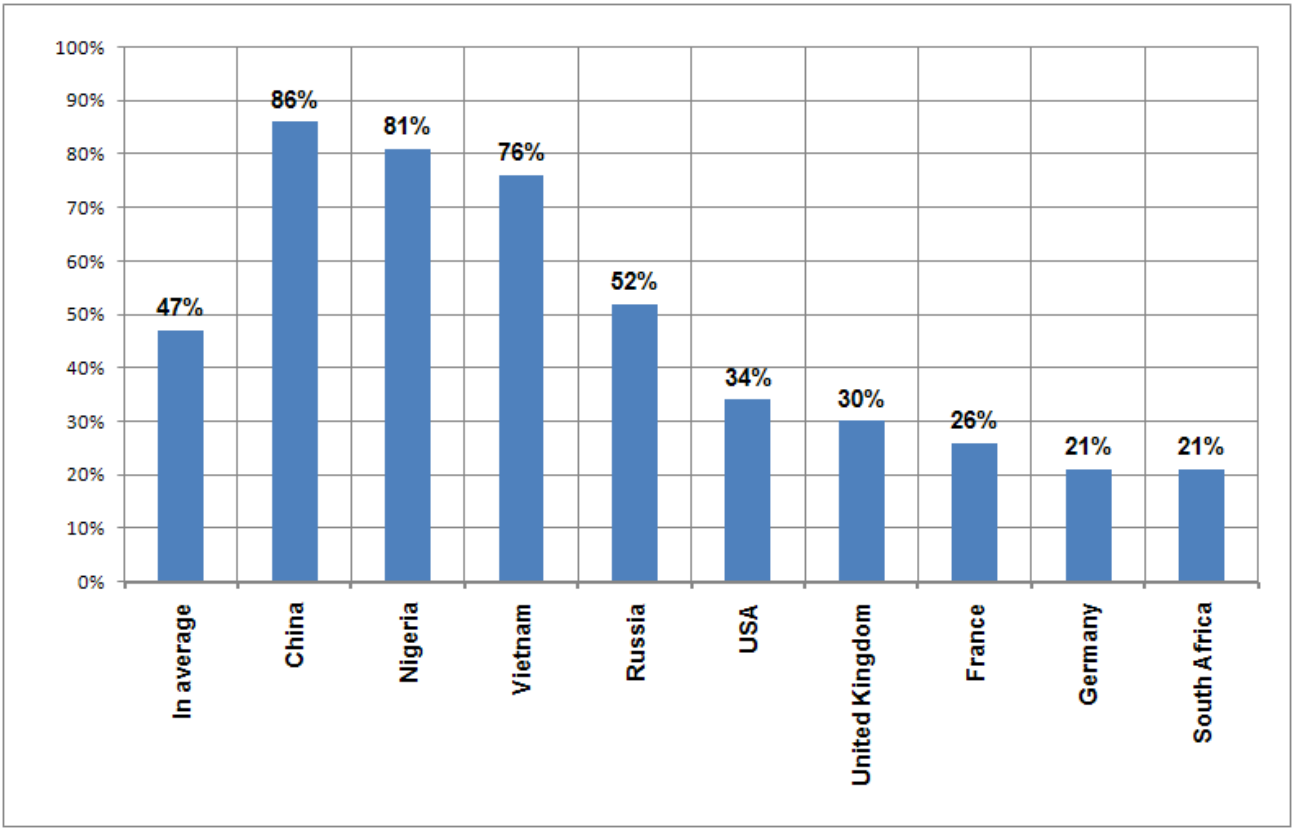
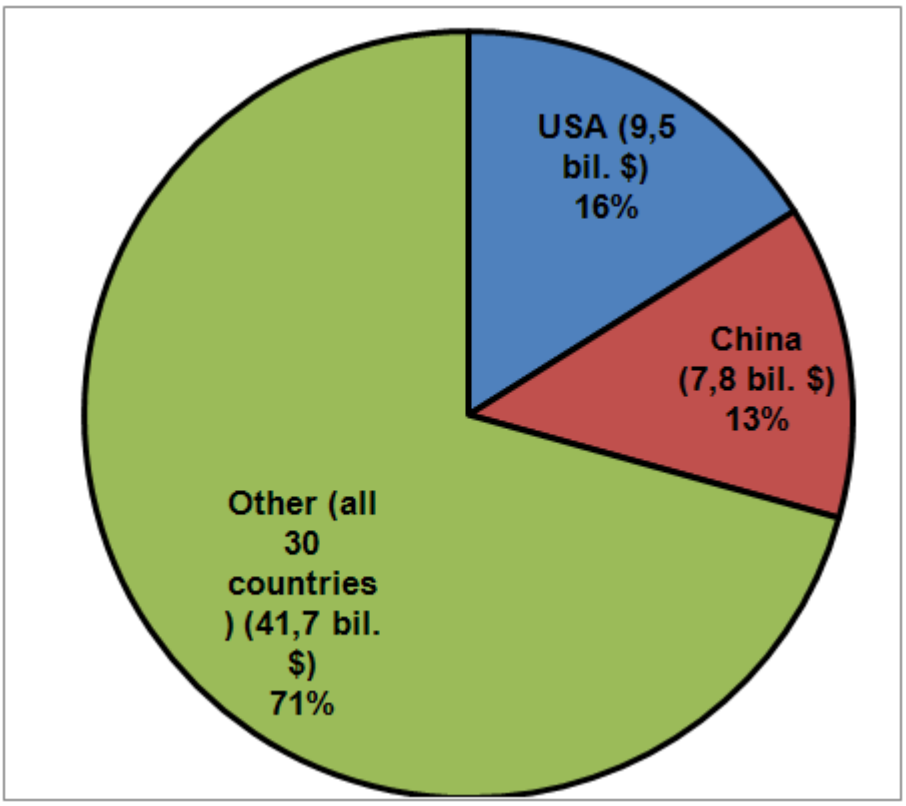
Statistical analysis in area of economic and information security

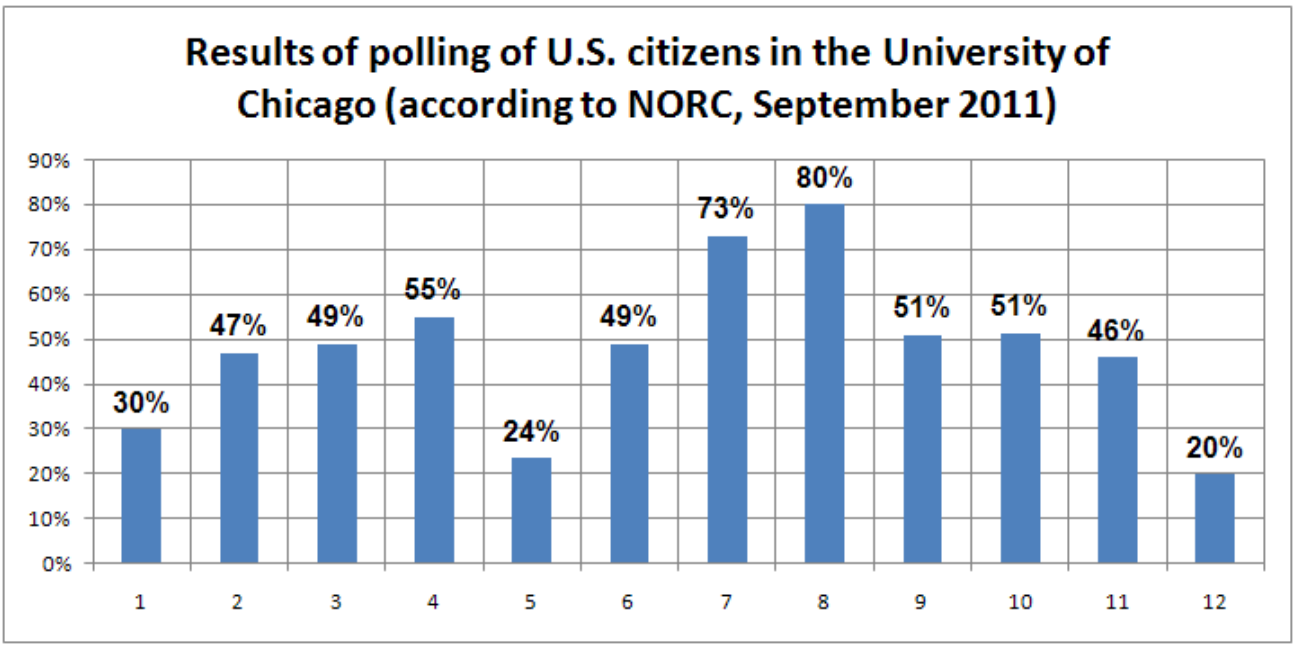
Report (description) of statistical indicators in areas of economic and information security part 1



