Deloitte.

Central Asian Information Security Survey Results (2014)

Insight into the information security maturity of organisations, with a focus on cyber security

Introduction and Executive summary

From September to November 2014 Deloitte performed its first “information security survey” in Central Asia to better understand the current state of information security programmes and governance structures at organisations in the region. The survey covers various industries and addresses how organisations view, formulate, implement and maintain their information security programmes.

The 39 survey questions covered the following areas:

1. organisational information
2. information security attacks and threats
3. information security data and technologies and
4. monitoring and reaction to identified security threats

The survey focused on cyber security risks and to that end we approached approximately 100 companies to fill in the online survey questionnaire.

We stipulate that we present the survey results without making a distinction by industry or organisation size and that the results are ‘anonymous’ to avoid making reference to individual organisations.

We would like to thank those organisations that participated in the survey for their cooperation. We would like to encourage other companies to participate in the next Deloitte “information security survey”.

Executive summary

The survey identified the five most relevant conclusions on the current state of information security programmes (cyber security) in Central Asia, as follows:

1. Majority of companies have not been exposed to cybersecurity incidents.
2. Information security policies, procedures and responsibilities are mostly in place and defined.
3. Insufficient controls to ensure third parties, (i.e. vendors / partners), comply with appropriate security standards.
4. Awareness of business (senior) management and end-user around cybersecurity risks is insufficient.
5. Though basic security measures are in place, more advanced solutions are uncommon.

Later in this report we provide more detailed insight on survey findings.

Comparing global trends with the information security status in Central Asia

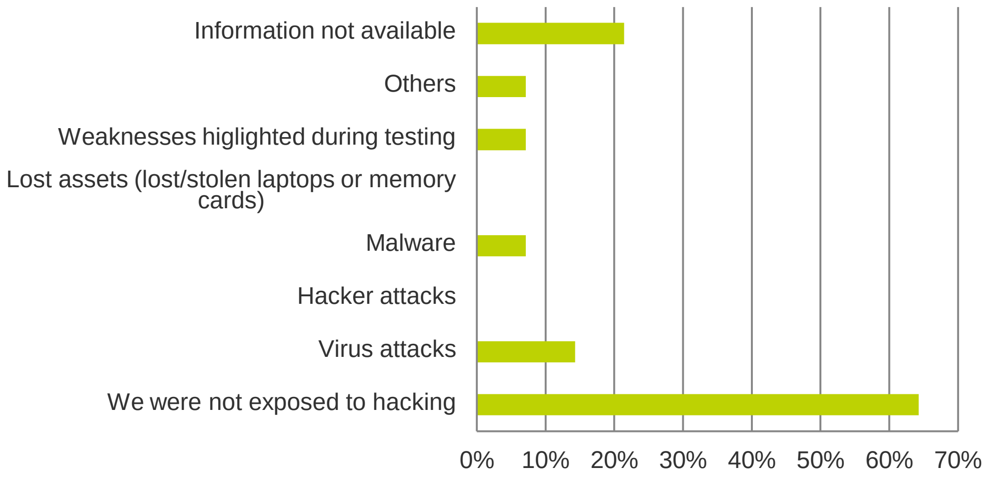
The number of information security incidents has been increasing globally, ranging from passive monitoring of communications to close-in attacks.

Undoubtedly, the recent Sony Pictures cyber attack, which involved hackers accessing some of the corporation's most confidential data, has garnered a lot of media attention, as did a massive data breach at JPMorgan Chase & Co. that ended up in 76 million records being stolen. Another example relates to the company "Home Depot" where credit card details of 56 million customers where syphoned, using Malware installed on cash register system.

Central Asia has also seen a number of security incidents making it to the news, However compared to other regions, the number of attacks appears to be limited and for the ones that have been reported, little information is available on the actual impact. According to the responses in this survey, approximately 65% of respondents have not experienced cyber attacks directed at their organisation (see question 1).

Although the number of publicly known cyber attacks appears to be small, this does not mean that organisations in the region are immune, and could ever be existing under a false sense of security. Given global trends and the increased number of attacks and attention given to cyber security, it could very well be that Central Asia may become the next target for hackers in the near future. When - not if - this happens, organisations need to be prepared.

Question 1: Have you suffered a breach in the last 12 months (multiple answers possible)?



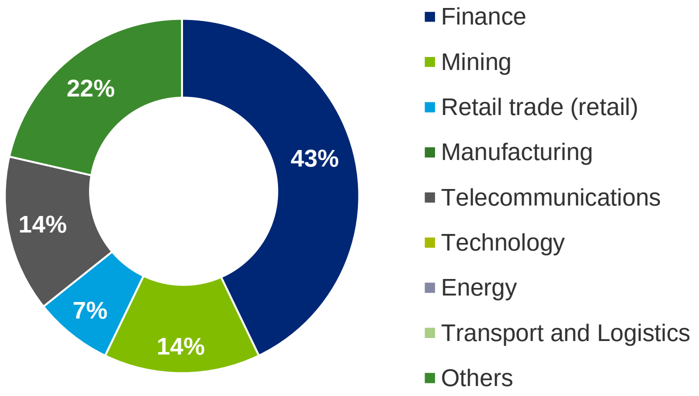
The majority of companies have not been exposed to cybersecurity incidents. However, evidence is insufficient as to whether this is reality or merely perception.

Profile of Central Asian Information Security survey respondents

Profile of Central Asian Information Security survey respondents (1/2)

Unsurprisingly, 65% of the respondents are in the Telecommunications and Finance industry (see question 2), which is not surprising as they are the industries most prone to cyber attacks.

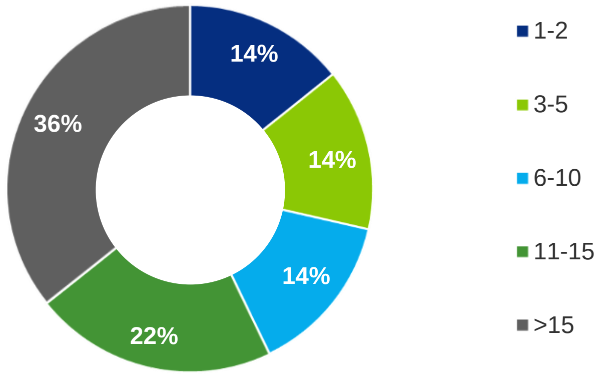
Question 2: Which industry is your organisation in?



In the meantime, governments have started to pay increased attention to the security of their strategic activities and assets (such as refineries and power stations) to protect critical IT-infrastructure - so called SCADA systems - from unauthorised access. For that reason, the expectation is that senior management in the resources industry (oil, gas, energy and utilities) should also be focusing on information security.

The majority of respondents (58%) employ more than 10 people in their IT-Departments. However, the survey also includes smaller IT-departments as show in question 3 below.

