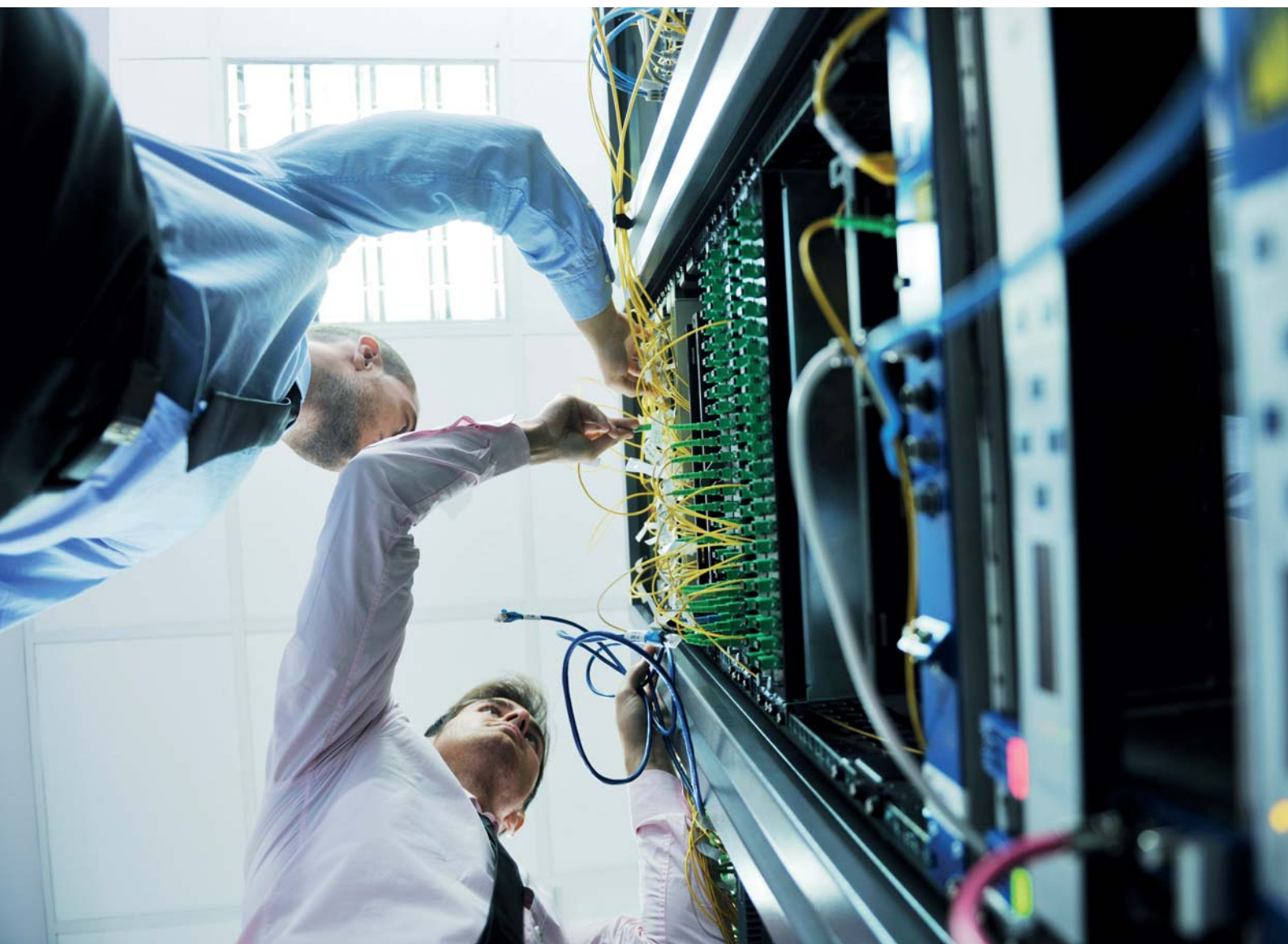


January 2016

In Defense of Digital Borders

or 5 tips on how to meaningfully strengthen
a company's security against CYBER risks



www.pwc.pl/badaniebezpieczenstwa



Plentzia
Kabilizes
Etxebarri
Basantzi

Plentzia
Kabilizes
Etxebarri
Basantzi

PLENTZIA

↑

↑

↑



Dear Reader,

The ever-changing business environment and the development of technologies require that leaders in the organizations make right decisions to ensure a competitive advantage. But do the leaders remember that their positions connect to the confidence in the way the information is managed and how effective customer data protection is?

We live in an age of cyberattacks and the crisis of confidence. What does matter is to be able to provide a quick and efficient response to incidents, one which synchronizes technology, legal actions and communication management. Cybersecurity has ceased to be a trend and has become a strategic necessity.

What are the current concerns of Polish companies and what cyber attacks and security breaches do we note? 31 per cent of our respondents have indicated that the incidents were related to the disclosure or modification of data. In 33 per cent of cases that translated into financial losses, losses of customers,

or litigation for a breach of information security. The reputation damage was also often mentioned as a consequence of attacks: 16 per cent of Polish companies have reported this problem. Companies which engage in the digital transformation build their business models on the basis of technology and solutions, and open up new revenue streams. Quite often such revenue streams go beyond their current fields of activities or even beyond their sectors. This requires a comprehensive approach which will cover not only a strategy, but also its effective implementation and risk monitoring.

As a result of making a comparison between the activities of Polish companies and those across the world and having analyzed the trends, we have come up with five tips for companies for an effective prevention of cyber-risks. We are confident that they will provide you with inspiration and will support the development of security strategies in your organizations.

Piotr Urban

Partner
Risk Assurance Leader for Poland
Cybersecurity and Privacy
Leader for CEE

Adam Krasoń

Chairman of PwC in Poland



Table of Contents:

<u>Tip 1.</u>	Take proportionate actions, or how doing the minimum is no longer enough	6
<u>Tip 2.</u>	Take a look at your closest environment first	10
<u>Tip 3.</u>	Get ready for something new	12
<u>Tip 4.</u>	Engage the highest rungs	14
<u>Tip 5.</u>	Look for an external support	18
	Methodology	23
	Contact details	24

Development of new technologies is one of the five global megatrends which shape our current reality. Computer systems which support multi-domain management evolve really fast. This development, however, has also brought about new threats. Compared to the previous year, the number of the reported information security breaches has grown worldwide by 38 per cent. This is what the PwC's "Global State of Information Security 2016" survey indicates. Studies in Poland which were conducted for this report show that in our country the percentage was even higher, and amounted to 46 per cent.

