level of importance.

How would you rate your organisation's exposure to cyber risk?



The survey shows that the majority of the respondents believe that the exposure of their companies to cyber attacks is medium level (45 percent) or high (35 percent).

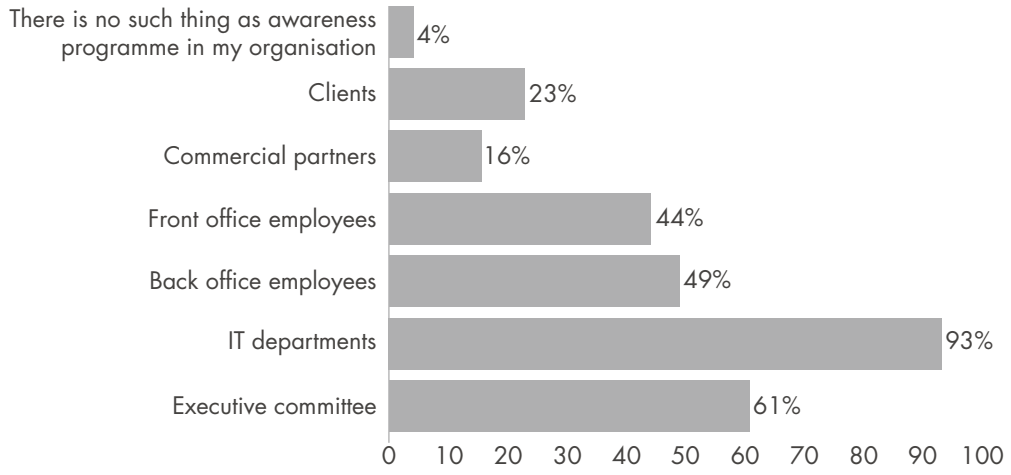
In your opinion, which one of the following elements makes your organisation more vulnerable to cyber risk?



65 percent of the respondents believe that the greatest vulnerability lies in human factors. Other respondents considered the greatest vulnerability to be a lack of strategy (10%), third-party systems (9%) and an inadequacy of budgets and IT resources (8%).

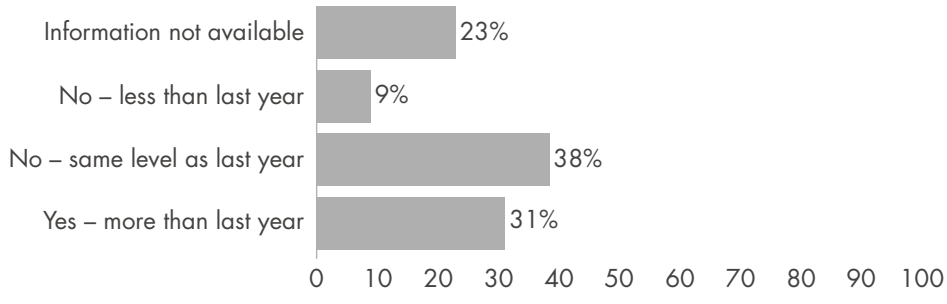
Notably, 4 percent of respondents consider that there are no elements that make their companies vulnerable to cyber risk.

Which departments participate in cyber security awareness initiatives in your organisation? (multiple answers possible)



In the large majority of companies (93 percent), IT departments participate in cyber security awareness initiatives. In some companies, there is also involvement from other departments, mainly in executive committees (61 percent) and back (49 percent) and front office employees (44 percent).

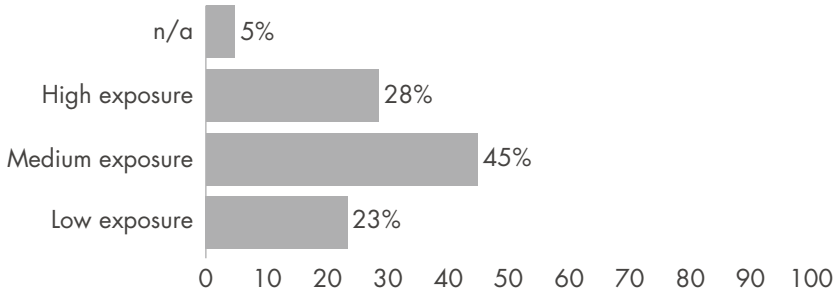
Have cyber attacks against your organisation increased during the last year?



Many of the companies surveyed reported having the same level of attacks as the previous year (38 percent), while almost the same number have seen an increase in attacks (31 percent).

23 percent of respondents didn't give or don't have any information about cyber attacks against their organisation.

In your opinion, what is your CEO's perception of exposure of your institution to cyber risk?



45 percent of respondents indicated that their CEO's perception of the company's risk to cyber attacks is at a medium exposure level. The numbers of respondents indicating that their CEO's perception is one of low exposure (23 percent) or high exposure (28 percent) was similar.

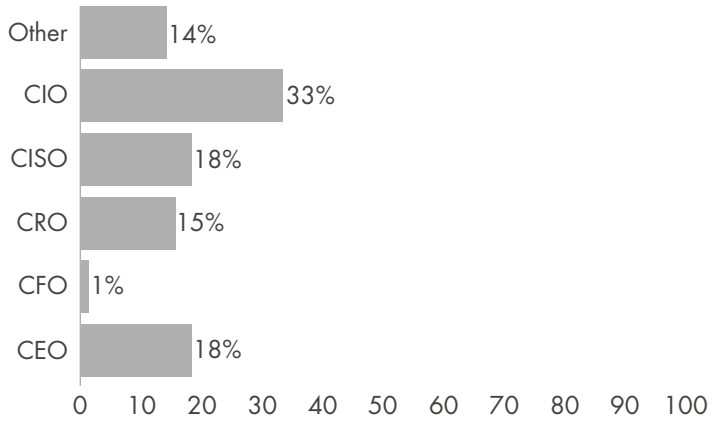
In your opinion, do you consider cyber security a:

The survey showed an emphatic result, cyber attacks are considered as an international issue (99 percent).