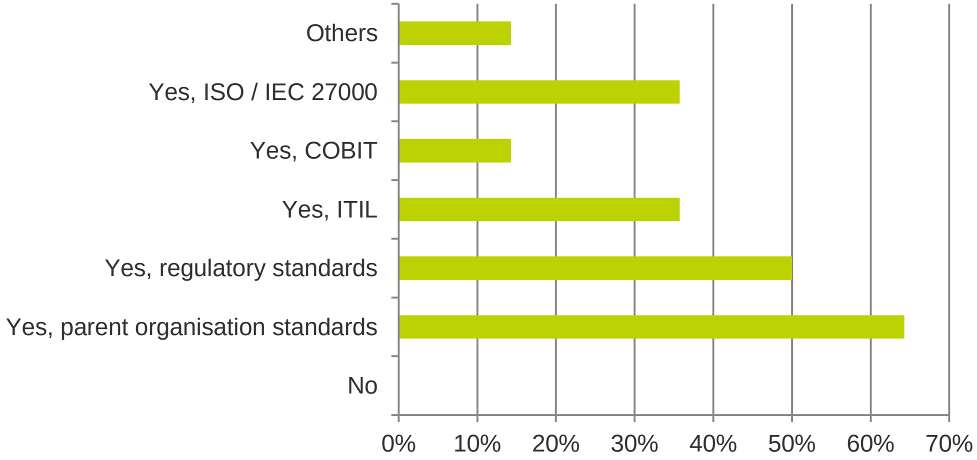
Question 3: How many people does your IT-department employ?



Profile of Central Asian Information Security survey respondents (2/2)

When asked about IT-governance standards (see question 4), the majority of organisations referred to internal (head office) policies (65%) and regulatory requirements (50%) rather than international standards such as COBIT or ITIL.

Question 4: Does your organisation adhere to IT process or security frameworks and/or standards, and if so, which ones (multiple answers possible)?



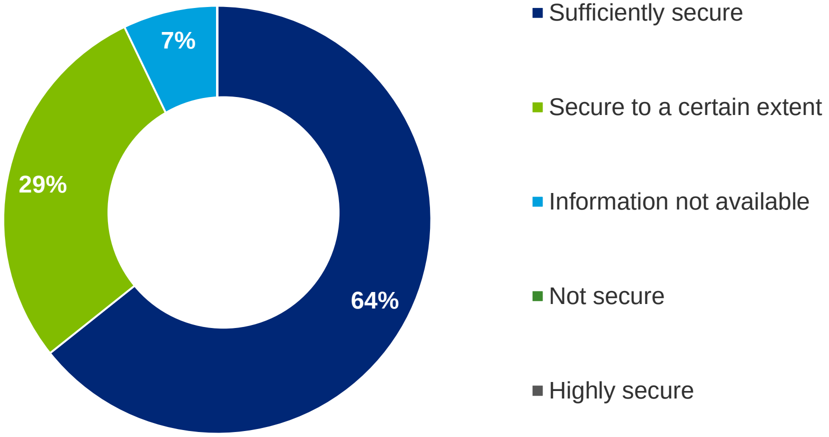
Corporate information security maturity in Central Asia

Corporate information security maturity in Central Asia (1/4)

A number of survey questions refer to information security maturity with respect to the following topics: (1) respondents' perception of their network security, (2) the existence of policies, (3) the extent to which responsibilities around information security are defined, (4) current maturity levels and (5) the key challenges to improving corporate information security.

64% of respondents consider their organisation has sufficient security policies and procedures in place (see question 5) and, interestingly, the number of respondents citing weak or insufficient security policies and procedures was zero.

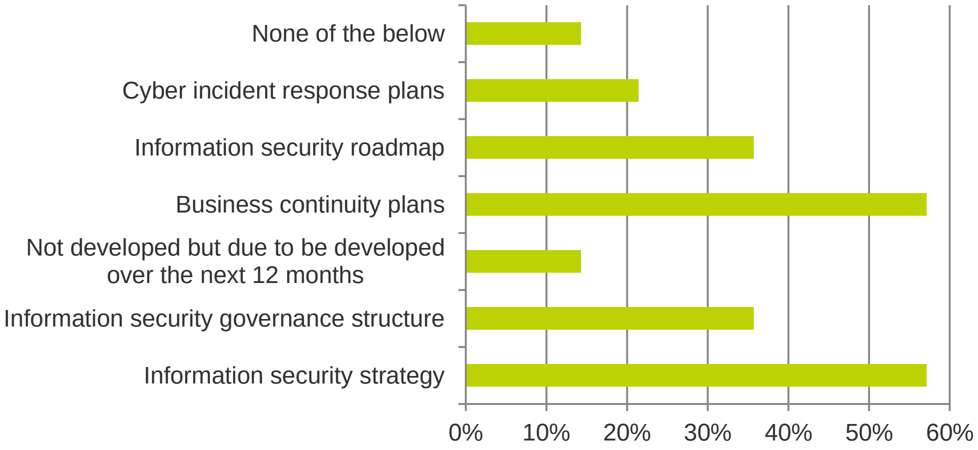
Question 5: How secure do you think your organisation's network is?



Most respondents have information security policies and procedures in place (or will introduce them in the near future), with responsibilities for information security defined.

It appears that the majority of respondents have policies and procedures in place; mostly related to (1) IT-security strategy and (2) business continuity plans (see question 6). However, only a limited number of respondents indicated that they had developed a response plan for cyber security incidents.

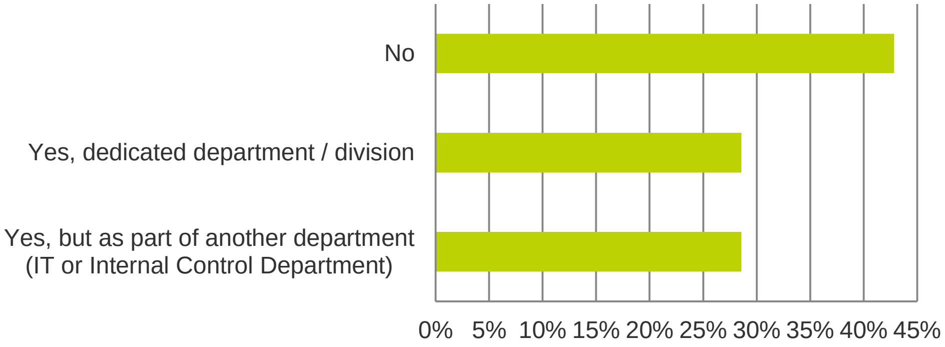
Question 6: Which of the following (policies / procedures) has your organisation documented and approved (multiple answers possible)?