The scale of the problem also shows through the number of the attacks. On average, there were as many as 126 cyberattacks on each company in Poland. And half of our surveyed companies reported more than 6 cyber incidents.

How do Polish companies react to these statistics? The research shows that 65 per cent of respondents believe that they have got effective cyber security measures. And it is still a moderate level of optimism vis a vis the results of the PwC's "Digital IQ" study of 2015, in which 88 per cent of respondents said that their companies thoroughly analyzed potential security risks and privacy concerns in digital technology projects. The conclusions of our simulation of attack scenarios on Polish companies also remain as they were. On average, the time taken to gain an unauthorized access to systems and data remains to be 4 hours. Also, only one in a hundred companies which were tested found out that it was a target of an attack.

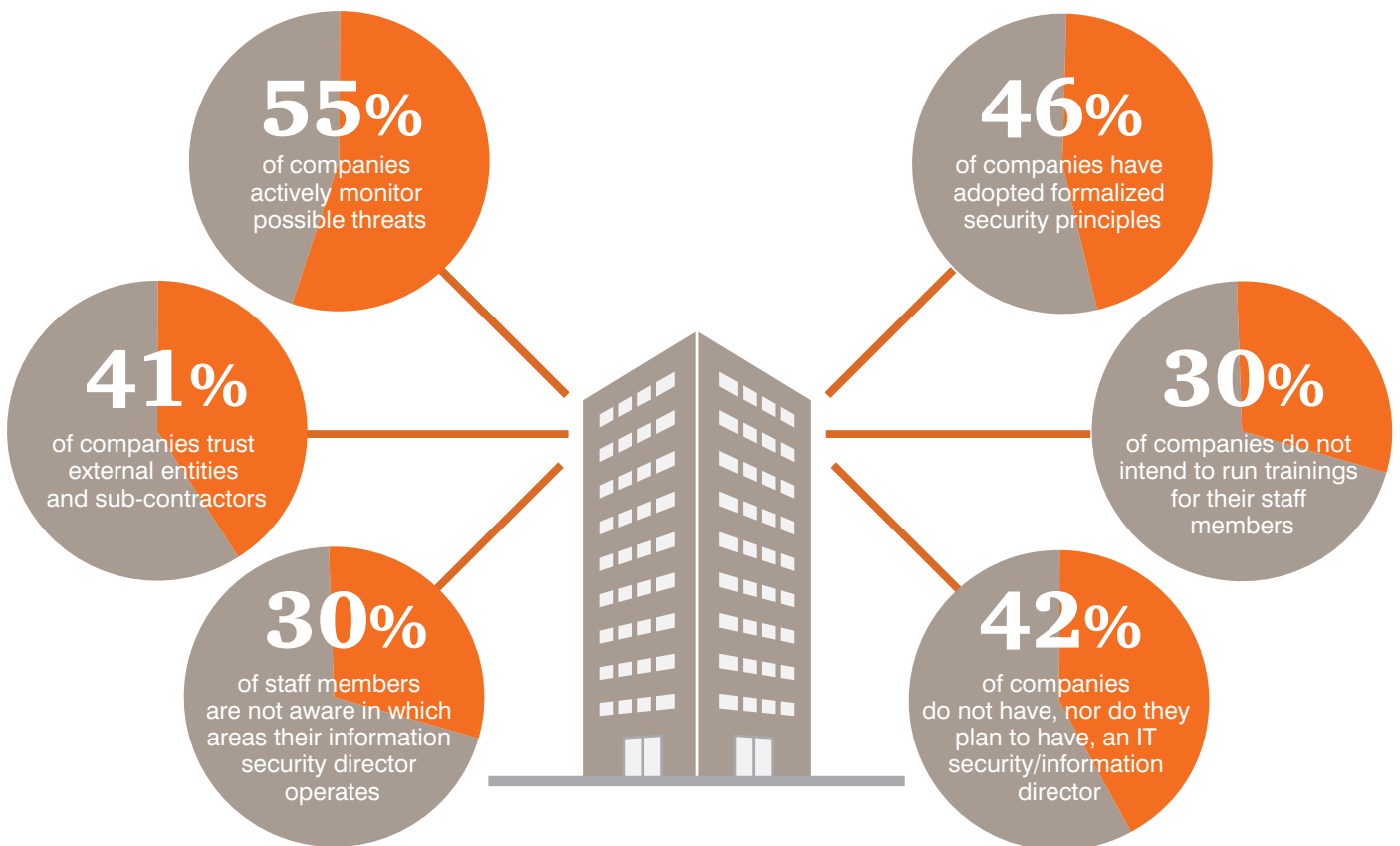
Until recently, the focus of cybercriminals has primarily been the financial sector.

But more and more often their victims are now companies from the industrial or energy sectors. Process control systems (SCADA/ICS) make an easy target, especially that often their original design did not fully encompass their integration with the IT environment. In the time of the tense geopolitical situation a possibility of exercising remote control over the enemy critical infrastructure becomes one of the weapons in the cyber-arsenal. Cases of such attacks on Polish companies were already observed in 2014, and at the end of 2015 there was a widespread failure of the power distribution system in one of our neighboring countries, which was most likely caused by a hacker attack, possibly by the Energetic Bear, that is the same group who was behind the attacks in a previous year. Production systems are particularly susceptible to cyber attacks because of their long lifecycles and their main focus on their availability and high utilization. It is worth verifying to what risks they are exposed and what is a way to possibly reduce them.




The level of maturity of Polish companies

These days activities which focus merely on compliance are not enough to protect a company's reputation and its customers' data