Number of PC users who use illegal software regularly or from time to time (according to the Business Software Alliance (BSA), September 2011)

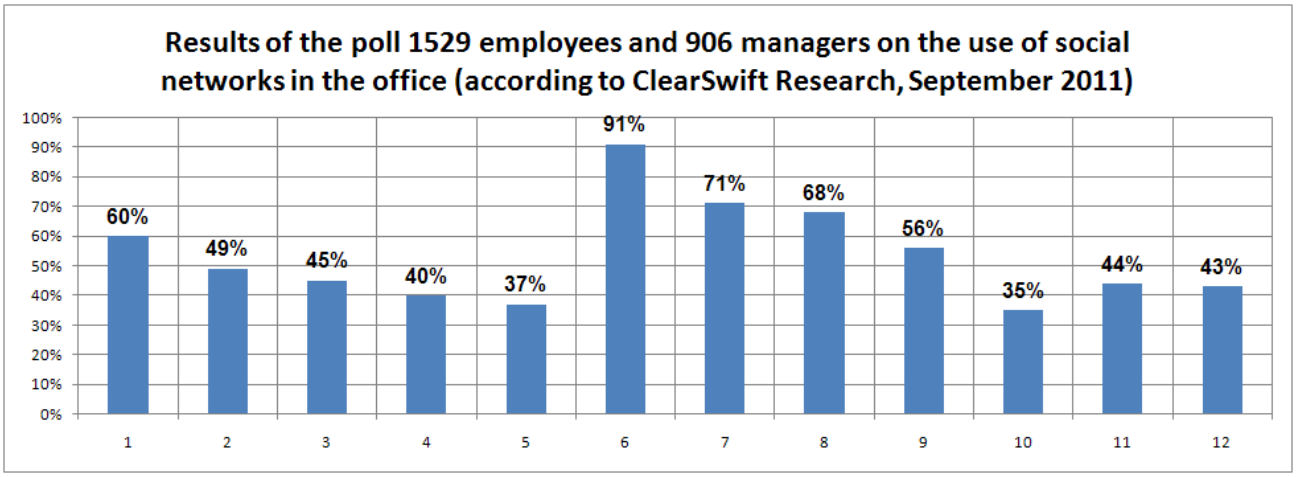


The damage caused by the installation of pirated software in 2010 (according to the Business Software Alliance (BSA), September 2011)

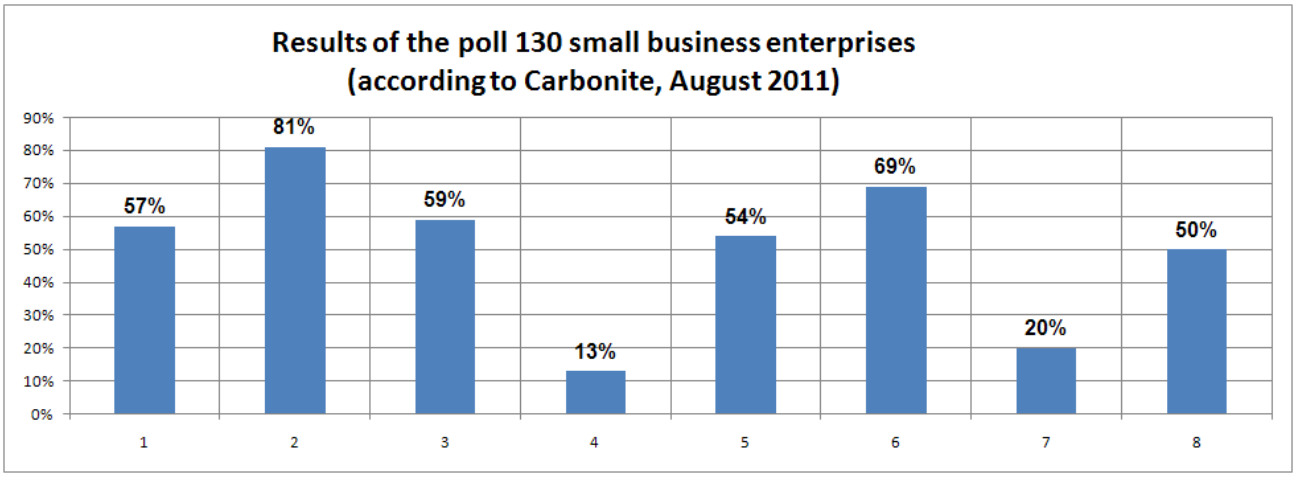


1- positive attitude towards the government to read their mail without permission; 2 - positive attitude to reading the data when it comes to communications addressed to foreigners;3 - Government must be able to browse someone's search history without judicial authorization; 4 - financial records can also be inspected without proper notice; 5 - positive attitude towards the government to listen to their phone calls; 6 - positive attitude towards the government to listen to their phone if calls are sent abroad; 7 - approved the video surveillance in public places; 8 - approved the video surveillance in public places, if respondents have children; 9 - consider torture of

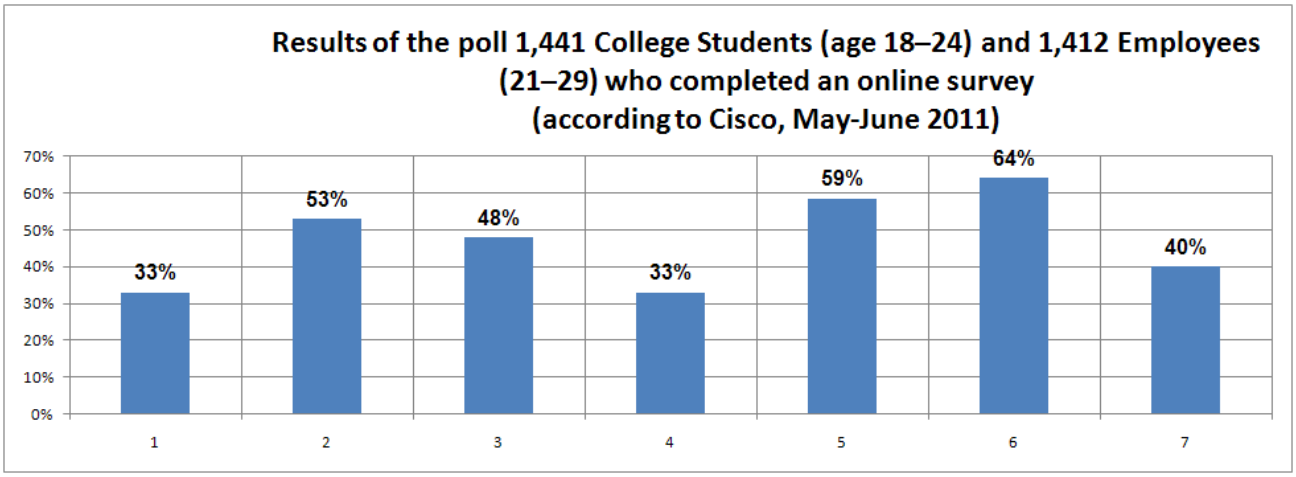
suspected terrorists norm; 10 - approve of "harsh interrogation measures" of suspected terrorists; 11 - considered torture is unlawful; 12 - U.S. is now on the right way