Level of significance

According to respondents, the responsibility for cyber security within the company lies with the IT department or the CIO, indicating that the CEO should have a greater awareness and responsibility in the future.

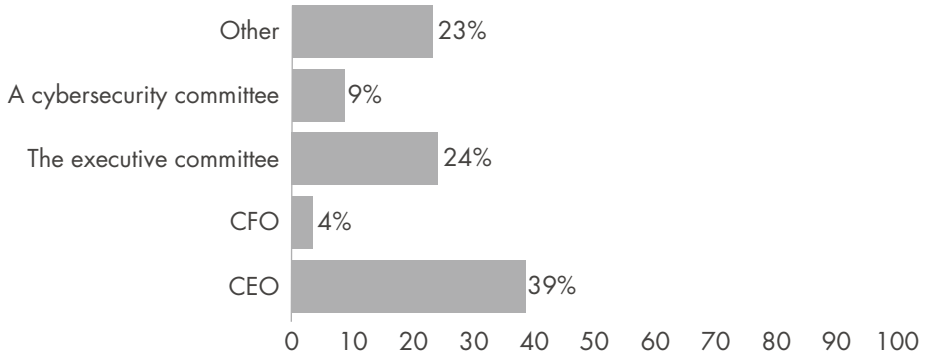
What role does the person with the highest level of responsibility for cyber security issues have in your organisation?



The person that has the responsibility for cyber security is in most of cases (33 percent) the CIO and the IT manager. In 18 percent of responses each, the CEO and CISO had the highest responsibility.

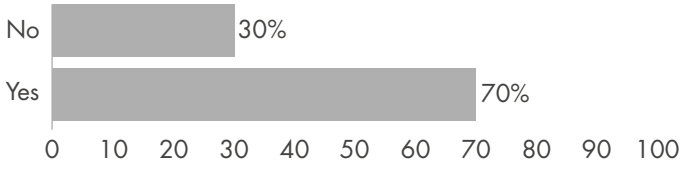
6 percent of respondents gave the Chief Operating Officer as an alternative answer.

Who does the person in charge of cyber security report to?



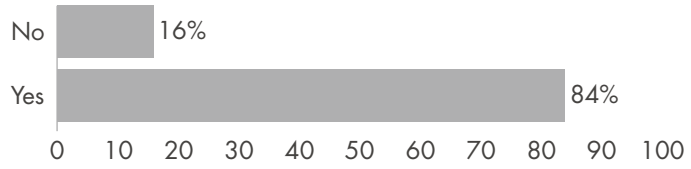
39 percent of respondents indicated that the person in charge of cyber security reports to the CEO and 24 percent to the executive committee, but the survey also revealed that 9 percent report to a specific group dedicated to cyber security.

Do you consider that cyber security should be a priority on your CEO's agenda at this moment?



Although almost three-quarters (70 percent) of the respondents indicated that cyber security should currently be a priority for the CEO, whereas 30 percent did not feel it should be a priority for the CEO or, therefore, the company.

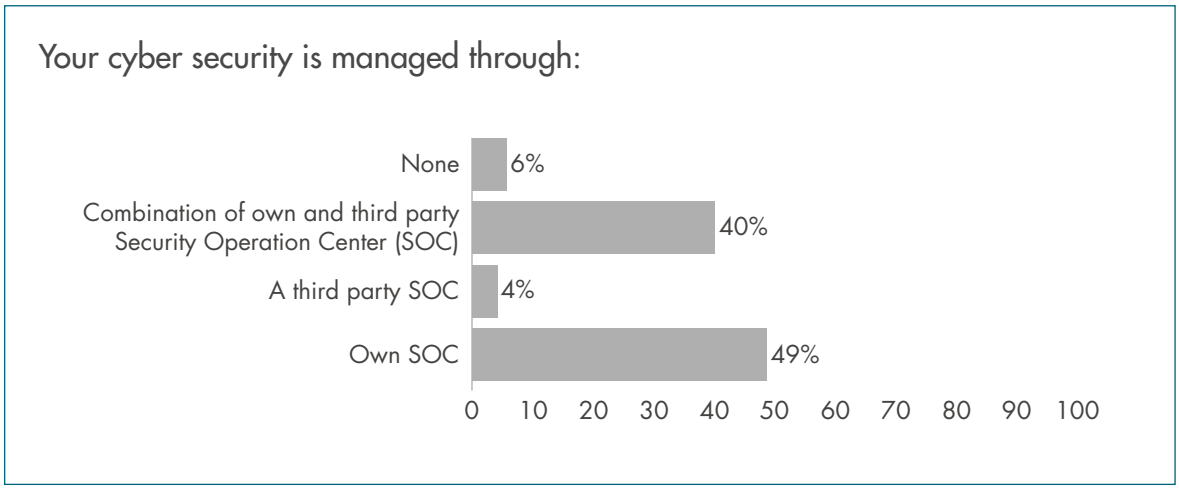
Do you consider that cyber security should be a priority on your CEO's agenda in the future?



Although some respondents (16 percent) felt cyber security should not be a CEO priority in the future, 84 percent of respondents felt it should be.