Tip 1. Take proportionate actions, or how doing the minimum is no longer enough



13%

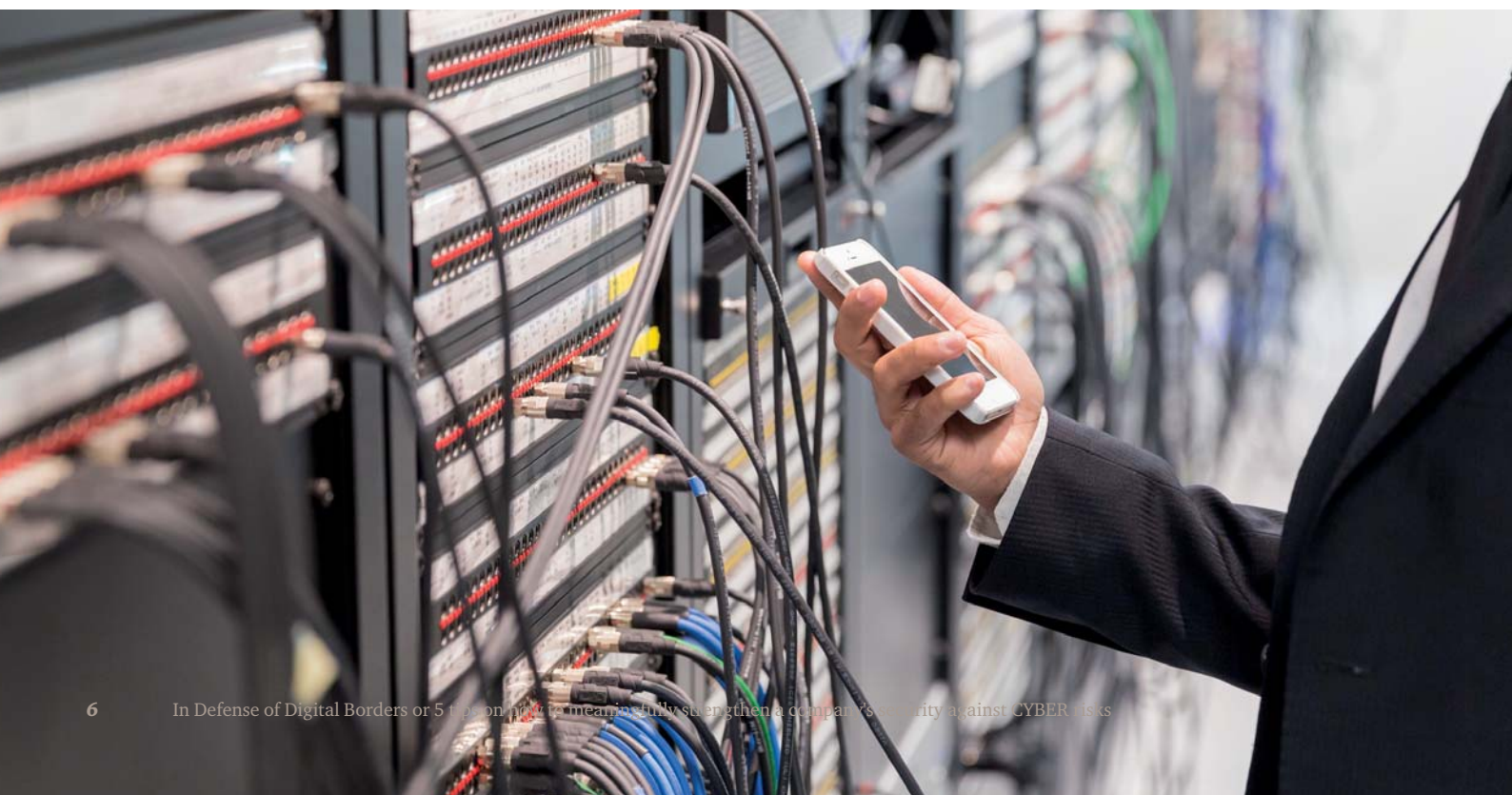
of companies do not have a person responsible for information security

Well, things used to be easier already, and are not any longer. These days the forecasts supported by the data from the recent years unequivocally state that:

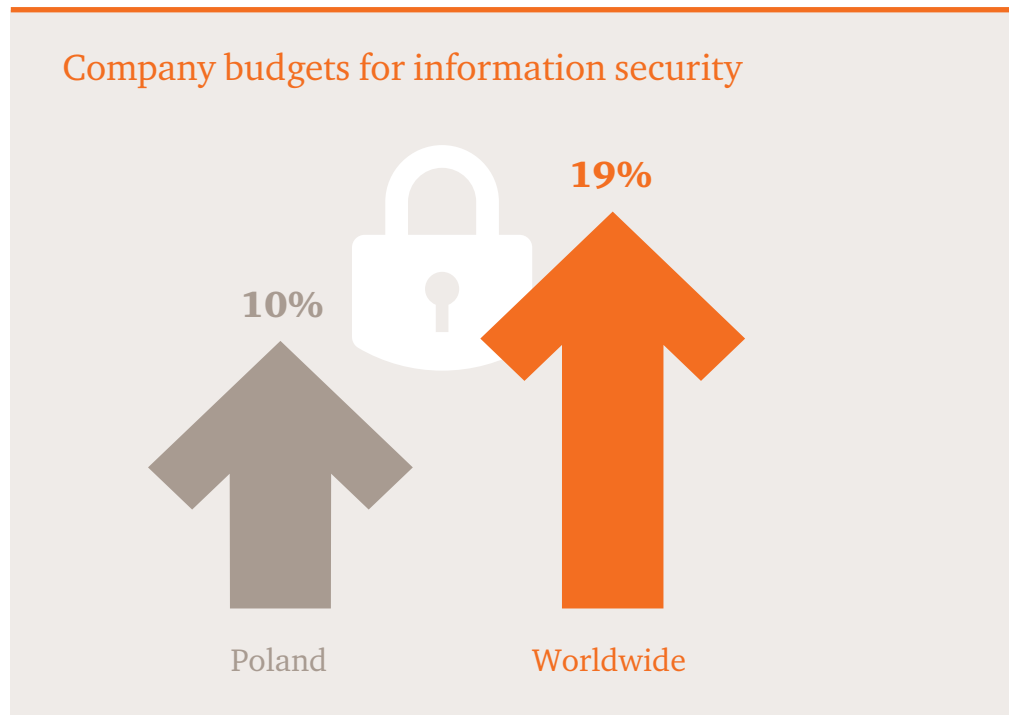
- the risk level will continue to increase. Looming cyber threats will cause losses such as destroying one's reputation, intellectual property, or competitive advantage,
- the threats may also limit one's ability to provide services. They will expose organizations to criminal or financial liabilities, and they will cause serious damages to reputation which will result in losses of customer confidence. In such a situation it will be necessary to take actions which go beyond basic cyber security activities as required by law.

According to the results of the study, in many companies cyber threats are still not high enough on the agenda of their Boards. It is especially surprising in the context of the results of the "PwC CEO Survey 2015" global study, which was addressed to leaders of companies.

CEOs of global companies stated that cyber security threats were the second most important risk that could jeopardize their businesses. Meanwhile in Poland, the main activities in this area are often focused only on achieving compliance with statutory requirements, which are primarily related to the protection of personal data. This approach has been confirmed in respondents' replies to our survey. 13 per cent of the respondents said that no one was responsible for the information security in their companies, and one in every three respondents claimed that only one employee was responsible in the entire organization. When the level of threats increases, it is important that companies hire or outsource support, if they already have got no such specialists on their own. And companies which do have such teams ought to think of expanding them in the future. Our recommendation is directed especially at 42 per cent of the respondents whose companies do not plan to employ any IT/information security manager.