Corporate information security maturity in Central Asia (2/4)

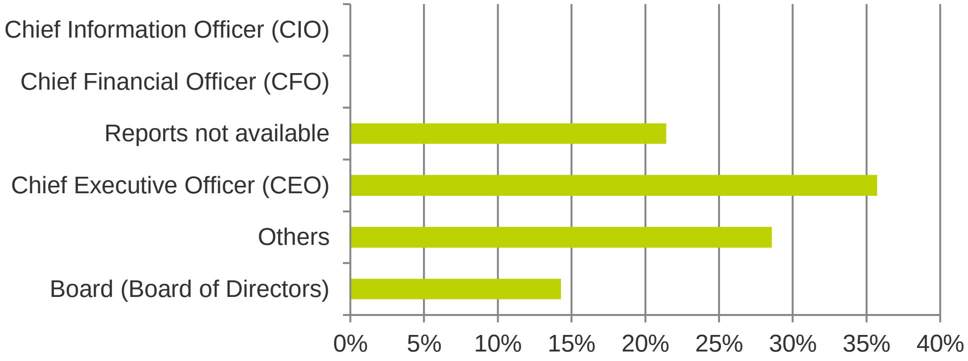
Question 7 shows that 57% of the respondents employ a security officer (or equivalent), while the remaining 43% stated that they had not yet defined information security duties.

Question 7: Does your organisation have a (dedicated) department responsible for network security?



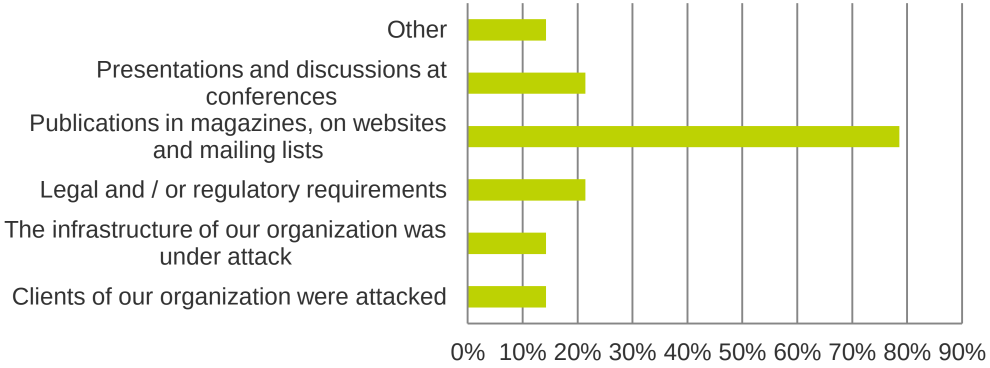
Information security reports tend not to be sent to the Chief Information Officer (CIO), but rather to the CEO (36%) or Board of Directors (14%). See question 8.

Question 8: Who does your information security organisation's executive(s) report to?



The majority (close to 80%) of organisations stay up to date on information security developments through publications and journals, mailing lists and the Internet (see question 9 and 10).

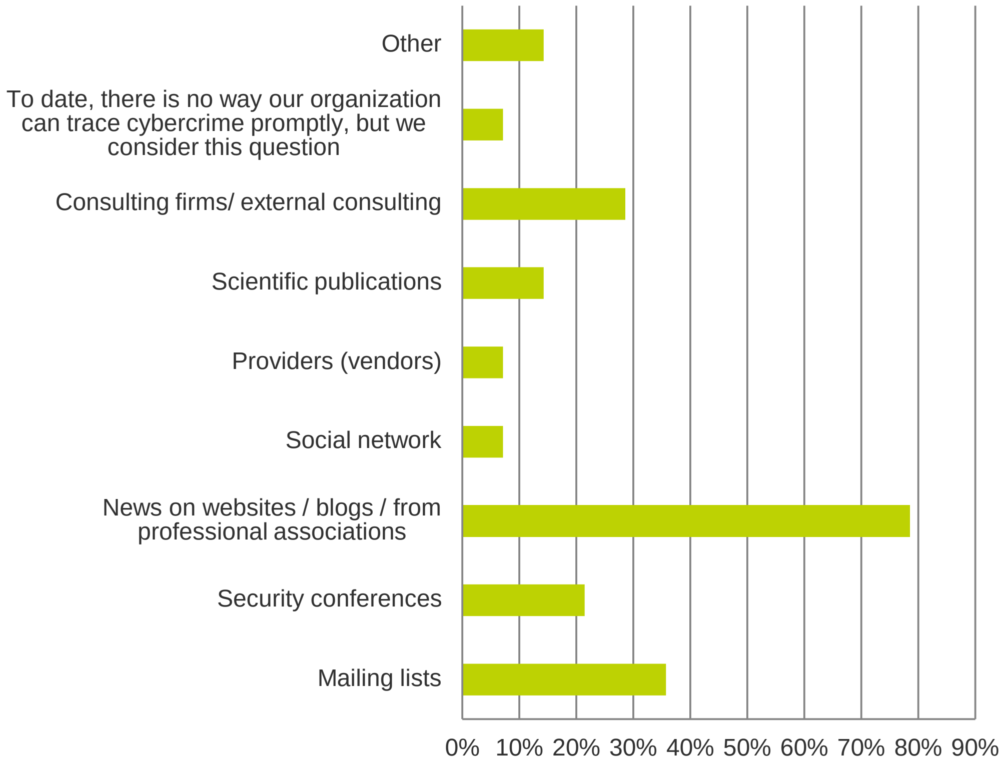
Question 9: What has raised your awareness of information security attacks (multiple answers possible)?



Corporate information security maturity in Central Asia (3/4)

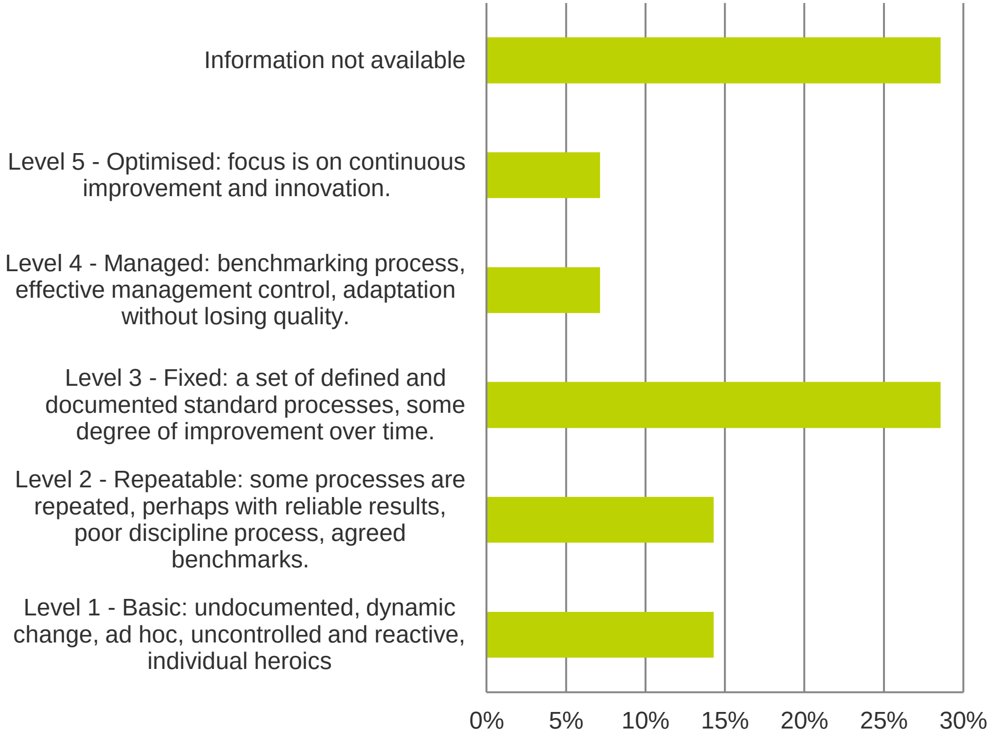
Given that each organisation is structured differently and faces different security threats (see question 13), the expectation was that more organisations would stay up to date through unique events and specific sources, such as conferences and consultants.