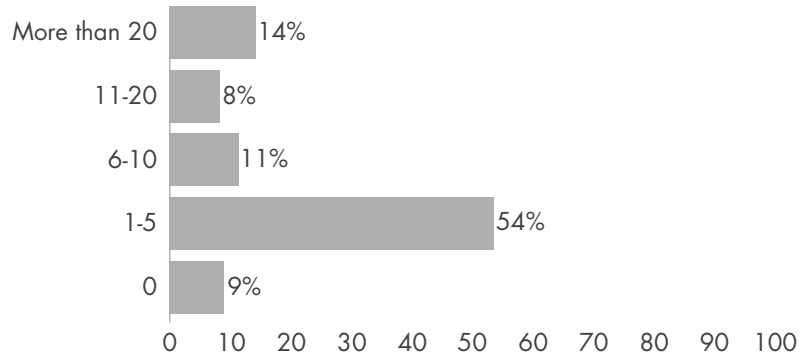
Level of implementation

Most companies have opted to manage cyber security through their own Security Operation Center (SOC), or a combination of a third party SOC and their own SOC, with up to five of their own cyber security specialists, who have at least implemented a cyber-risk security control model for the IT department.



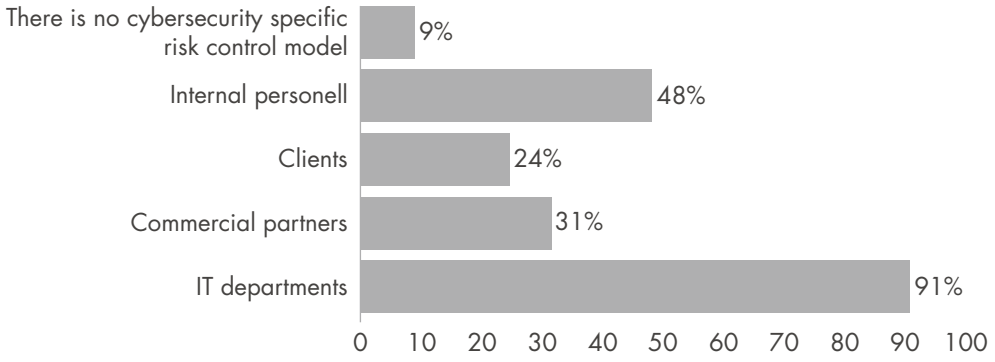
According to 49 percent of respondents, cyber security in their companies is managed through their own SOC. However, there are also 40 percent that use a third party SOC combined with their own SOC. It should be noted that the 6 percent of respondents didn't have a dedicated team for managing cyber security.

How many cyber security full-time practitioners do you have in your organisation?



54 percent of respondents have between one to five professionals in their company who are exclusively dedicated to cyber security. While 9 percent of companies don't have specialised internal professionals exclusively dedicated to cyber security, it is notable that bigger teams with more than 20 professionals, are present in 14 percent of the participating companies.

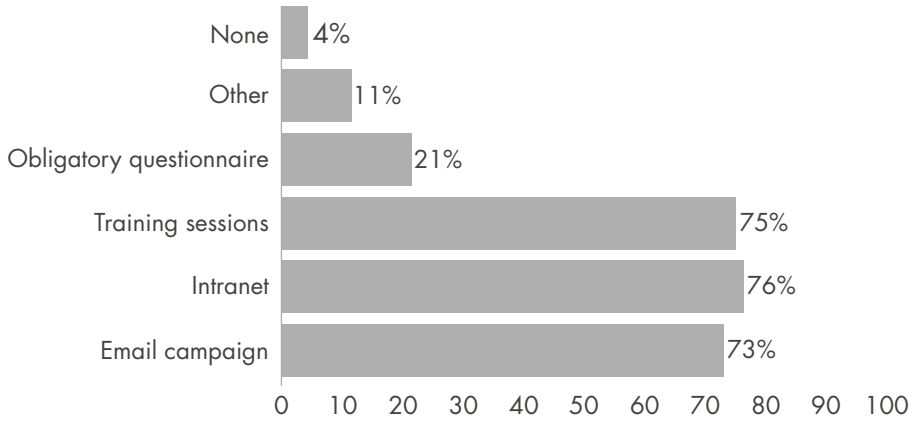
Which agents are included in the scope of your cyber security risk control model? (multiple answers possible)



The IT department is included in the risk control model's scope in 91 percent of respondent's companies.

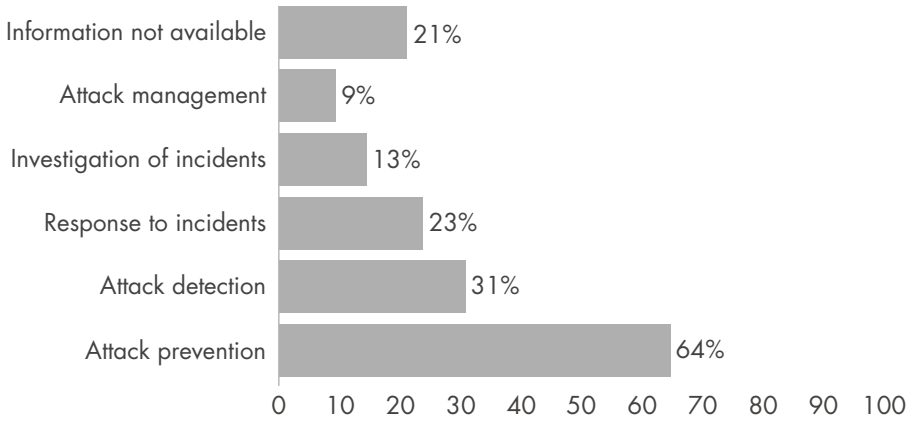
It is noteworthy that 9 percent doesn't have a cyber-risk control model. On the other hand, it is not unusual for clients (24 percent) and commercial partners (31 percent) to be included.