However, some organizations are aware of the scale of the existing threats. This is confirmed by the declared level of expenditure for the IT security. Nearly half of the respondents have said that their businesses spend more than half a million zloty in this area. The share of such expenditure in the overall IT budget has increased from 5.5 per cent to 10 per cent, and it is very likely to grow more. It is worth pointing out that in the world, according to the results of the PwC “Global State of Information Security 2016” survey, this proportion has noted an increase to 19 per cent. This trend can already be observed in the subsequent study. So, given the global trends we may still be investing too little, but the trend is positive.



50%

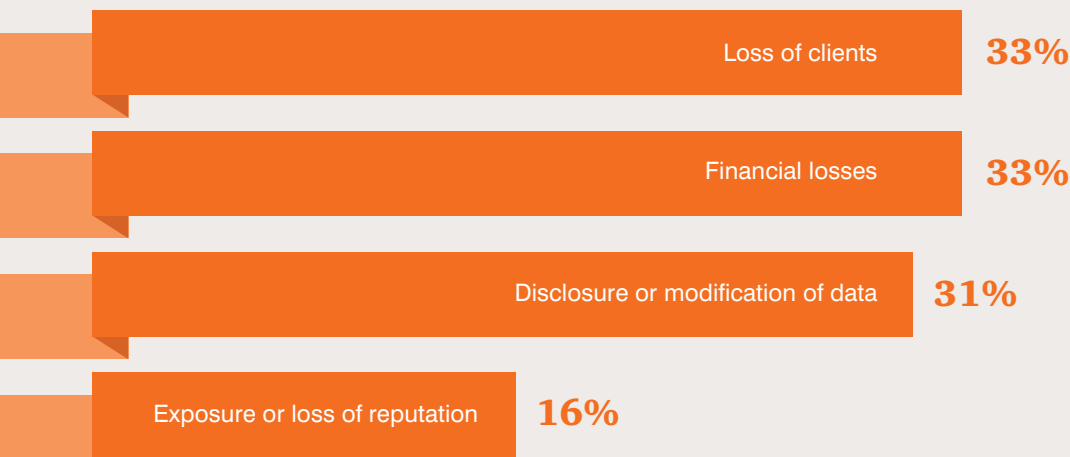


of companies spend
PLN0.5 million
on information security

“Increasing the budget for cyber security is an important and positive moment in any CISO’s career. Unfortunately, as we can see in the cases of spectacular blunders by some global organizations, the answer to the question “in what to invest?” is at least as important as the answer to the “how much?” question. One should always remember that we are not talking about investing strictly in the IT security. We can find challenges in any part of any business where digital technologies are employed: telecommunication, SCADA systems in the power industry, oil and fuel production systems, traffic control systems, medical devices and so on, and many of these areas are very relevant to the company’s operations, but at the same time are much less invested into, cyber security-wise, than the “traditional” IT”.

Rafał Jaczyński – Director, Cyber Security Team for Poland and Central Europe

Consequences of cyber attacks for companies



While not too many companies report six-figure losses, cases do get reported of prolonged (longer than five days) downtimes in business operations. It is worth noting that such downtime in business activities can mean a lot more losses – and in the case of critical infrastructure, may mean irreparable losses across the country.

It is also disturbing that only 46 per cent of companies in Poland are guided by clearly defined formal security rules. Across the world the percentage is almost twice as high, and amounts to 91 per cent. Interestingly, 70 per cent of companies declare that they comply with the requirements of the Act on the Protection of Personal Data.

This means that after several years since the introduction in Poland the Data Protection Act, almost one third of companies have not complied with it and should take urgent action. It is all the more important since the EU intends to implement regulations which could punish companies with a penalty of up to 4 per cent of their global turnover for defaulting with regards to the personal data protection. This pending new EU General Data Protection Regulation will impose even more obligations on businesses. Its implementation will require not only a “reproductive” application of these regulations, but will bring about a requirement to carry out an independent analysis of the possible risks and to adopt appropriate means to secure personal data.

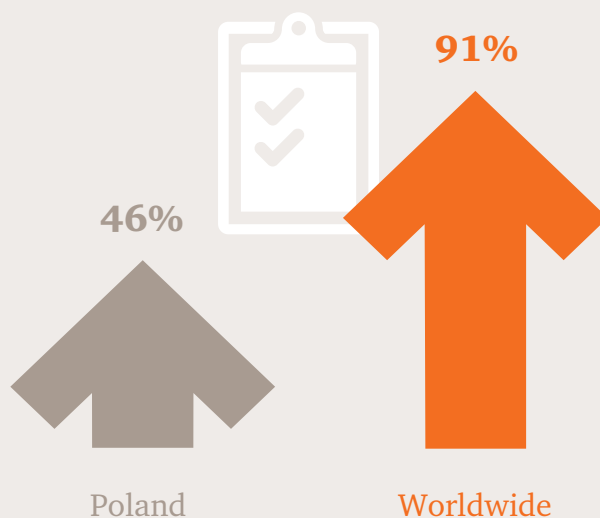
“In December 2015 the EU bodies agreed on the wording of the directive concerning measures to ensure a high common level of network and information security across the European Union (NIS Directive). The aim of the Directive is to provide a common high level of network and information security. The Member States will be required to guarantee a required level of national capacities by setting up competent network and information security authorities, establishing computer emergency response teams (CERTs), and adopting national strategies and plans for networking and information security. The new regulation also imposes obligations on companies. Enterprises in certain critical sectors (electronic communication, providers of services for information society, e.g. e-commerce platforms, online payment portals, social networking sites, search engines, cloud computing services, app stores) and public administrations will be required to assess the risks to which they are exposed and to adopt appropriate and proportionate measures to ensure network and information security. These entities will be required to report to the competent authorities any incidents which seriously threaten their networks and IT systems and which could significantly distort the continuity of critical services and the supply of goods. Also, an obligation to report an incident (with regards to the personal data protection) will be imposed on business entities under the EU General Data Protection Regulation. Companies will have to utilize a number of measures to monitor incidents, prevent them, and respond to the disclosed threats or violations”.