Question 10: How do you keep informed of new forms of information security attacks and threats (multiple answers possible)?



We asked respondents to indicate their current information security status based on our 5-level model. Approximately 30% of respondents admitted being at level 3 (see question 11), implying "the presence of a set of defined and documented standard processes, and some degree of improvement over time".

Question 11: What maturity level is your organisation currently at?



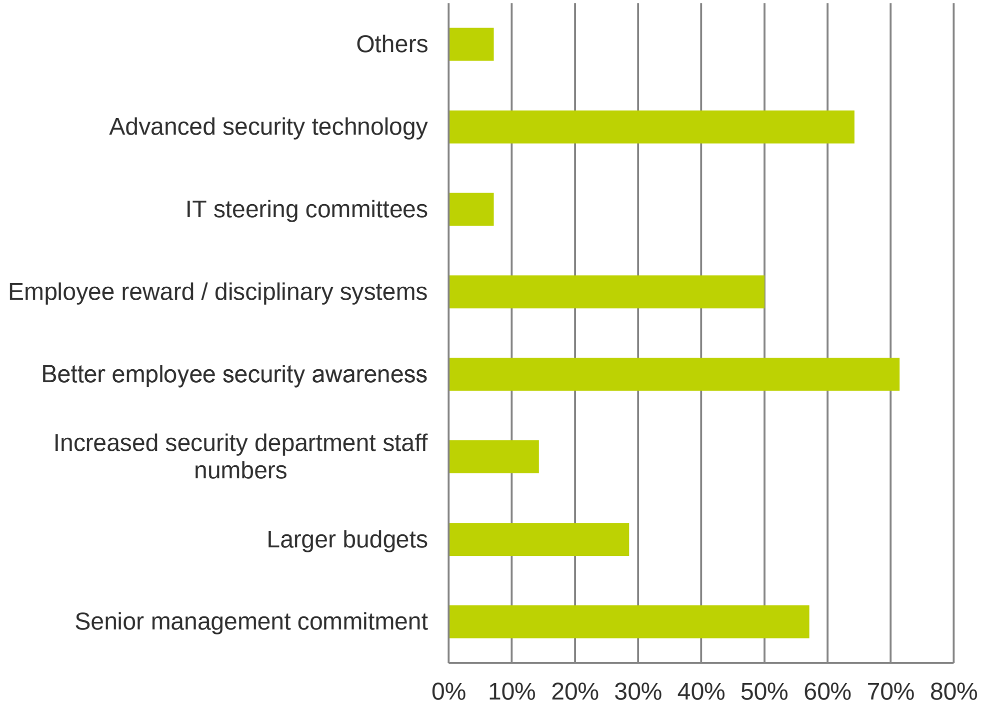
Corporate information security maturity in Central Asia (4/4)

To qualify for the 3rd maturity level, it is important that policies and procedures are not only defined but also implemented within an organisation. We are unable to comment to what extent organisations have truly implemented policies and procedures as that would require a more detailed assessment or audit. However, experience indicates that in reality, the majority of organisations in Central Asia are at maturity level 2, with only some at 3.

Finally we asked the respondents to indicate what would help them to improve information security maturity. The majority referred to the need for: (1) more advanced tooling, (2) increased awareness and (3) commitment from senior management to improve information security (see question 12).

Although IT-departments are aware of cybersecurity risks, business management and end-user awareness is considered to be insufficient.

Question 12: What do you think will help improve your organisation's security levels (multiple answers possible)?



Overview of the most commonly implemented security measures

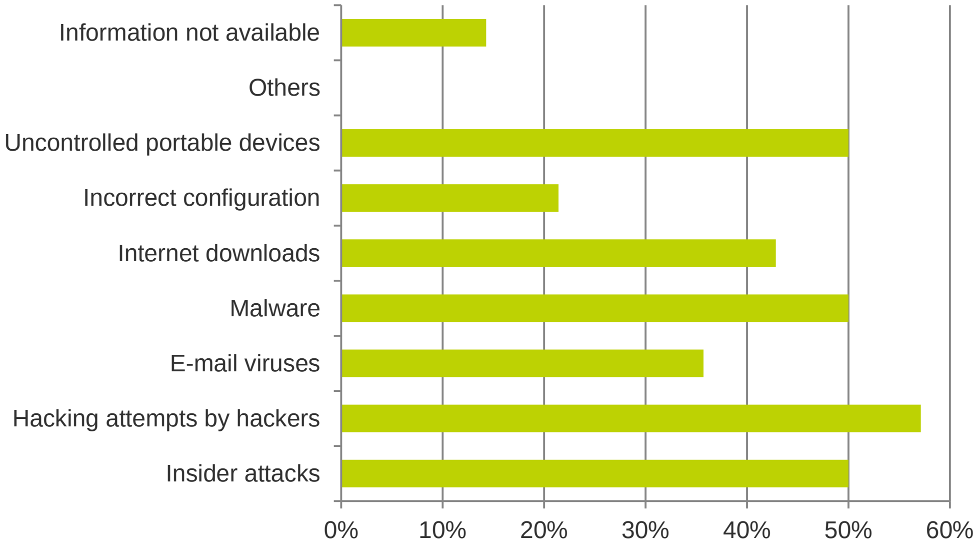
Overview of the most commonly implemented security measures (1/2)

This section of the report provides an overview of the information security threats respondents consider to be most relevant for their organisation and the security measures that have been implemented to control these threats, specifically with regards to cyber security.

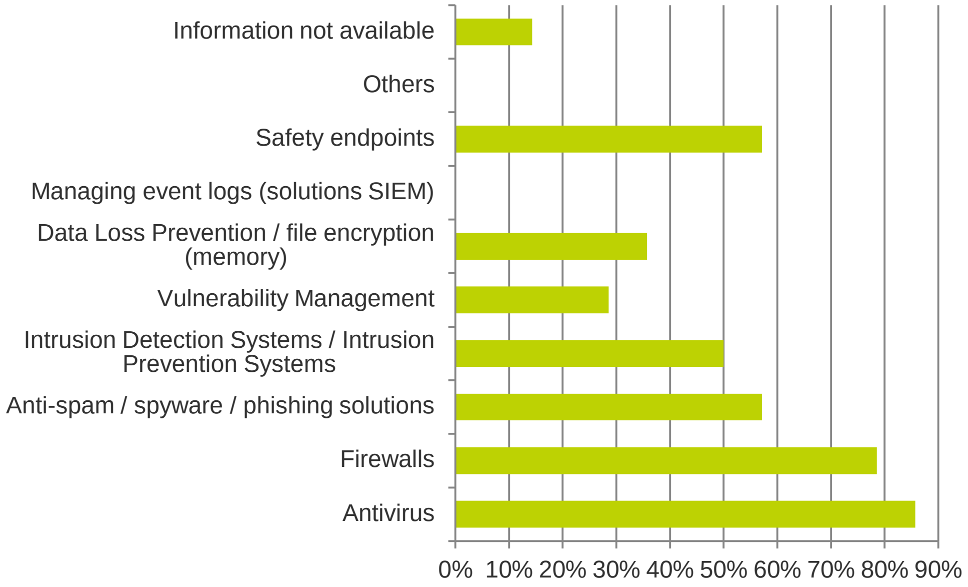
We asked respondents what risk they thought to be most relevant (see question 13). The results were quite diverse, indicating a wide range of cyber security risks faced by the organisations in the region.