Which of the following tools are used in your organisation to achieve a cultural change in terms of awareness? (multiple answers possible)



According to data provided by the respondents, the primary tools used for cyber security awareness within companies are the corporate intranet (76 percent), training sessions (75 percent) and email campaigns (73 percent). These are traditional methods of communication; no specific innovations for cyber security communication were detected by the survey. Only 21 percent use obligatory questionnaires to increase awareness. 4 percent of respondents say they don't have any tools of awareness in their companies.

Currently in your organisation, which of these activities are the most budget-intensive? (maximum two answers)



Based upon the answers given by respondents, 64 percent indicated that their company spends more money on preventing cyber-attacks than other issues such as detection (31 percent) or response (23 percent). Attack management has a minor presence in budgets (9 percent).

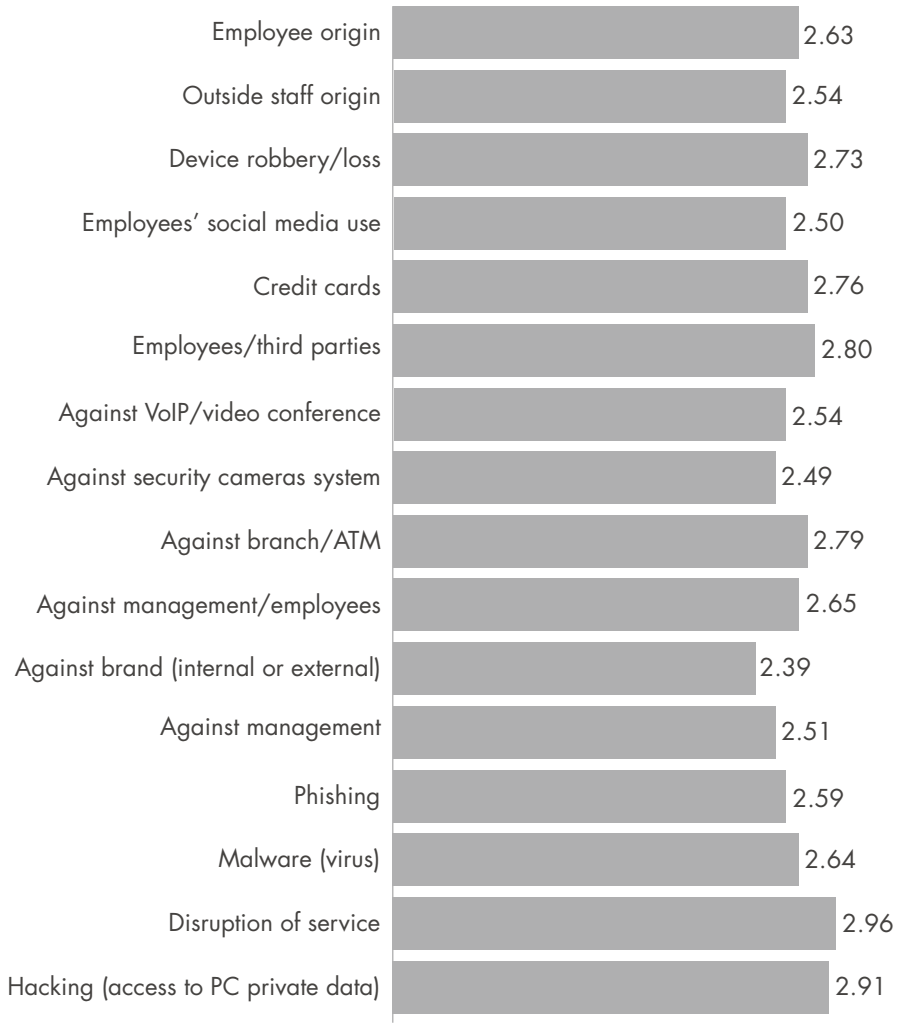
21 percent of respondents didn't have or didn't provide information about this item.

Gap identification and concerns

There is a perception that companies are quite robust to many types of cyber attack, but still with capacity for improvement. Of the impacts of a cyber attack, companies are most concerned about their reputational risk.

Companies are conscious that cyber attacks are an international issue, but most of them don't participate in international organisations that combat these hazards.

To what extent do your current cyber security measures protect you against these threats?

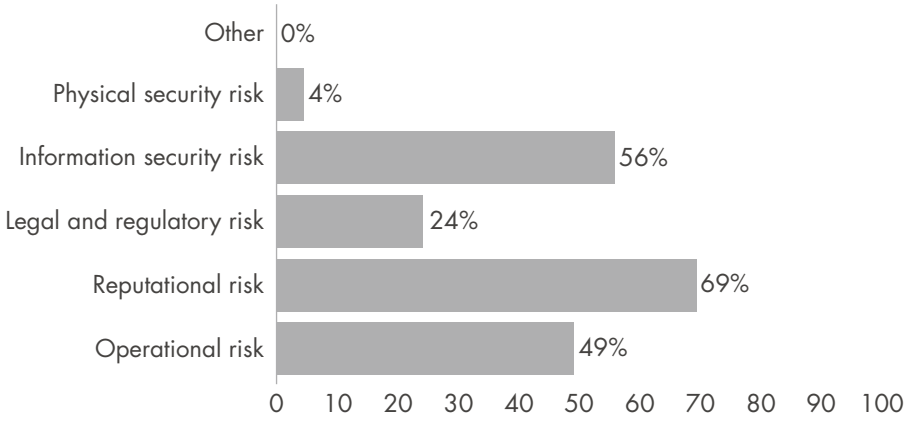


The previous chart shows the weighted average of the threats indicated in the survey. Each of the identified threats has a scale (1 to 4) according to the level of protection that is implemented in the company, with level 4 the greatest level of protection. The respondents indicated the level of protection for the threat in question.