Anna Kobylańska – advocate, counsel at the PwC Legal



companies do not comply with the requirements of the Act on the personal data protection

Companies which have adopted formalized security rules:



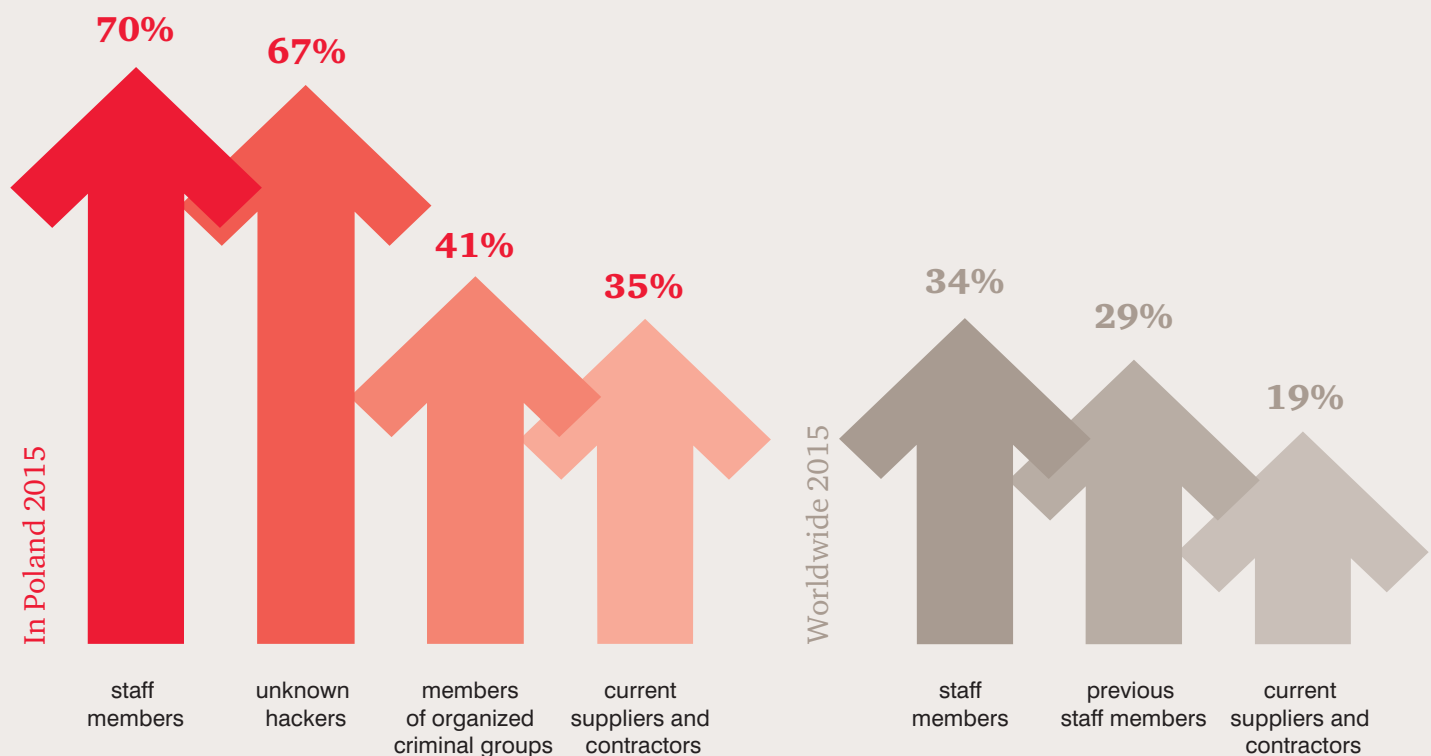
Tip 2. Take a look at your closest environment first

In order to better protect oneself against threats and, above all, to effectively avoid them, it is important to properly identify their sources. Only a thorough analysis can contribute to an effective elimination of negative phenomena. According to 48 per cent of the respondents, the main source of threats in last year's survey were the employees. This year 70 per cent of the respondents have chosen this answer. In the previous year 35 per cent of the respondents said that they were attacked by unknown hackers, and this year the number of such responses almost doubled: 67 per cent of respondents said so.

A similar case was with organized crime: the number of such indications increased year on year from 26 per cent to 41 per cent. The upward trend also shows regarding a threat posed by service providers: an increase from 17 per cent to 35 per cent.

In the world, current staff members in the companies have been identified as the source of threats by 34 per cent of respondents, and 29 per cent of the respondents have indicated former employees. 19 per cent of the respondents said that it was the current suppliers who were the source of threats, and 16 per cent of the respondents said that their business partners were such a source.

Main sources of cyber attacks



70%

companies do not monitor their employees' behavior



Many corporate executives are aware that a significant proportion of the risks originates from the company employees. Despite this, they do not monitor their behavior with a view to eliminate actions which bear the most risks: 70 per cent of the respondents in Poland said so. 60 per cent of the respondents said that they ran trainings for their employees, and 6 out of 10 respondents said that their companies required that external parties adhered to the rules of the security policy.

Although 78 per cent of the companies say that they have an overall security strategies, nearly 30 per cent of companies still do not plan to run any trainings on cyber security. This is important because most of the security breaches regarding information occur in office environments and through social media, as 64 per cent of the respondents confirmed. Employee often mistakenly perceive monitoring of their behavior as surveillance.

At the same time, it happens that employees involuntarily become tools for executing attacks. This can happen if malicious software steals their access data and uses it to perform unauthorized activities in the corporate systems. Efficient monitoring helps detect irregularities and non-standard behaviors which may be the results of a cyber attack.

“Effective monitoring of the ICT environment for security requires a good knowledge of the characteristic features of threats and attacks. They are specific and vary from one company to another. As the forms of attacks develop together with the ingenuity of the attackers and with new vulnerabilities, appropriate monitoring scenarios should also be continually evolving. Devising and implementing an initial monitoring strategy brings us half way towards a success. It is important to skillfully develop mechanisms to be put in place, and to constantly improve them, to adapt them to the risk profile of a given ICT infrastructure and to the risks which keep changing. Monitoring and ensuring security is a process, not a one-off investment. For big companies it is often crucial to have a team – a Security Monitoring Center, to be responsible for the day-to-day monitoring, providing adequate responses and enhancing security, including monitoring mechanisms which get devalued during the technological progress and need to be continuously developed. Buying even the best technologies in support of security monitoring without their proper configuration, or without developing them in a sustainable way, or not relevant processes and human resources, is a dead end gives a false sense of security, of which we should be especially mindful”.

Tomasz Sawiak – Deputy Director, Cyber Security Technology Services Team

Tip 3.