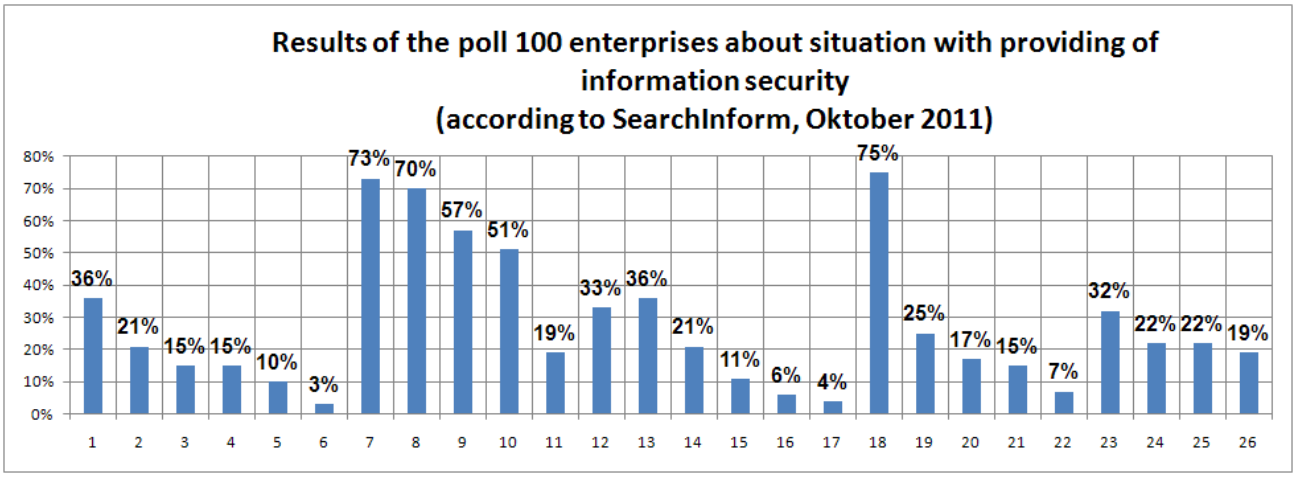
1 - concerned that the free access of employees to Web 2.0, opens free access to viruses and worms; 2 - are afraid of loss of confidential information because of carelessness of employees; 3 - are afraid of loss of confidential information because of hacking; 4 - working worried about decreased productivity; 5 - there is a possible threat to the enteprise's reputation with inappropriate use of networks; 6 - concern about security and fear of loss of information does not allow them to take Web 2.0; 7 - issued tutorial on using of Internet in the workplace; 8 - monitoring activities of employees on the Internet; 9 - have blocked access to certain social networks in the workplace; 10 - 18-24 year olds will be happy to stay at work if they find that the employer has a policy limiting use of social media; 11 - 25-34 year olds will be happy to stay at work if they find that the employer has a policy limiting use of social media; 12 - documented cases of violations of information security that have occurred as a result of using the Internet



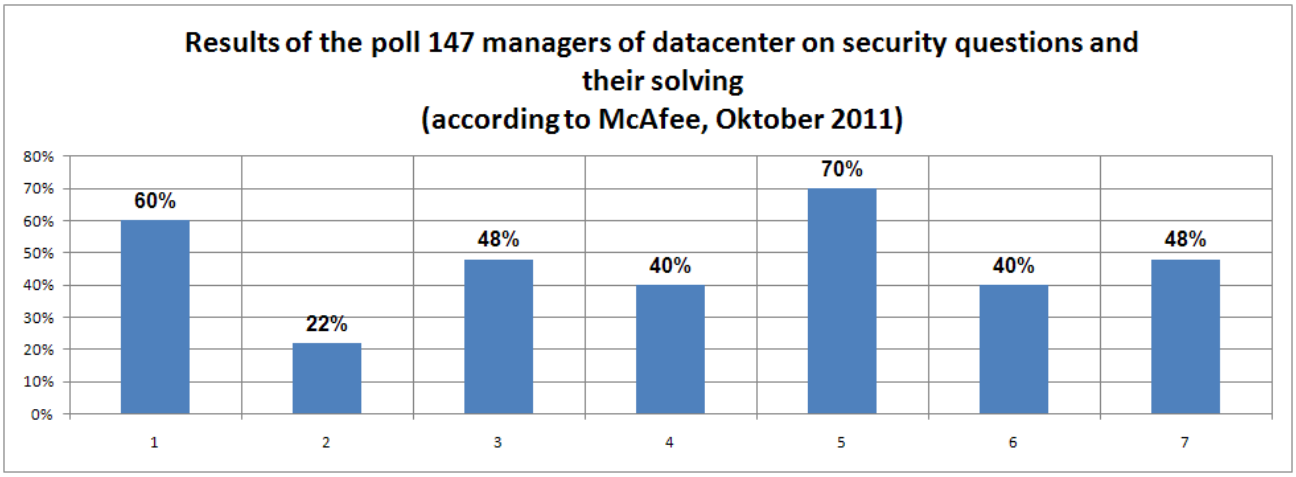
1 - do not have a plan for disaster recovery data; 2 - considered the data to their most important asset; 3 - never thought of data protection; 4 - believe in the probability of falling Database; 5 - no accident databases are not able to affect their business; 6 - think they will suffer financial losses if their business can not function in a single day; 7 - costs classified to the reason that they do not want to buy protection system; 8 - are unable to return to business after data loss



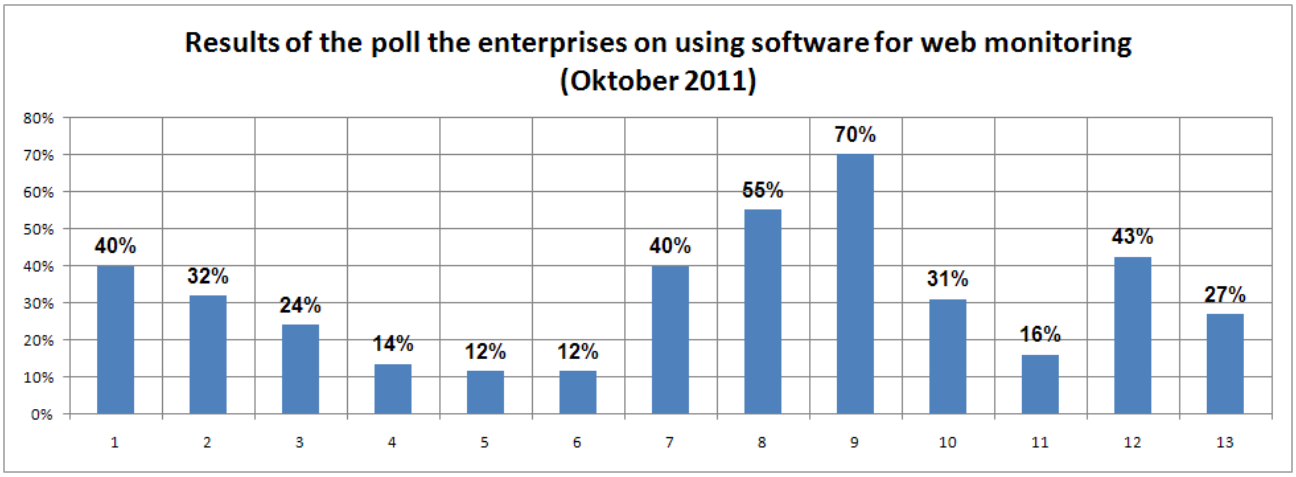
1 - consider the Internet to be as important as air, water, food, and shelter; 2 - could not live without the Internet and cite it as an "integral part" of their lives; 3 - consider the Internet to be _close‘ in importance to water, food, air, and shelter in their lives; 4 - consider the Internet to be as important as these critical needs; 5 - indicate they could not live without the Internet, it is an integral part of their daily life; 6 - would prefer to have access to the Internet versus a car; 7 - consider the Internet to be most important in their daily life