Among the various threats that could occur in a company, most respondents believe that their security measures are at an acceptable level, although they believe there are hazards that are not sufficiently mitigated, where measures for improvement are needed, for example against brand, security camera systems and employees' social media use.

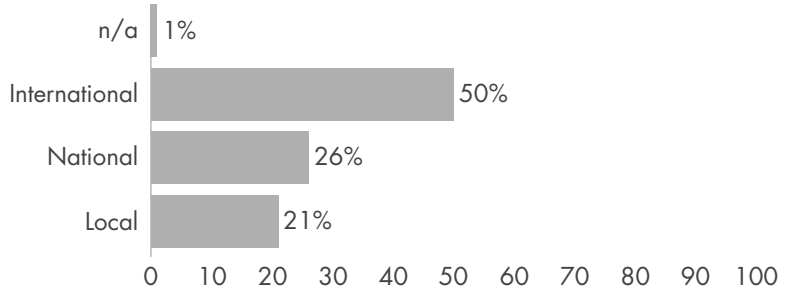
The security threats considered most important were disruption of service, followed by hacking.

If your business was to suffer a cyber attack, which aspects would you be more concerned about? (maximum two answers)



Of the different impacts of a cyber attack, reputational risk to the company is a concern for 69 percent of respondents, risks in information security a concern for 56 percent and operations risk a concern for 49 percent.

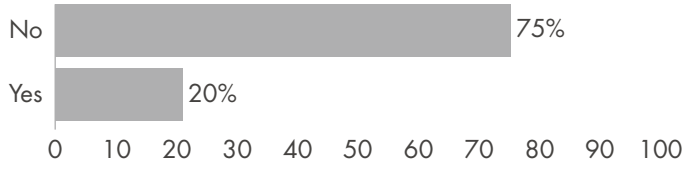
What is the scope of the measures being carried out by your business to prevent cyber attacks?



For half of the respondents, the security measures undertaken by the company are international, while the remaining respondents have implemented measures at a local or national level.

Only one percent of respondents indicated that there are no security measures being carried out within their business.

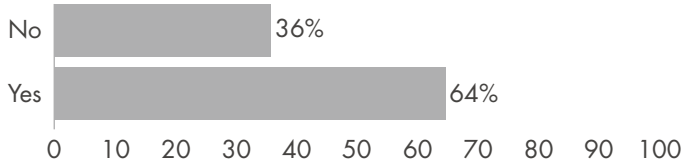
Is your company a member of any international organisation that fights against cyber attacks?



75 percent of respondents said that their company is not part of any international organisation that works to mitigate cyber attacks, although 99 percent consider cyber security an international issue.

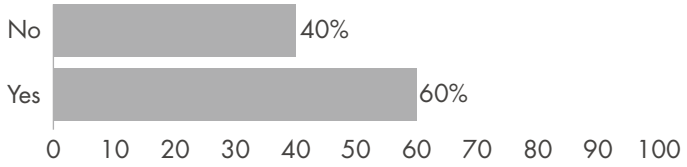
Payments

Have you conducted a cyber risk assessment of your payment systems in the last 12 months?



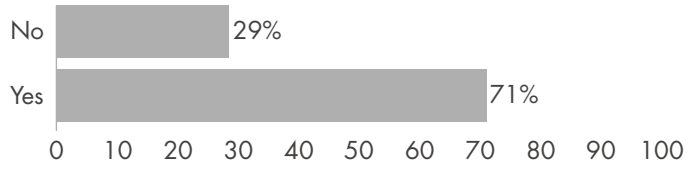
The majority of respondents are conscious of cyber security risks in relation to payments systems, with 64 percent of those surveyed stating that they have conducted a cyber risk assessment of their payments systems in the last 12 months and 60 percent having implemented a separate security policy for online and/or mobile payments.

Have you implemented a separate security policy for online and/or mobile payments?



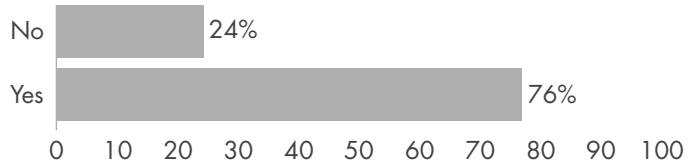
Policies and procedures form a key part of an effective governance framework and support the development of a robust and effective control environment.

Have you implemented two-factor authentication for your payment systems?



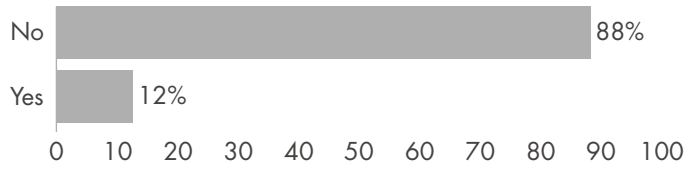
A large majority (71 percent) of those surveyed have implemented two-factor authentication for their payments systems.

If your response to the previous question is No, then are you planning to implement two-factor authentication for your payment systems in the next 12-24 months?

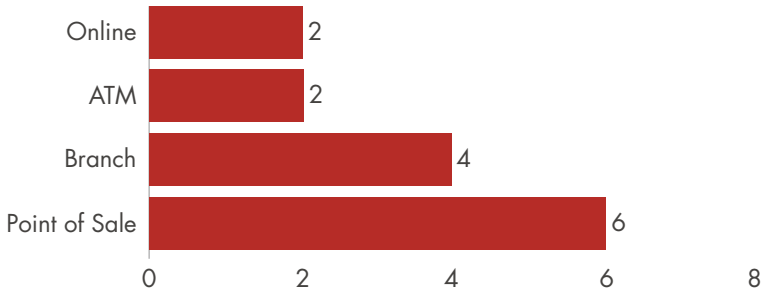


Of those who have not implemented two-factor authentication (see previous question), 76 percent stated that they do intend to do so in the next 12-24 months. This reflects what we see in the market, with two-factor authentication, in one form or another, being widely accepted as a key control for high-risk online payments systems.