Get ready for something new

30%



of companies in Poland use cloud computing

Companies are eager to utilize the opportunities which the new technologies offer them. Unfortunately, they involve many advantages, but at the same time they pose many previously unknown threats which, if unidentified and unknown in time, can pose a risk to the organization.

One of the increasingly common solutions which is used in many business areas is cloud computing. This solution receives various ratings from security and privacy issues specialists. When it comes to security, the benefits of cloud computing are notable. It happens increasingly often that a solution which

is delivered as a service, provides a smaller organization with an opportunity to use security tools which were previously unavailable to it for the reason of costs, such as data analysts, access management, and advanced authentication. High computational power cannot be overrated when large data sets need to be processed. In this context, one needs to note the distance between Polish and global companies: in the global survey 69 per cent of the respondents said that they were using cyber security services in the cloud. In Poland, cloud computing is used by 30 per cent of companies.

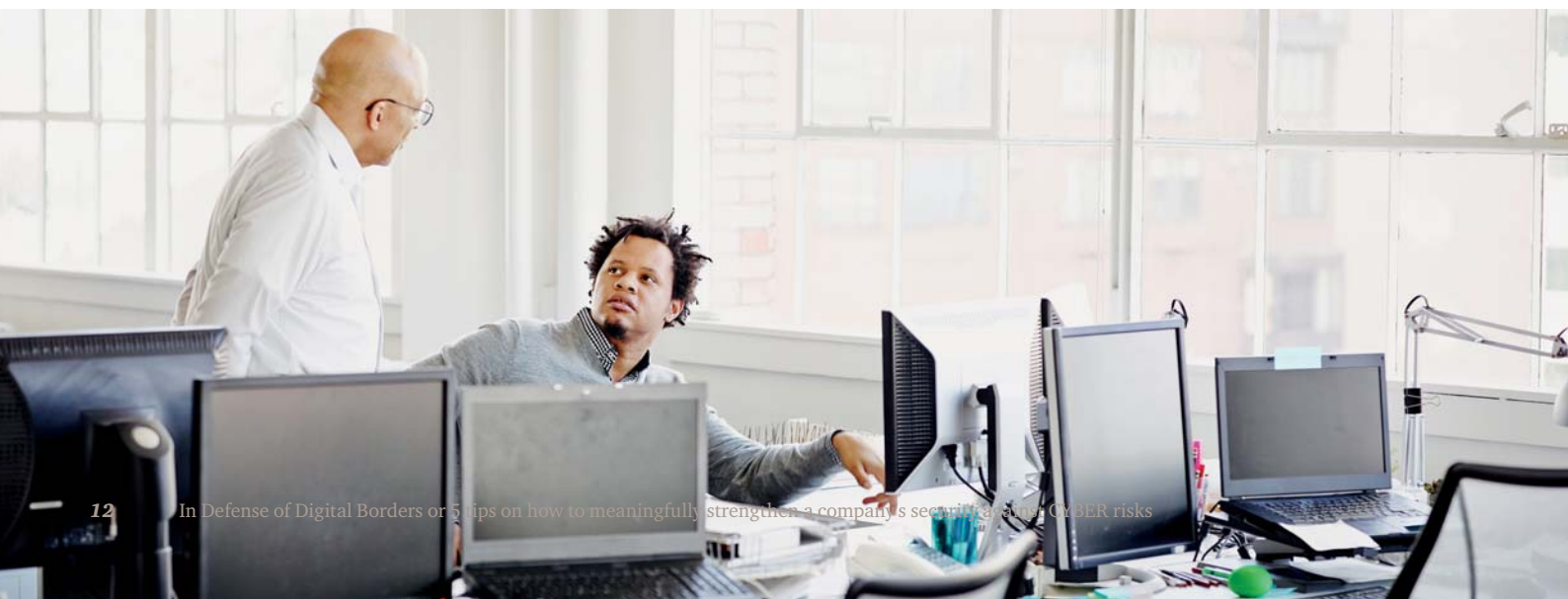
69%



of companies across the world use cloud computing

“The cloud is ok. In PwC, we have created tools which use Google cloud analysis power to analyze large data sets. It is needed when we to look into security breaches. We have used the same technology to build a platform to analyze the worldwide threat intelligence data which we collect: it relates both to the data entered by our employees or partners, and coming from our network sources. Our experience clearly indicates that, in the case of major analytical projects and in the context of providing information on threats, we have already exceed the capabilities of traditional analytical platforms”.

Rafał Jaczyński – Director, Cyber Security Team for Poland and Central Europe

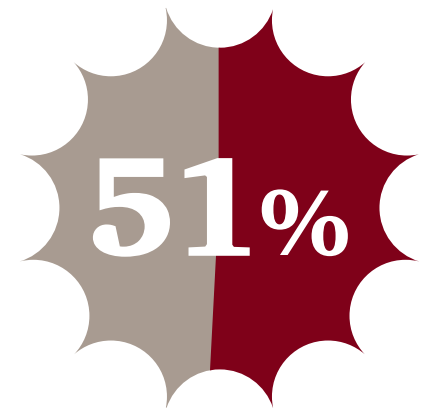


Also, Big Data technologies are employed to model and monitor cyber threats. A data-based approach can possibly lead to a revolution in the way the data are protected. Since data mining requires significant computing power, it is often combined with the computing cloud. Data can also be used to enhance security, e.g. access management. According to the PwC's "Global State of Information Security 2016" survey, the Big Data technology is employed by 59 per cent of companies. And in Poland 67 per cent of the respondents said that they do not use Bid Data technologies, nor do they intend to use them in the future.

Nevertheless, 50 per cent of Polish respondents say today that their companies do not plan to introduce separate security strategies for cloud computing, and 63 per cent say that they do not plan such ones for the Big Data.

More surprising is the fact that 51 per cent of the respondents said that their organizations do not plan to implement any information security strategy for social media.

Applying an ostrich strategy to the looming threats works well only in extremely rare cases, and every new ICT must be perceived both as an opportunity and as a threat. So it is not good to bury one's head in the sand in the presence of technological changes such as cloud computing, Big Data, or social media, as they already relate to almost every Polish company.



of companies do not plan to implement any information security strategy for social media

“When we audit security issues and the management of the IT environment, we find a lot of organizations with inadequate risk and IT security management, or it happens that the IT management bases solely on bans which they enter into their procedures. What is missing is the control over the administrators’ activities, no proper access limitations or no separation of the responsibilities in the IT systems, and also the security configuration of the platform is often poor. It often happens that the management processes in different applications are not coherent with one another and have got different requirements, which adds to the confusion and results in the lack of real supervision over the integrity of the IT environment. If companies are serious about their own security, they need to apply a holistic approach. The processes must be comprehensive and coherent in order to address change management and projects, ensuring both the quality and security already at the levels of architecture and the IT design”.