Questions 14 and 15 show that most respondents have basic security measures in place such as anti-virus solutions, firewalls and access control lists. However, more advanced solutions such as intrusion prevention systems, file encryption, vulnerability management systems and event log management (including active reviews) are not as common. Given that hackers globally are rapidly becoming more sophisticated in their hacking methods, the current state of security measures could pose an increased threat to companies in Central Asia.

Question 13: What do you consider to be your greatest security risk (multiple answers possible)?



Question 14: Which security measures has your organisation implemented (multiple answers possible)?

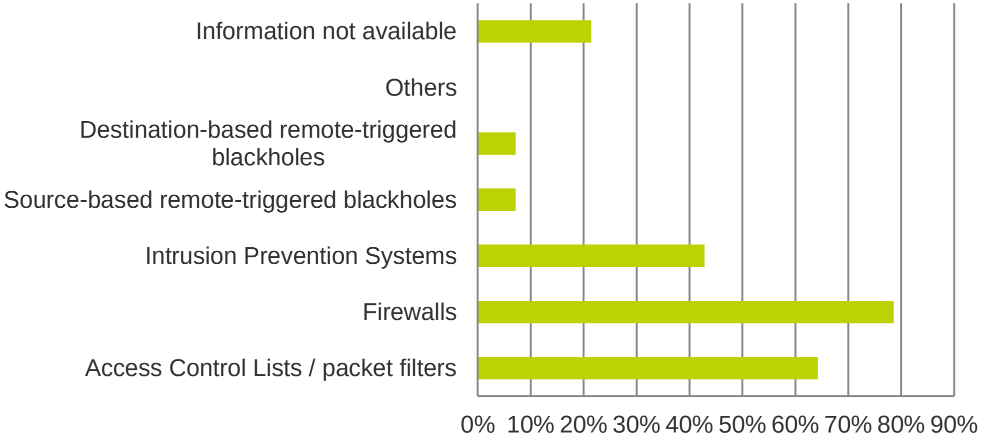


Overview of the most commonly implemented security measures (2/2)

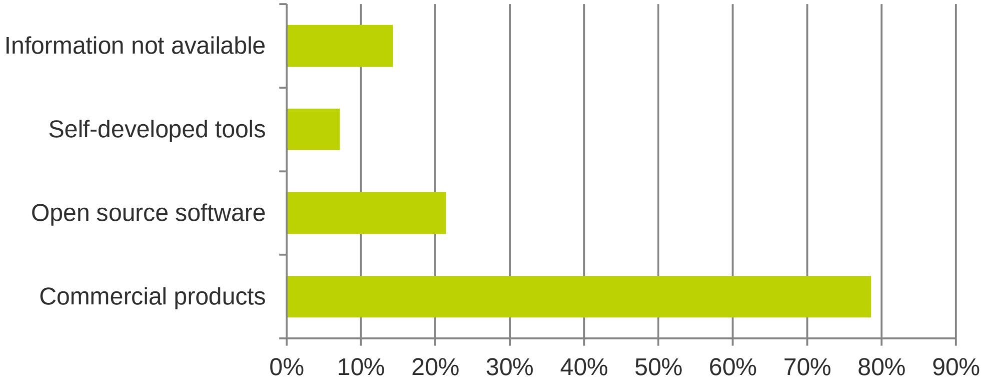
Most respondents have basic security measures in place such as anti-virus solutions, firewalls and access control lists. However, more advanced solutions such as intrusion prevention systems, file encryption and vulnerability management system are uncommon.

Question 16 indicates that companies in Central Asia mainly make use of commercial products to secure their environment rather than company specific solutions. When relying on commercial products, it is important to perform periodic (security) updates to ensure reasonable protection against the most common security risks.

Question 15: What measures do you usually take to mitigate network attacks targeted at your organisation's infrastructure / customers (multiple answers possible)?



Question 16: What tools does your organisation use to detect attacks (multiple answers possible)?



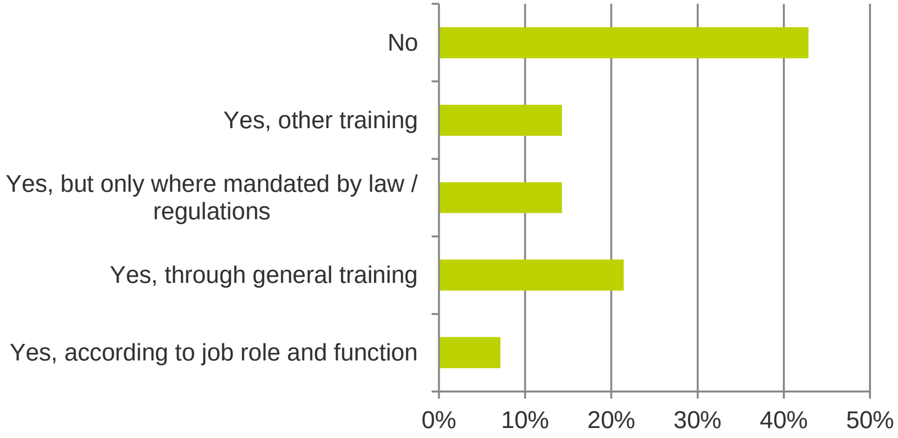
We believe that continuous investment in security threat knowledge, including any tools and practices that could be used to reduce security risk to acceptable levels, is paramount. This involves developing measures that focus on company-specific characteristics, i.e. industry and data types, and intellectual property). We stress that effective information security governance requires both preventive and investigative controls.