Do you currently use biometric security (such as fingerprint identification, iris recognition, voice recognition) for any of the following payment channels?

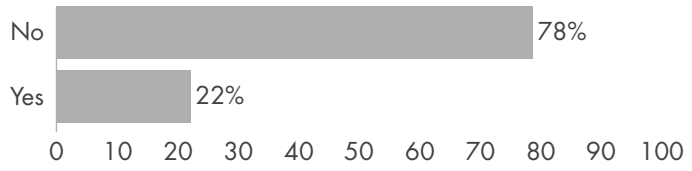


Of those who use biometric security, the payments channels are the following:



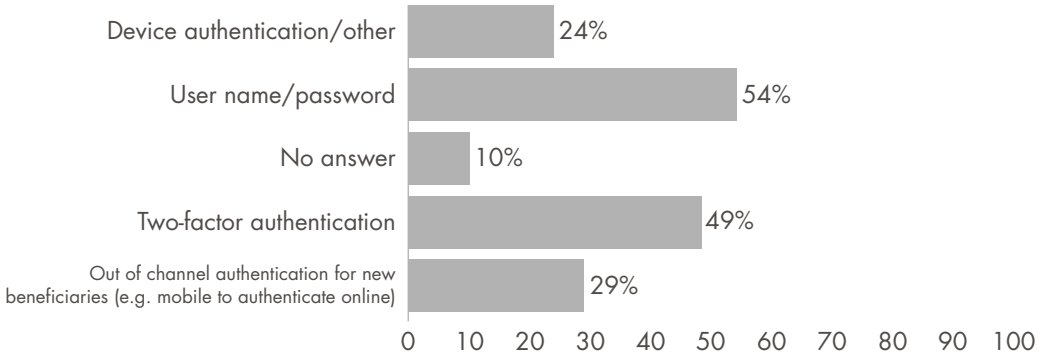
Our report finds that only 12 percent of those surveyed currently use biometric security (such as fingerprint identification, iris recognition and voice recognition), most commonly for the point of sale channel (43 percent), followed by branch (29 percent), then ATM (14 percent) and online (14 percent).

If you have selected No in response to the last question, then do you have plans to implement biometric security for any payment channels in the next 12-24 months?



For those surveyed who stated they do not currently use biometric security for payments channels, the majority stated that they do not intend to implement biometric security in the next 12-24 months.

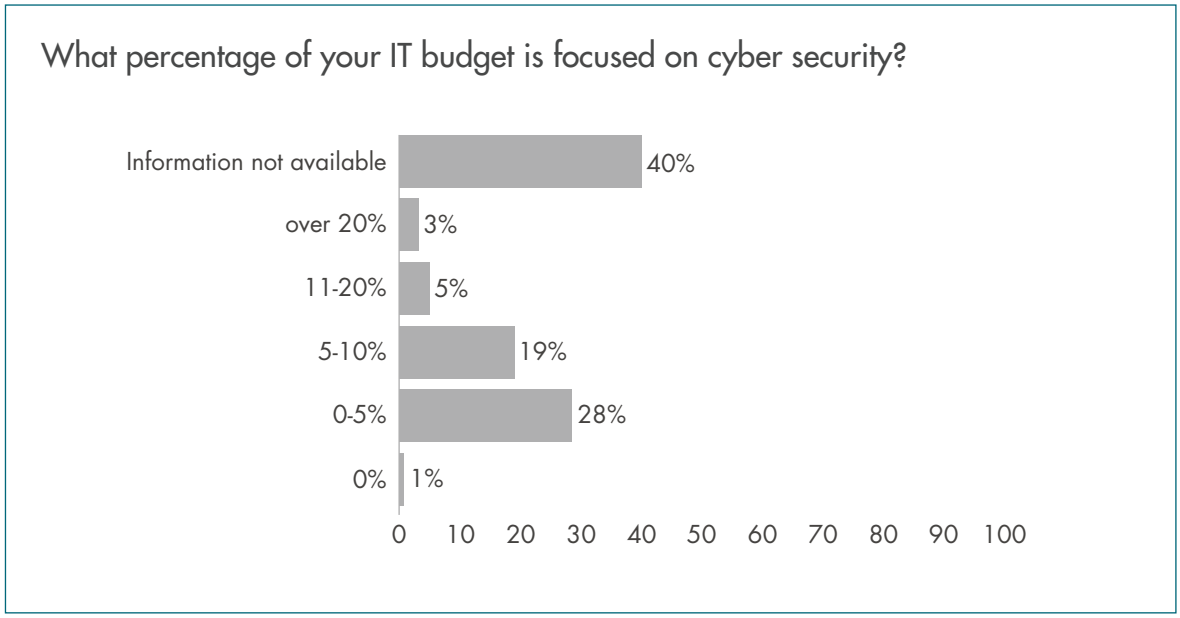
What methods of security do you use for online payments? Select all that apply.



Our survey found that the most common methods of security for online payments are user name and password, followed by two-factor authentication, with 54 percent and 49 percent respectively of those asked stating they use these methods.

Out of channel authentication for new beneficiaries (e.g. mobile to authenticate online) was stated as a method of security for 29 percent of respondents. 24 percent of those surveyed stated they use device authentication or another method of security for online payments.