Jacek Masny – Deputy Director, IT Risk Management Team

Tip 4.

Engage the highest rungs



of companies believe that their boards should directly fund information security projects

An efficient and secure operation of the organization is only possible if the security issues are given enough priority and are supported by the management. Let us admit honestly: the so called “tone at the top” is of fundamental importance for any field of business whose relevance cannot be directly defended by its sales figures.

It is obvious that the board’s fundamental role is to ensure cyber security.

41 per cent of the respondents said that it was the management board which should directly finance information security programs. The Board’s involvement should also include operational security issues, particularly crisis management. In case of incidents involving leakage of sensitive information or downtime, the support and operation of the board will be necessary to both mitigate financial losses and look at the legal consequences.

“More and more management boards understand that security projects cannot be treated in isolation and be detached from the wider context of the company. One cannot base such projects merely on the calculation of the return on investment, because under such an approach the return is simply impossible to be identified in a short term. Security issues are now perceived differently. For this reason, in initiatives where security is an important business aspect, it makes an important added value for a business purpose, and at the analysis stage it begins to be considered as part of the overall project return. An example is the launch of the new mobile banking, where ensuring security of the service provided by the bank is an indispensable part of the project. In this case, the implemented mechanisms increase the security and the value of the new solution. It is essential to make investments in adequate financial resources in order to build security mechanisms. Or if not, the service may turn out to be just worthless, bringing about serious damage for the company or for its reputation, which will quickly lead to the loss of customers. Compliance or investments related to increasing the level of security of the IT infrastructure (which result from, e.g., a strategy which the company has adopted) are quite another matter. Both these cases do not directly translate into business projects, and are the foundation for the security of services which already exist in the organization. It is extremely difficult to calculate the return on investment of this type of work”.

Jacek Sygutowski – Director, Cyber Security Technology Services Team

Marcin Makusak – Deputy Director, Risk Management Team

30%

of companies do not know in which areas their information security director engages



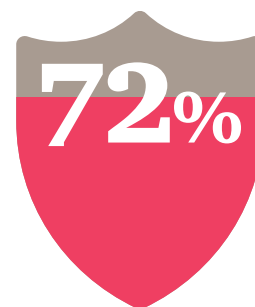
An effective way to increase the level of cyber security is personal involvement by the company's CEO in security issues. One solution which is frequently applied in order to improve the flow of information regarding existing or potential threats, and their countermeasures, is shortening the reporting path from the person responsible for cyber security management. It happens already in many companies that the Director of Information Security reports directly to the CEO. This is actually the case in the 50 per cent of the surveyed organizations. Of course the fact that the head of security is optimally located within the organizational structure does not, however, release him/her from a duty to be active. A perceptible proportion of 30 per cent of the respondents are unaware of the areas in which their Information Security Director is engaged, nor do they know either the scope of his/her responsibility or the type of the job.

Notwithstanding the strategic and financial issues, one of the important tasks of corporate boards is to provide support to a culture of information security. Many threats can be eliminated by preventive actions and by making employees aware that there are behaviors which expose businesses to data losses or to using their infrastructure for launching attacks on other entities.

38 per cent of the respondents are convinced that such support is necessary. Additionally, 72 per cent of companies still perceive cyber security in a very narrow way and treat it only as a part of (or a problem of) their IT departments. It often happens that there is lack of understanding of the impact of cyber risks on the whole organization, including on its finances.

“In Polish companies the risks connected to information security increasingly make it to the risk maps of the boards of directors, which is a positive trend. Unfortunately, their assessment is still not based on reliable data, for example on an analysis of breaches. There is also a lack of reliable information regarding the effectiveness of the information security management mechanisms, obtained e.g. through comprehensive audits. The role of internal audits is important, as they increasingly address cyber security issues. Internal auditors usually outsource such tasks to external entities, knowing what limitations they have to face. There is only one thing which is worse than the lack of information on the organization's stage of preparedness to tackle the information security risks. And it is a false sense of security, which is the result of a poorly performed audit”.

Piotr Rówiński – Director, Risk Management Team



of companies perceive their security issues as the job of their IT departments

Currently, CISO or CIO must not only be experts in cyber security, but also in risk management and in general management. They must have access to the key people in the organization to be able to highlight cyber security issues to them. Key communication skills are of critical importance, enabling a transparent way to inform the environment, especially in crisis situations.