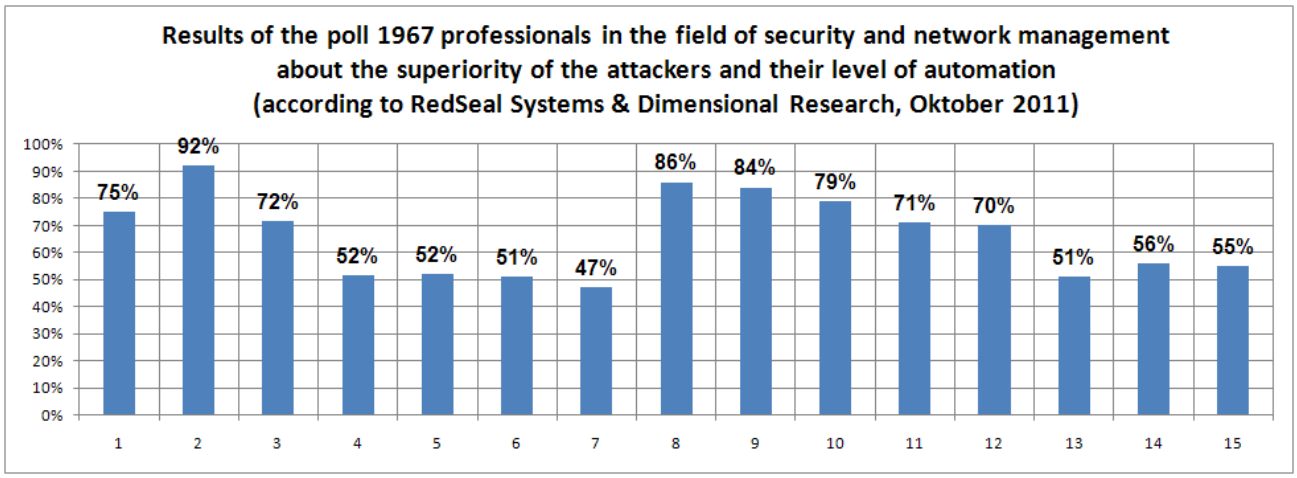
1 – at the enterprise responsible for information security is the IT department; 2 – at the enterprise responsible for information security (IS) is the special department of IS; 3 – at the enterprise responsible for information security (IS) is the department of internal security; 4 – at the enterprise responsible for information security is the direct top management; 5 – at the enterprise responsible for information security is none; 6 – not answer; 7 – conducted training on information security; 8 – do not use the software to prevent data leakage; 9 – there were some in the enterprise of incidents involving leakage of confidential data; 10 – the enterprises are faced with trying to laid-off \ firing employees take with confidential information; 11 – the trying to laid-off \ firing employees take with confidential information was not; 12 – be segregated from the use of certain data transfer channels; 13 – social networks prohibit; 14 – prohibit ICQ and Skype; 15 – prohibit e-mail; 16 – prohibit the use of USB-devices; 17 – prohibit visiting certain sites; 18 – has established control over the channels that are not prohibited; 19 – has established control of external data carriers; 20 – has established control over e-mail; 21 – has established control over HTTP; 22 – has established control over the documents you print from now; 23 – does not provide sanctions for incidents of violation of corporate security policies; 24 – provides a fine or deprivation premiums; 25 – provided for layoffs; 26 – provided reprimands



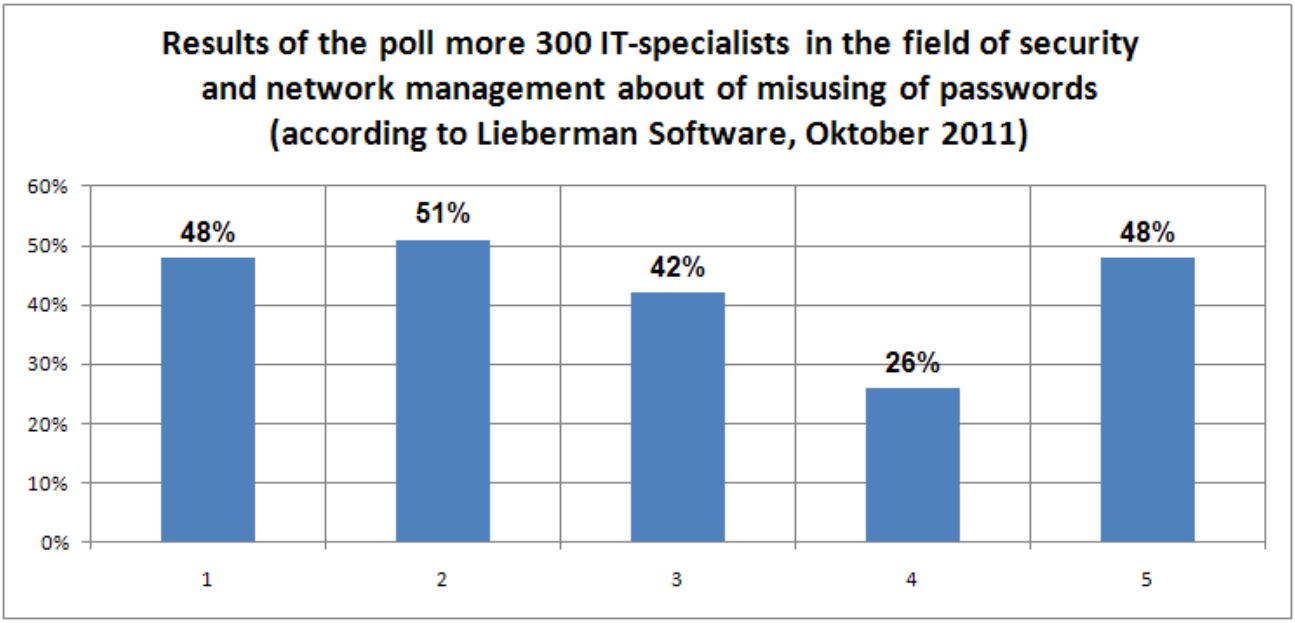
1 – the company management believes that the security is stronger than it really is; 2 – the company management knows about the true readiness of the security services; 3 – are constantly finding new security holes; 4 – performance security system of their organization behind the rate of propagation of threats; 5 – skeptical about the public "cloud" security; 6 – current security does not match standards required by their official policy; 7 – believe that virtualization and private "cloud" computing environment is a unique security challenge