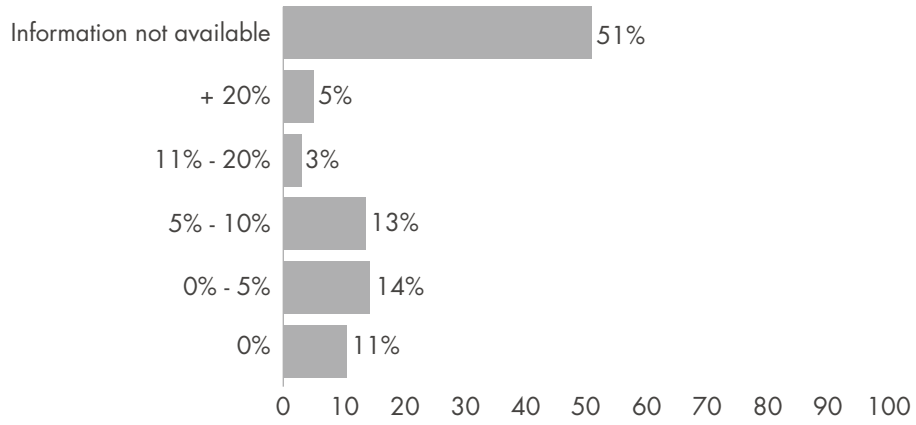
Facts and figures



47 percent of the companies surveyed invest up to 10 percent of the IT budget on cyber security while for 28 percent, investment does not exceed 5 percent of the IT budget. In contrast there are 3 percent of the companies that make investments of over 20 percent of the IT budget. Only 1 percent of companies don't make any investments in cyber security.

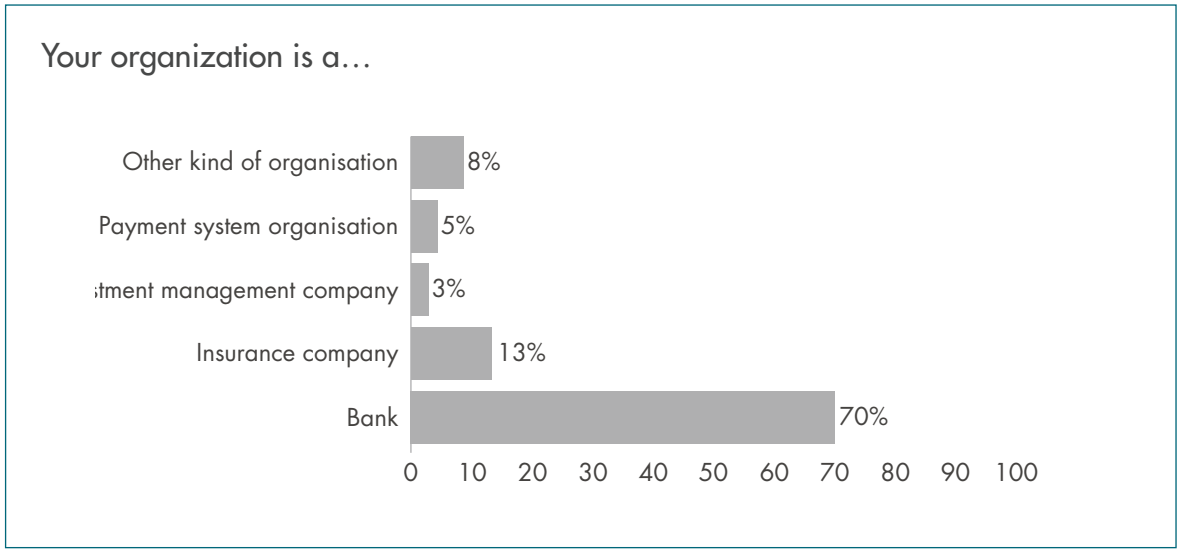
40 percent of the survey respondents do not have information about budgetary investments on cyber security.

By what percentage has the cyber security budget in your company increased in the last year?

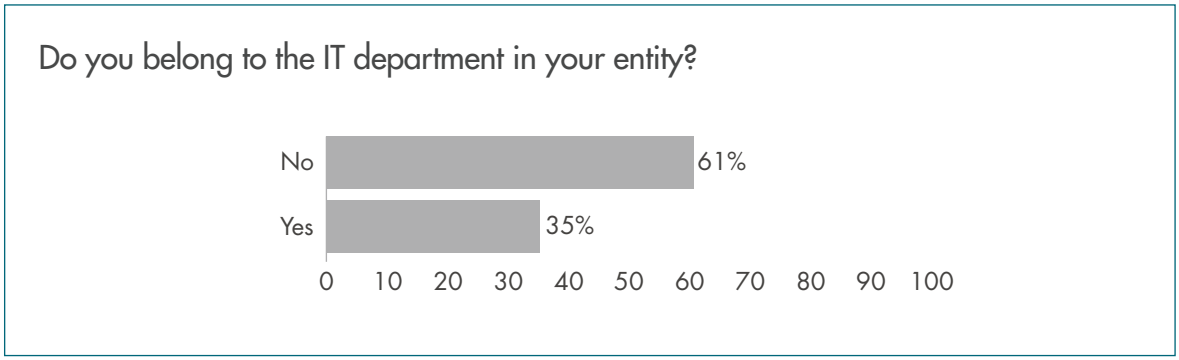


According to the data, budget increases over previous year for cyber security are minimal, with 11 percent of respondents seeing no increased at all. 51 percent of the survey respondents do not have or did not give information about budgetary evolution for cyber security in the last year.