Information security awareness within the organisation

Information security awareness within the organisation (1/2)

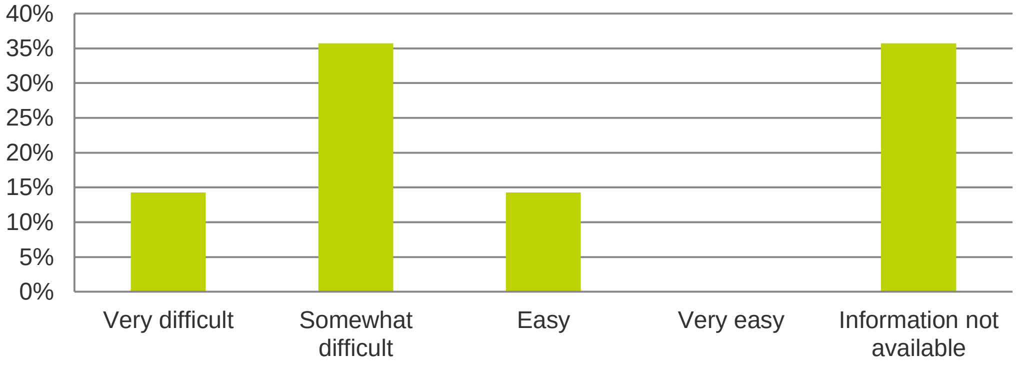
As shown in questions 9 and 10, IT-department awareness of cyber security risks is mainly through publicly available information and reports. Although IT-departments appear to be informed about and aware of cyber security risks, end-user and (senior) management awareness is less apparent (see question 17).

Question 17: Does your organisation provide employee training to raise information security awareness?



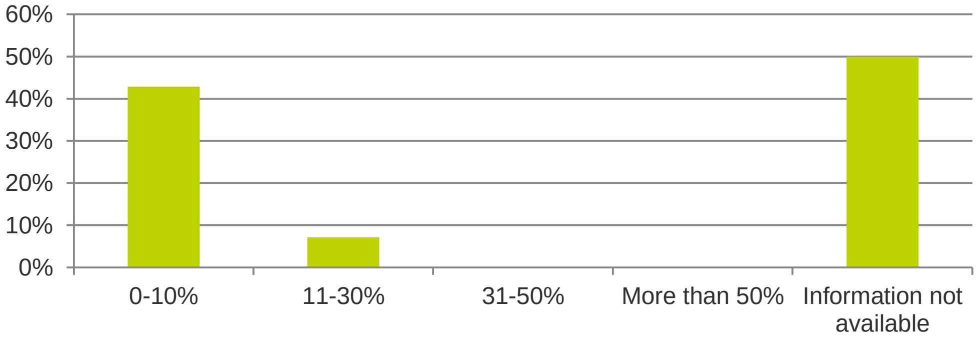
Having cyber security on corporate leadership's agenda is therefore also considered one of the key challenges IT-departments are facing in the coming period (see question 18).

Question 18: How difficult is it, in your opinion, to convince management to invest in security solutions?



Questions 19 and 20 show that a significant number of respondents did not provide information on (a) the current IT-security expenses and (b) the expected expense trends.

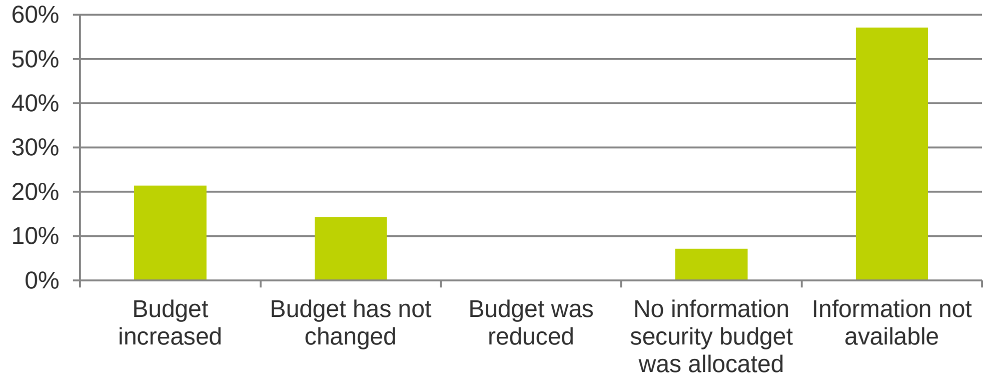
Question 19: What percentage of your IT-budget was spent on security in the last 12 months?



Information security awareness within the organisation (2/2)

This could either imply that respondents consider this information confidential or it is simply not available. If the latter is the case, we would strongly recommend improving how finances around information security are tracked as this type of information is essential to ensure an effective decision-making process (i.e. in the case of a cost-benefit analysis for proposed security measures).

Question 20: Can you describe year-to-year spending in terms of your information security budget?



Although it is not clear whether respondents' responses were caused by a genuine lack of information on actual and expected expenses or whether the information was simply not shared for the purpose of this survey, we should point out that organisations need to be aware of their current and future financial status as senior management needs to consider whether investment covers potential costs in the event of incidents.

Third party control should be a key focus areas for organisations in Central Asia

Third party control should be a key focus areas for organisations in Central Asia (1/2)

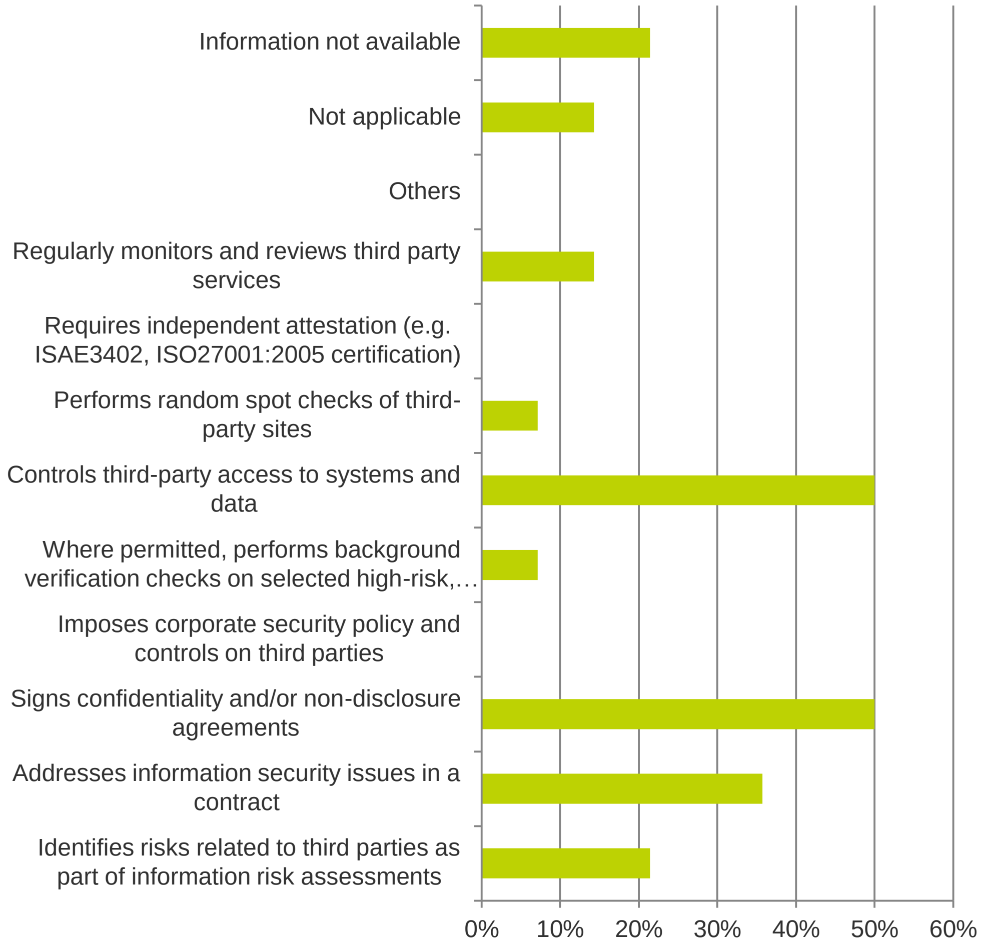
One of the most significant survey results is that information security control over third parties (contractors, vendors, and partners) is mainly based on contractual requirements and trust.