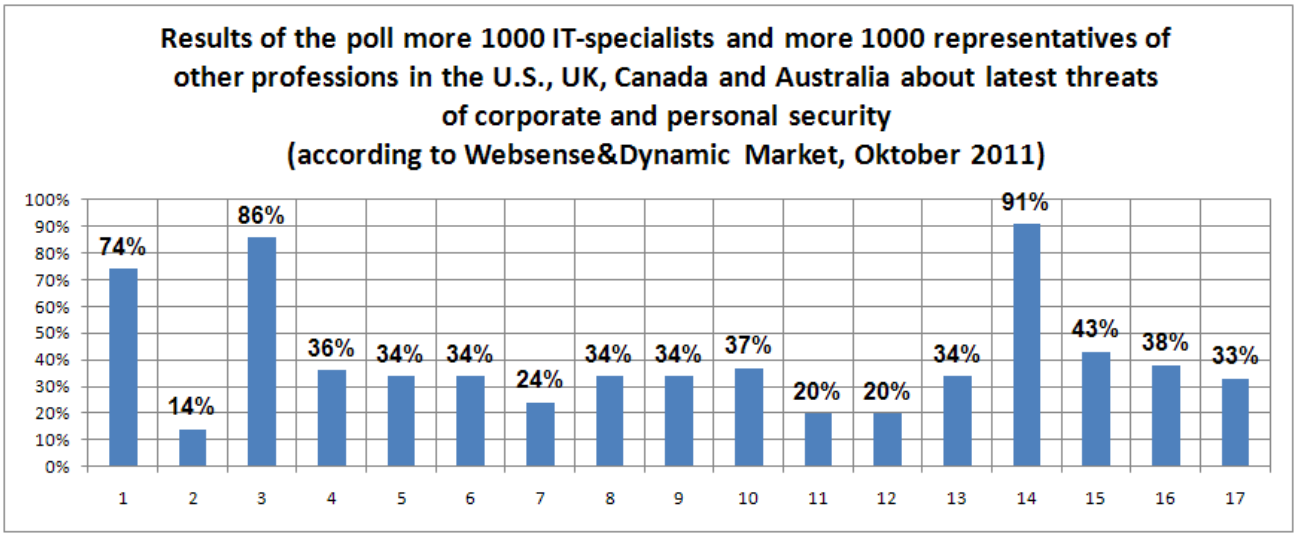
1 - enterprises suffered from a security breach because of unprotected web surfing, 2 - enterprises have not developed policies to control the use of social networking sites, 3 - using software for web monitoring to ensure productivity of their employees, 4 - use software for web monitoring to save bandwidth and speed of networks, 5 - use software for web monitoring to prevent employees visiting inappropriate websites, 6 - do not use software for network monitoring and filtering, 7 - enterprises have experienced any security breaches as a result of the opening employees of sites containing malware as a result of downloading infected files, as well as the actions of malicious code, 8 - enterprises using software for network monitoring is not considered an essential part of their protection from infected sites, 9 - enterprises that do not use software to filter and network monitoring, claim that they have no problems with the use the network, 10 - do not have any policy regarding the use by social networks such as Facebook and Twitter, 11 - have a similar policy, but there is no way to see to it whether employees adhere to this policy, 12 - have no way of assessing the security of a site based on its reputation, 13 - interested in the possibility of assessing the security of a site based on its reputation



1 - are sure that automated tools allow hackers to advantage in evading security systems that are used by most enterprises to protect their critical assets and data, 2 - their employers, which are likely to be big organizations can not provide the necessary level of protection because of their inability to determine where their systems are holes, 3 - admitted that their network exposed to external threats because of improper configuration problems that are present in the infrastructure of security devices, 4 - had no idea how many internal hosts of their organizations were "exposed" to the Internet, 5 - their initiatives for the control of vulnerability would not allow them to place the correct methods to prioritize based on the probability of real attacks, 6 - are the people responsible for a network containing 100 units or more, 7 - their employers and follow the advice to use a metric approach, 8 - employees of energy companies believe that hackers are more advanced toolkit, 9 - Government officials believe that hackers are more advanced toolkit, 10 - employees of telecommunications companies believe that hackers are more advanced toolkit, 11 - health workers believe that hackers are more advanced toolkit, 12 - employees of the financial services industry believe that hackers are more advanced toolkit, 13 - directors of information security do not believe or do not know what tools to assess vulnerabilities provide the amount of information that is needed to identify the major risks to the security systems, 14 - directors of information security have been told that they either have no effective way to measure the effectiveness of security systems or they do not know of their existence, 15 - network management employees were told that they either have no effective way to measure the effectiveness of security systems or they do not know of their existence

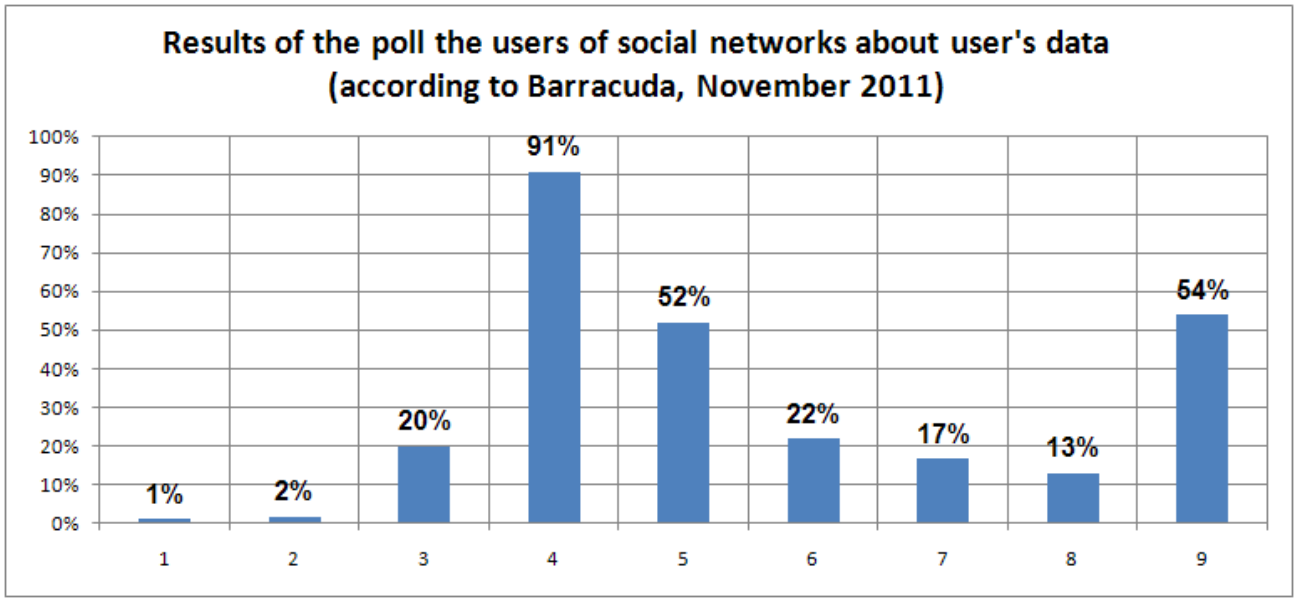


1 - interviewed experts in IT security are working for the organization, whose network has been compromised by hackers, 2 - respondents have 10 or more passwords used in the work, 3 - respondents said that their organizations, IT staff is divided with one another and password access to systems and applications, 4 - respondents said they were aware that some members of the IT staff abuse their privileged position in illegally obtaining access to important information, 5 - respondents work in companies that do not change their privileged passwords within 90 days