Information about survey respondents

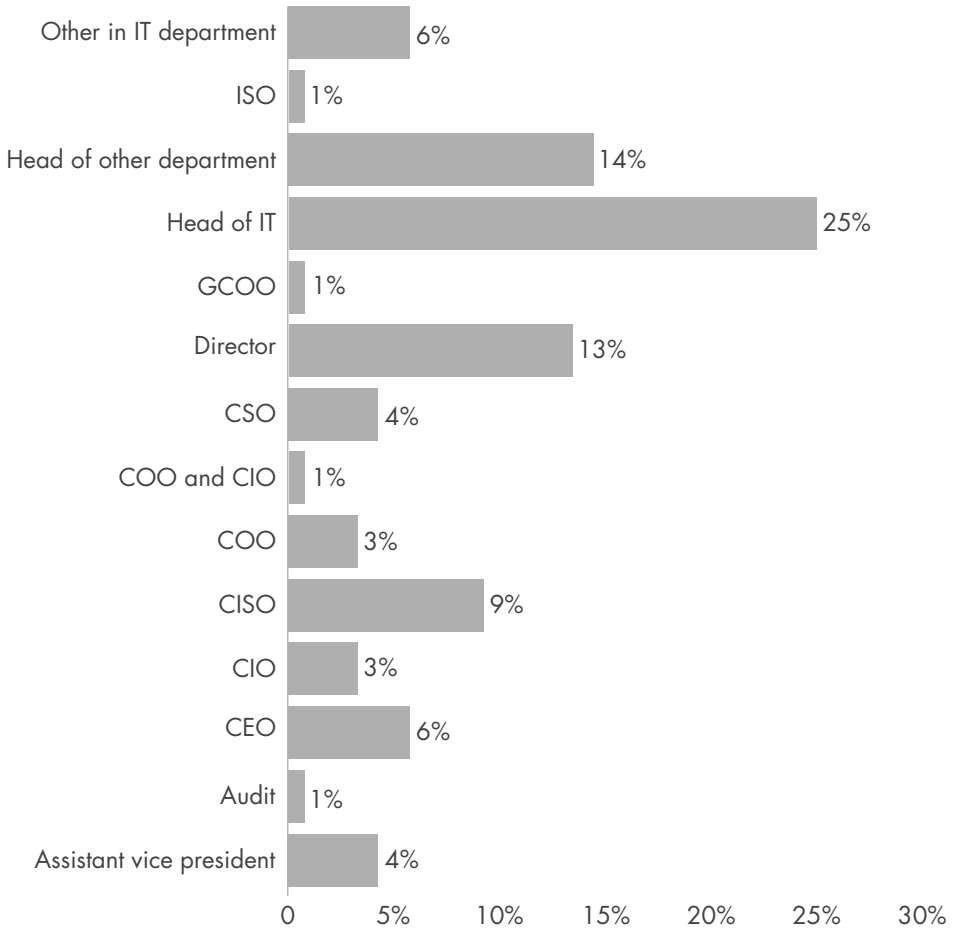


70 percent of the respondents belong to the banking sector. Insurance companies represent 13 percent, investment management 3 percent and payment system organisations 5 percent. Other sectors represent 8 percent of the respondents.



Most respondents (61 percent) do not work within the IT department of their company.

What is your job title?



A quarter of respondents belong to the IT department; and more specifically are the head of the department. 14 percent are the heads of other departments, like operations, and 13 percent are directors.

Conclusions

1. The number of cyber attacks to the financial sector is increasing

The perception of IT and operation managers is that the number of cyber attacks they sustain is growing. Financial companies feel that every second they are more and more exposed to cyber risks, and they are not the only ones. This situation is considered as a global concern, not only affecting their companies.

New attacks to ATM infrastructure, aiming at online banking services directly or indirectly, are carried out by attacking end clients with advanced and persistent malware, such as the infamous ZeuS botnet.

2. The awareness strategy is traditional and inadequate to the risk perception

The human factor is perceived as the most vulnerable element in the protection of the company's information. As a consequence, awareness programs should be wide and demanding, especially because information security depends after all on the people using it. Traditional strategies, such as training sessions, information available on corporate intranet and awareness email campaigns, do not seem to be efficient enough to leave a mark on employees and contractors.

Nowadays the amount of attacks aimed at end users and their workstations is increasing exponentially and, in spite of the technical perimeter protections, these attacks are effective partially because of users' lack of awareness.

3. Cyber security budgets are moderately growing

The information extracted regarding budgets points out a moderate growth of the cyber security budget in contrast to last year's information. Such budget is mainly spent on attack prevention and detection, especially organisations' own cyber SOCs.

4. There is a high concern about cyber security on payment systems but current measures are not effective enough

In spite of the wide adoption of the ECB Secure Pay recommendations, two-factor or biometric methods are not considered to be the only controls to authenticate users to put in place for the protection of online and mobile payments. Multi-layered control frameworks supported by mature governance are considered to be the most effective security frameworks, that following consultation, this has now been incorporated into the final guidelines published by the ECB on 19 December 2014.

About us

As a global not-for-profit organisation, Efma brings together more than 3,300 retail financial services companies from over 130 countries. With a membership base consisting of almost a third of all large retail banks worldwide, Efma has proven to be a valuable resource for the global industry, offering members exclusive access to a multitude of resources, databases, studies, articles, news feeds and publications. Efma also provides numerous networking opportunities through working groups, online communities and international meetings.

For more information: www.efma.com or info@efma.com

Deloitte is the brand under which tens of thousands of dedicated professionals in independent firms throughout the world collaborate to provide audit, consulting, financial advisory, risk management, tax and related services to select clients. Deloitte has more than 210,000 professionals at member firms delivering services in audit, tax, consulting, financial advisory, risk management, tax, and related services in more than 150 countries and territories. Revenues for fiscal year 2014 were US$34.2 billion.

For more information: www.deloitte.com

Next steps in cyber security

March 2015