- 50% of respondents state that control is governed through confidentiality agreements
- 36% of respondents state that control is contractually enforced

Even though 50% of respondents also indicate that governance is ensured through ‘access policies’, a significantly lesser percentage has more stringent controls in place such as (a) reviews, spot checks or audits of third parties or (b) requesting third parties to provide formal certification (see question 21).

> Controls to ensure that third parties, such as suppliers and partners, comply with appropriate security standards, seem to be insufficient.

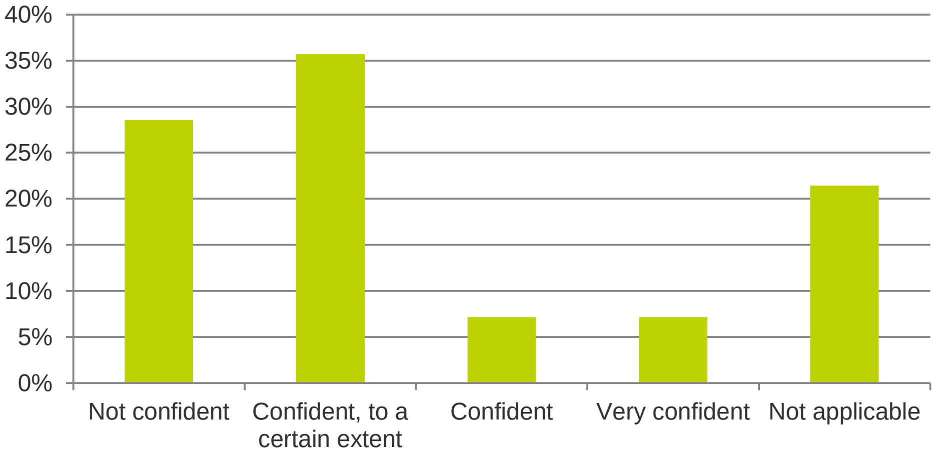
Question 21: How does your organisation ensure an adequate and appropriate level of information security over third parties (multiple answers possible)?



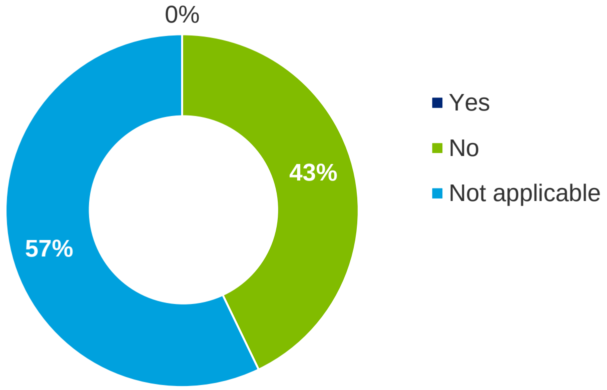
Third party control should be a key focus areas for organisations in Central Asia (2/2)

Unsurprisingly, almost all respondents are unsure that third parties involved in (critical) operations adhere to the required information security standards (see questions 22 and 23).

Question 22: How confident are you in the information security practices of your third parties?



Question 23: Does your organisation share information on information security attacks with third parties?



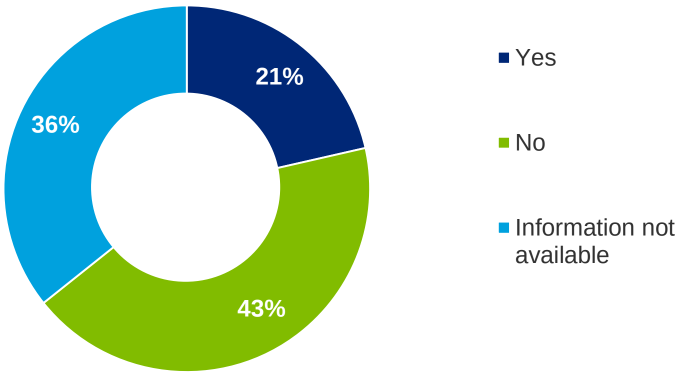
Although, a good contract defining information security responsibilities and liabilities does need to be in place, it should not be relied upon solely to govern a business relationship with a third party. It is equally important to monitor third parties for compliance with security standards. This can be done in several ways, some more far reaching than others but all with the intention to ensure that agreements are truly implemented and followed by contracting parties.

Auditing and testing information security principles

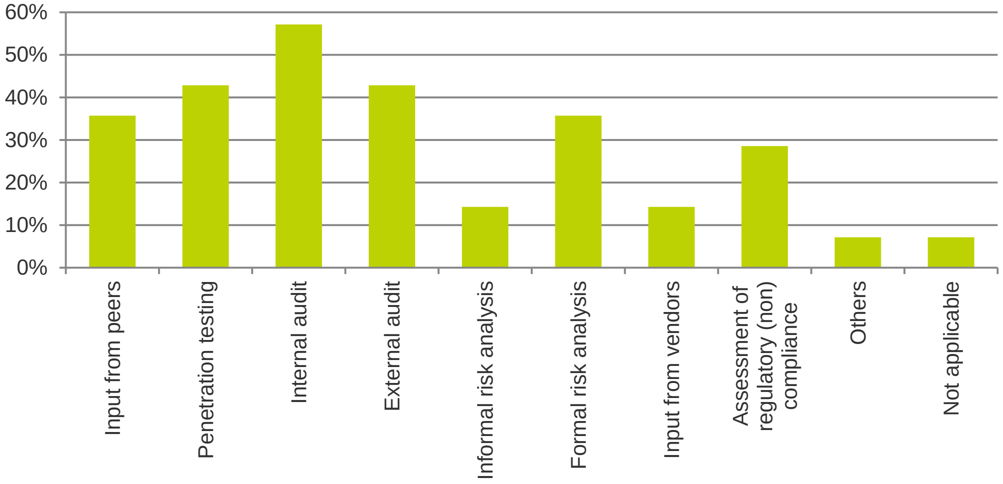
Auditing and testing information security principles (1/2)

We asked respondents to indicate to what extent their organisations perform security auditing and testing. In general, we noted that although “deep packet inspections” (DPI) cannot be performed internally due to a lack of technical ability (see question 24), most organisations perform such auditing and testing in-house (see questions 25 and 26).