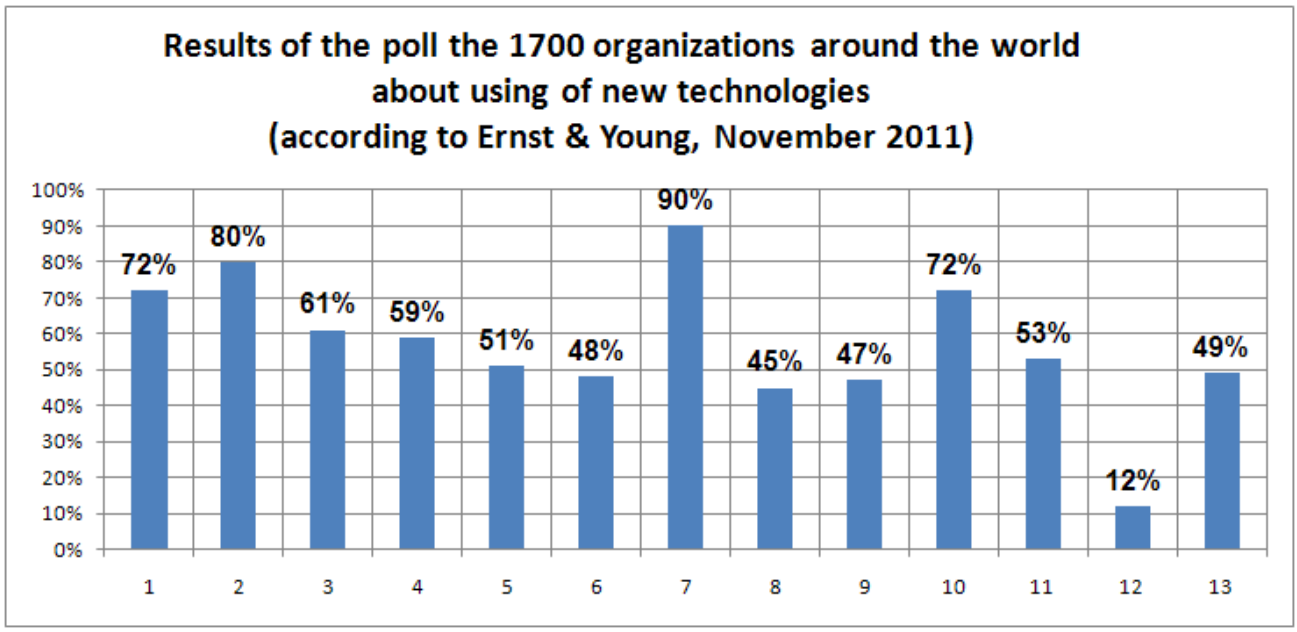


1 - data protection company causes more stress than a divorce, the payment of a debt or a minor accident; 2 - job loss would be less stressful for them than the ranking of current position; 3 - their career be at risk, if there is an incident with breach of security, including cases of leakage of confidential data belonging to the directors; 4 - their career be at risk, if there is an incident with breach of security, including cases of leakage of confidential data belonging to other managers; 5 - their career be at risk, if there is an incident with breach of security, including cases of leakage of confidential data are required to perform specifications; 6 - their career be at risk, if there is an incident with breach of security, including cases when confidential information will be posted on social networking sites; 7 - reported that they have leaked data belonging to the directors or other governing persons; 8 - said that there was a leak of data required for regulatory compliance; 9 - reported that the confidential data been published on social networking sites; 10 - declared that there

were cases of data loss employees; 11 - asserted that data related to compliance were at risk; 12 - seen confidential information on social networking sites; 13 - not reported to the heads of of the random loss of data; 14 - reported that the new levels of leadership involved in last year's meeting dedicated to protection of data; 15 - reported that the heads of IT departments were involved in last year's meeting dedicated to protection of data; 16 - reported that administering were involved in last year's meeting dedicated to protection of data; 17 - reported that the CEOs of the companies involved in last year's meeting dedicated to protection of data

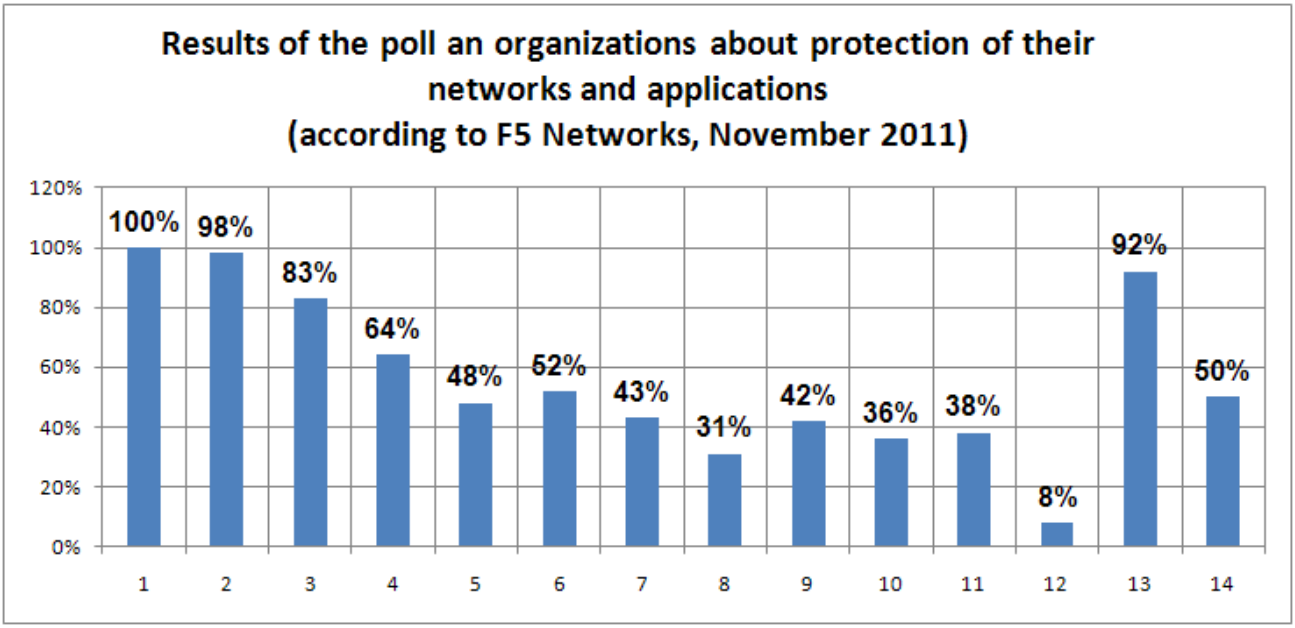


1 - number of tweets that are by malicious; 2 - number of messages Facebook, which are by malicious; 3 - number of companies that prevent the use of LinkedIn employees at work; 4 - number of users that received spam through social network; 5 - number of users that were phishing attacks; 6 - number of users that received malware; 7 - number of users whose accounts are used to send spam; 8 - number of users whose accounts have been captured or were stolen passwords; 9 - number of users who are dissatisfied with the privacy policy on Facebook

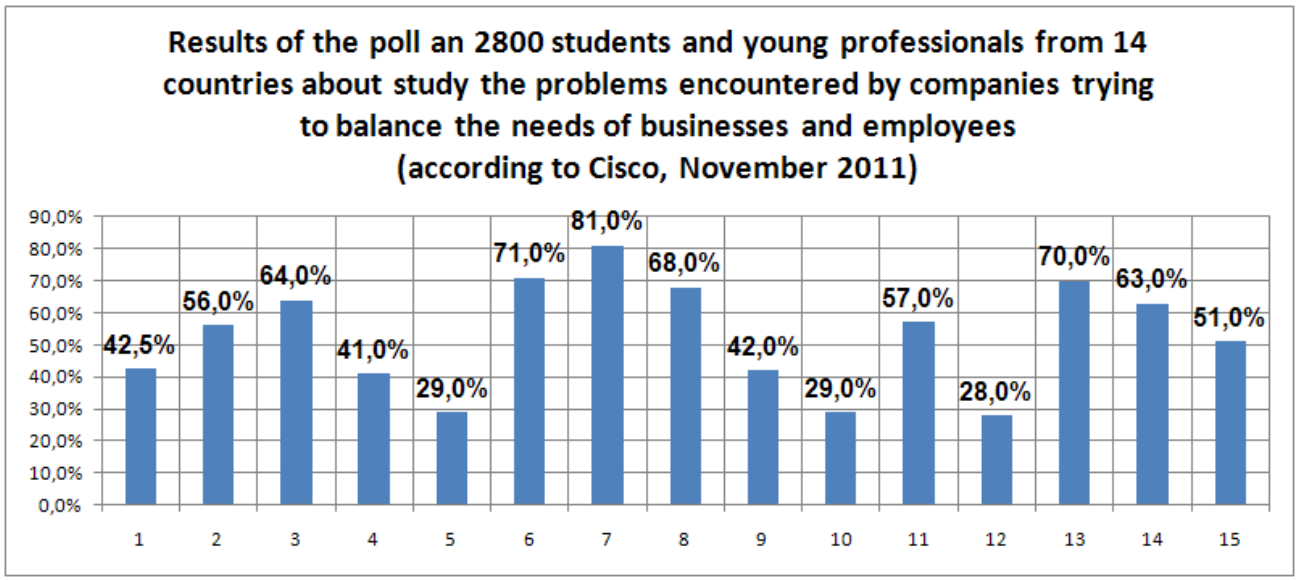


1 - The number of users who are aware of the growing risk level of external threats; 2 - The number of organizations that use or intend to use tablets; 3 - The number of organizations that use or intend

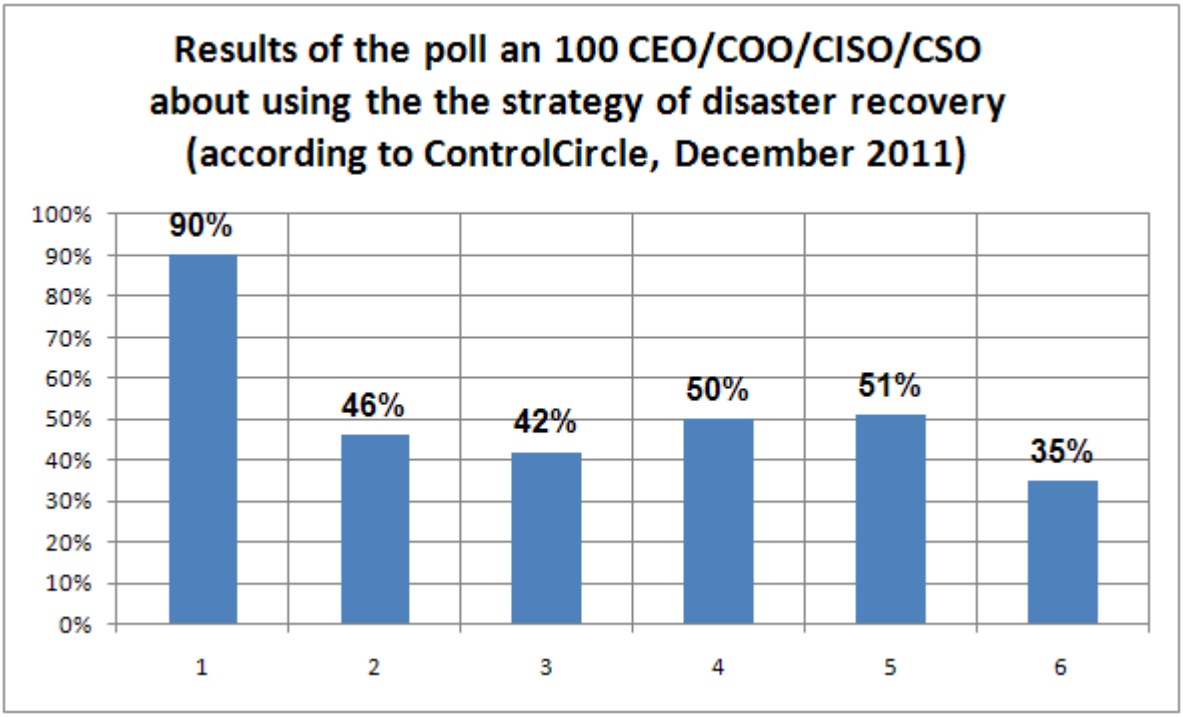
to use cloud computing services; 4 - The number of organizations that are planning to increase expenditures on information security; 5 - The number of organizations who said they owned the documented strategy for information security; 6 - The number of organizations who felt that the introduction of cloud computing - a complicated process; 7 - The number of organizations that prefer an external certification; 8 - The number of organizations that claim that it should be based on specific standards; 9 - The number of organizations that use encryption techniques; 10 - The number of organizations that have declared that they care about most external attacks; 11 - The number of organizations that block access to social networking sites; 12 - The number of organizations that discuss issues of information security at every meeting; 13 - The number of organizations that have stated that the information security function coincides with the priorities of the organization



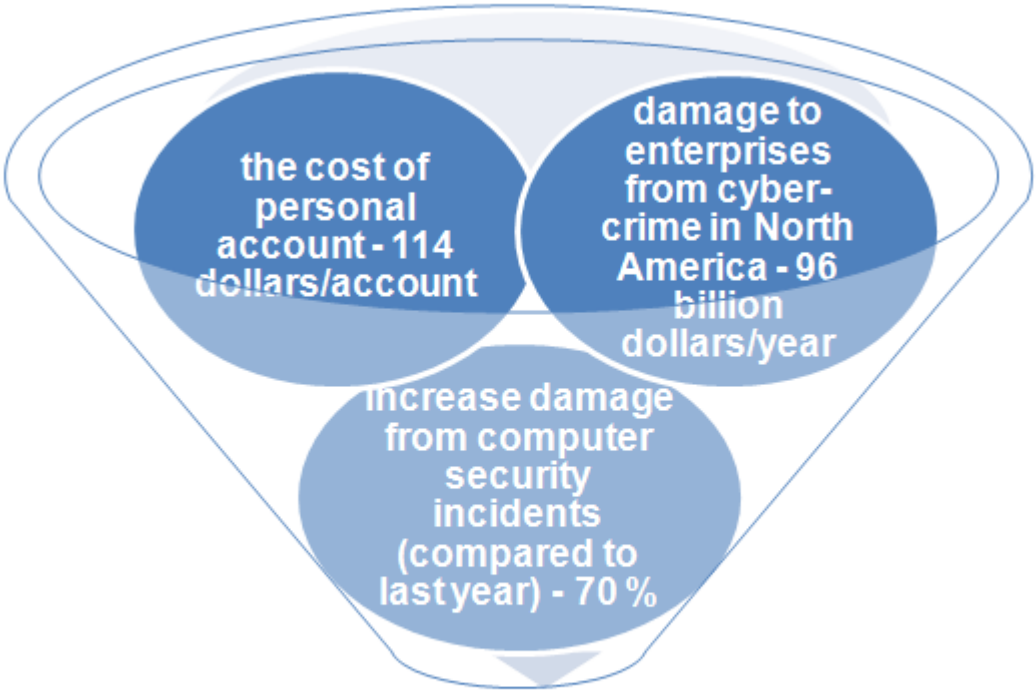
1 - complexity (or importance) of cyber-attacks directed to DNS; 2 - complexity (or importance) of cyber-attacks directed to Network layer DoS; 3 - complexity (or importance) of cyber-attacks directed to Access of encrypted data; 4 - complexity (or importance) of cyber-attacks directed to Misconfiguration; 5 - complexity (or importance) of cyber-attacks directed to App layer DoS; 6 - number of respondents who reported a decline in productivity; 7 - number of respondents who reported a loss of data; 8 - number of respondents who reported a loss of profits; 9 - number of respondents who recorded a firewall failure because of intensive network DoS-traffic; 10 - number of respondents who recorded a firewall failure during DoS-attacks at the application level; 11 - number of respondents who believe that traditional methods of protection provides security at least "not very good" in the understanding of network traffic and protect against complex blended threats; 12 - number of respondents who believe that their traditional security tools are robust enough and see no need to apply ADC; 13 - number of respondents who see the special role of ADC in ensuring the security; 14 - number of respondents who believe that the ADC can replace most traditional means of security