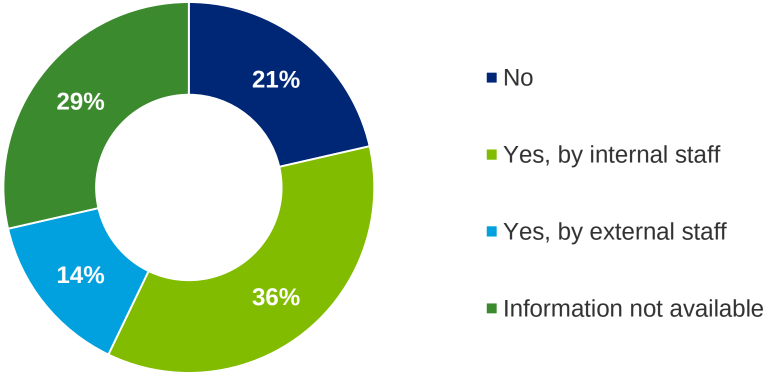
Question 24: Does your organisation have the technical ability to perform network-wide deep-packet inspections?



Question 25: How do you highlight information security weaknesses, risks and non-compliance in your organisation (multiple answers possible)?

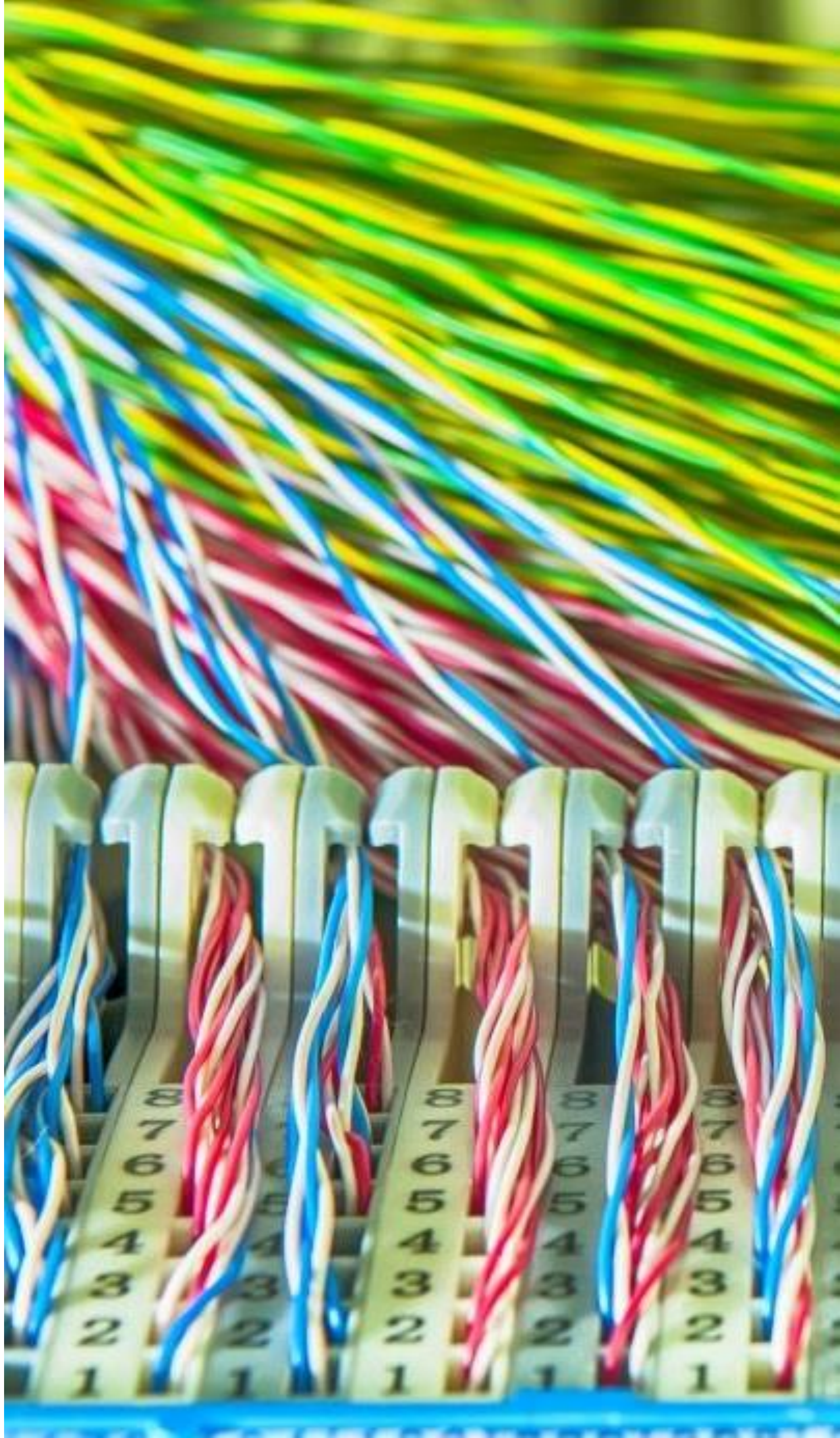


Question 26: Has penetration testing ever been performed in your organisation?



Auditing and testing information security principles (2/2)

Auditing and testing can give important insights to senior management on the current maturity status around information security practices within the organisation. In order for it to be effective, testing and auditing needs to be performed by professionals with extensive knowledge of information security, best practices and international developments so as to identify potential weaknesses that could be exploited by hackers and to provide recommendations on how to resolve them. Regular testing and audits will reduce the risk of becoming a victim of a cyber attack.



Contacts:

Michiel van Hulsteijn

Senior Manager
Phone: +7 (727) 258 13 40
Ext. 2796
Fax +7 (727) 258 13 41
Mobile: +7 (777) 438 4518
E-mail: mvanhulsteijn@deloitte.kz

Sergei Buhanov

Director
Phone:+7 (495) 580-9778
Ext. 3032
Fax: +7 (495) 787 06 01
Mobile: +7 (985) 787 6054
E-mail: sbuhanov@Deloitte.ru

Aituar Akimzhanov

Senior consultant
Phone: +7 (727) 258 13 40
Ext. 2782
Fax: +7 (727) 258 13 41
Mobile: +7 (707) 555 5988
E-mail: aakimzhanov@deloitte.kz

Kazakhstan

36 Al Farabi Avenue
Almaty Financial District
Almaty, 050059
Tel.: +7 (727) 258 13 40
Fax: +7 (727) 258 13 41

Kyrgyzstan

Office 905/906, Business Centre "Russia"
19, Razzakov Street
Bishkek, 720040
Tel.: +996 (312) 39 82 88
Fax: +996 (312) 39 82 89

Tajikistan

Office 307, S.A.S. Business Centre
24A Ayni Street
Dushanbe, 734012
Tel.: +992 (44) 600 62 00
Fax: +992 (44) 600 62 01

Uzbekistan

Inkonel Business Centre
75 Mustakillik Avenue
Tashkent, 100000
Tel.: +998 (71) 120 44 45/46
Fax: +998 (71) 120 44 47

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms. Please see www.deloitte.com/ru/about for a detailed description of the legal structure of Deloitte CIS

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte’s more than 200,000 professionals are committed to becoming the standard of excellence.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.