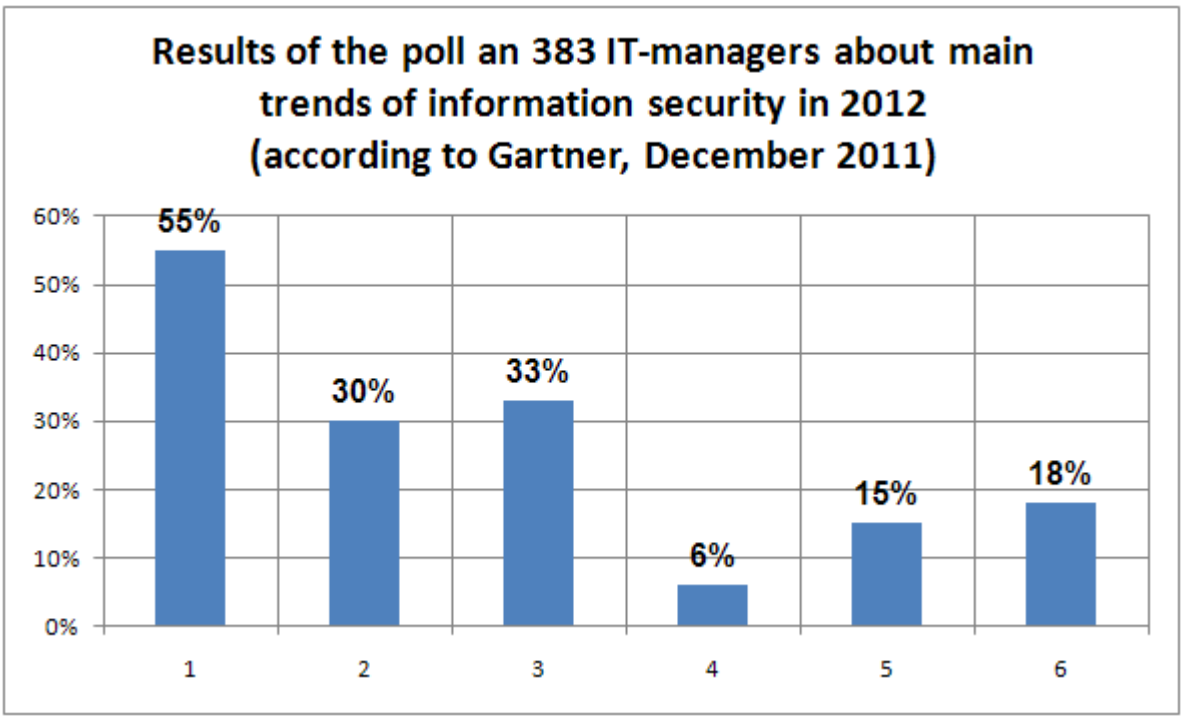
1 - number of respondents who choose the company with a lower salary, but with greater mobility, freedom of choice of electronic devices and access to social networks; 2 - number of respondents who said that if the employment they find that access to social networking closed, or then they will not agree to work in that company or they will seek ways to circumvent the ban; 3 - number of respondents who are planning raise the question of policy of access to social networks during an interview with the employer; 4 - number of respondents who said that their companies have agreed to make concessions on access to social networks and free using electronic devices for the purpose of their employment; 5 - number of respondents who said that the lack of remote access can lead to a decision on dismissal, reduction in work efficiency or refusal to offer a potential employer; 6 - number of respondents who believe that companies should allow the use of corporate electronic devices for both work and for personal purposes because "communication at work" and personal communication are closely intertwined; 7 - number of respondents who want to select same device for use at work; 8 - number of respondents who believe that companies should allow them access to social networks and personal sites from computers working; 9 - number of respondents who believe that companies should show more flexibility and understanding to their needs to stay connected through social networks and personal sites; 10 - number of respondents who believe that to be able to work remotely on a flexible schedule - rather their right and not privilege; 11 - number of respondents who can connect to corporate networks from remote locations several; 12 - number of respondents who are able to do so at any time in any place; 13 - number of respondents who did not see the need to constantly be present in the office except for important meetings; 14 - number of respondents who would like to have access to the corporate network from home computer; 15 - number of respondents who would like to have access to the corporate network from personal mobile devices



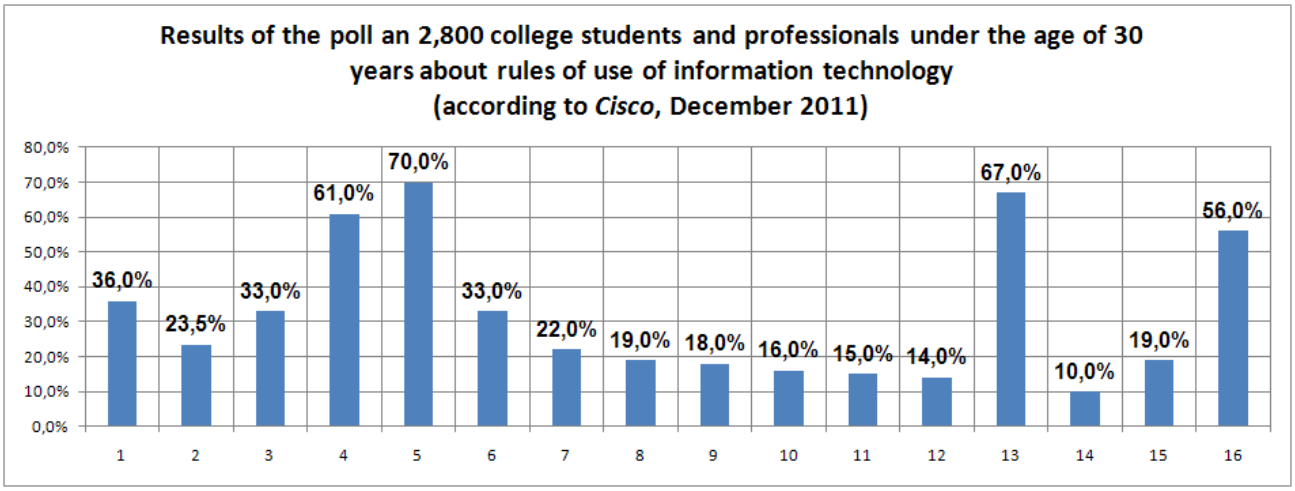
1 - respondents have disaster recovery strategy; 2 - respondents checked and tested their business continuity procedures in the last 12 months; 3 - respondents either did not have a strategy, or they are not sure when it was tested last time; 4 - respondents have a strategy in which 2 years and more; 5 - respondents reported that the recovery after a crash or system failure, will take several hours; 6 - respondents admitted that they had leaves more than 24 hours to return all systems to normal mode functioning



The reference data in area of information security



1 - respondents reported that their budgets will remain the same in 2012; 2 - respondents confirmed that their budgets will remain the same in 2012; 3 - respondents expect to increase their budgets in 2012; 4 - respondents expect to increase IT-budget by 5% or more in 2012; 5 - respondents the previous year said they expected to reduce IT-budget in 2012; 6 - respondents admitted that they are not PCI-compliant (Payment Card Industry Data Security Standard (PCI DSS))



1 - respondents do not respect your IT department; 2 - respondents in the age of 30 becoming victims of theft of personal data; 3 - respondents (college students) are not afraid to transfer personal information over networks; 4 - respondents believe that responsibility for data protection and device is not for them, and for IT departments and telecom operators' 5 - respondents who are familiar with the rules of corporate IT, acknowledged that violate these rules, more or less regularity; 6 - respondents did not see there is nothing wrong; 7 - respondents stated that access to unauthorized programs and applications they need to perform their professional responsibilities; 8 - respondents acknowledged that corporate IT rules in their companies are not respected; 9 - respondents said that during the work they did not before having to think about these rules; 10 - respondents believe such

rules are uncomfortable; 11 - respondents about corporate IT rules simply forgotten; 12 - respondents to justify their behavior so that the heads of them still do not follow; 13 - respondents believe that IT-rules is necessary to change in order to reflect contemporary realities of life that require greater flexibility in the workplace; 14 - respondents mentioned the fact that corporate IT rules forbid the use of the iPad and other tablet PC; 15 - respondents said they access the Internet through a neighbor's access point without the knowledge and consent of the owner; 16 - respondents said that they allow an outsider: family, friends, colleagues and even strangers - an uncontrolled use of their computers