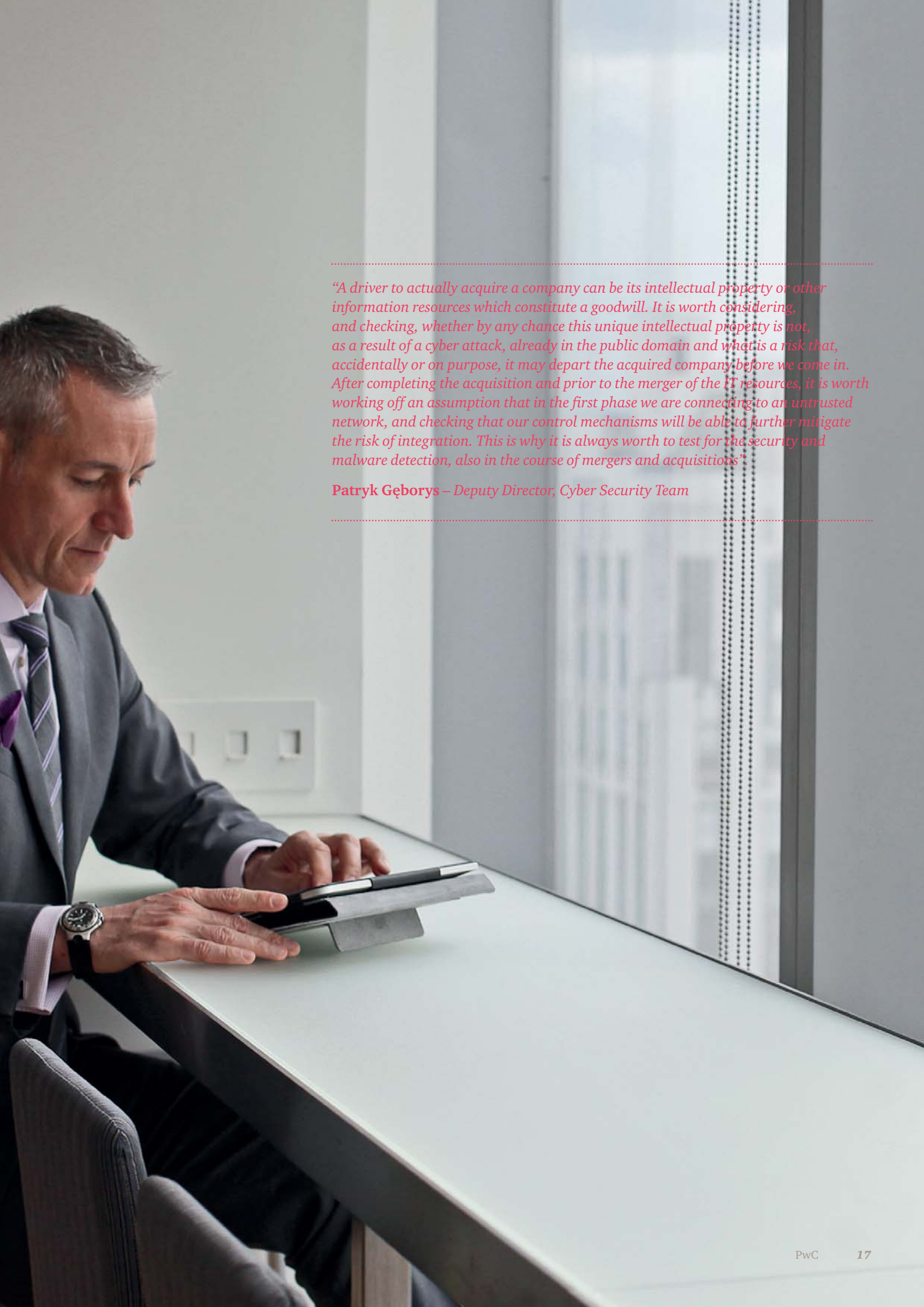
Cybersecurity is also one of the elements which should be looked at during mergers and acquisitions. Prior to a transaction, due diligence of the company to be acquired may be advisable with regards to cyber security.

Giving such issues a light treatment can potentially endanger the business. Criminals may choose to infiltrate smaller organizations and wait for them to be taken over by large companies where, after their systems have been integrated, they are going to gain access to the information which they are after. When assessing the risk of cyber security during a transaction, the following issues should be considered: the country in which the business is located and the markets in which it operates, the sector in which the company operates, the cyber-security practices which have been adopted, and the number of and the reasons for recent breaches.

“A contemporary CISO faces a difficult task. Two factors which are critical to a company’s success when it comes to the effectiveness of its information security are the competencies related to communication skills, and to the risk management. The former one is useful to persuade the management and business departments that money spent on cyber security is not only “a necessary evil” but that it contributes to building goodwill and reduces exposure. On the other hand, CISO’s communication with cyber security and IT experts is important to effectively translate strategic goals into operational actions. Another critical competency component is CISO’s ability to adequately assess the seriousness of threats and the vulnerability to information security”.

Szymon Sobczyk – Deputy Director, Cyber Security Technology Services Team





“A driver to actually acquire a company can be its intellectual property or other information resources which constitute a goodwill. It is worth considering, and checking, whether by any chance this unique intellectual property is not, as a result of a cyber attack, already in the public domain and what is a risk that, accidentally or on purpose, it may depart the acquired company before we come in. After completing the acquisition and prior to the merger of the IT resources, it is worth working off an assumption that in the first phase we are connecting to an untrusted network, and checking that our control mechanisms will be able to further mitigate the risk of integration. This is why it is always worth to test for the security and malware detection, also in the course of mergers and acquisitions”.

Patryk Gęborys – Deputy Director, Cyber Security Team

Tip 5.

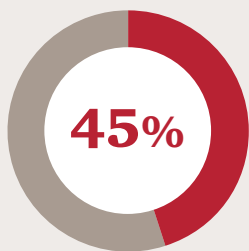
Look for an external support

In cyber security it is important to share knowledge with other stakeholders as it can help prevent and address threats. A problem exists here, however, of the lack of trust and limited willingness to cooperate. Only 41 per cent of the respondents have said that they trust external entities or subcontractors, which translates into a limited willingness to cooperate and thus narrows down the area in which it can be implemented. According to the respondents of the survey, 45 per cent of companies have collaborated with partners in their industry in order to improve information security, but nearly as many (42 per cent) do not collaborate with such partners. And the reason for this is the distrust, the fear of using external sources

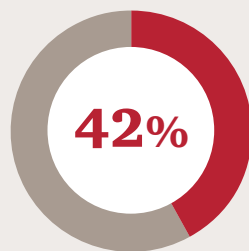
information, and the belief that such cooperation can pose a threat to the security of personal data.

Surely, even the most extensive cooperation and efforts to protect a company may prove to be ineffective. One of the options to minimize the negative effects may be to purchase an insurance against cyber threats. The idea is still not too popular in Poland, since only 8 per cent of the respondents said that their companies decided to take out such insurances. Elsewhere in the world the proportion is much higher. According to the “*Global State of Information Security 2016*” survey, 59 per cent of companies have taken out such insurance policies.

Cooperation with external entities

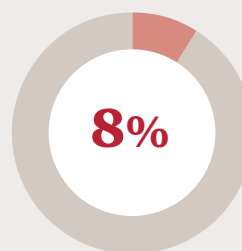


of companies have established collaboration with other companies in their industry in order to enhance information security



of companies have not established any collaboration with other companies in their industry in order to enhance information security

Insurance against cyber threats



of companies in Poland is insured against cyber threats



of companies worldwide is insured against cyber threats

“The Polish market takes time to slowly warm up to the idea of insurances against the effects of cyberattacks. When we compare our situation to more mature markets, we see that a wealth of available products in this area is yet to come. An insurance policy certainly will not be an alternative to technical and logical security system, which safeguards the company’s information and its reputation, but it definitely can be a good complement of these activities. In particular, it is worth considering an insurance strategy towards sensitive customer data. If the data is leaked, the insurance will protect the company against financial problems which may result from e.g. an avalanche of claims coming from dissatisfied customers. Looking towards the near future one can notice that insurance policies against consequences of cyber attacks will become increasingly important: on the one side is our focus on investments into technical and logical security plus the insurance policy, and on the other side there are the consequences of a successful attack”.

Marcin Makusak – Deputy Director, Risk Management Team

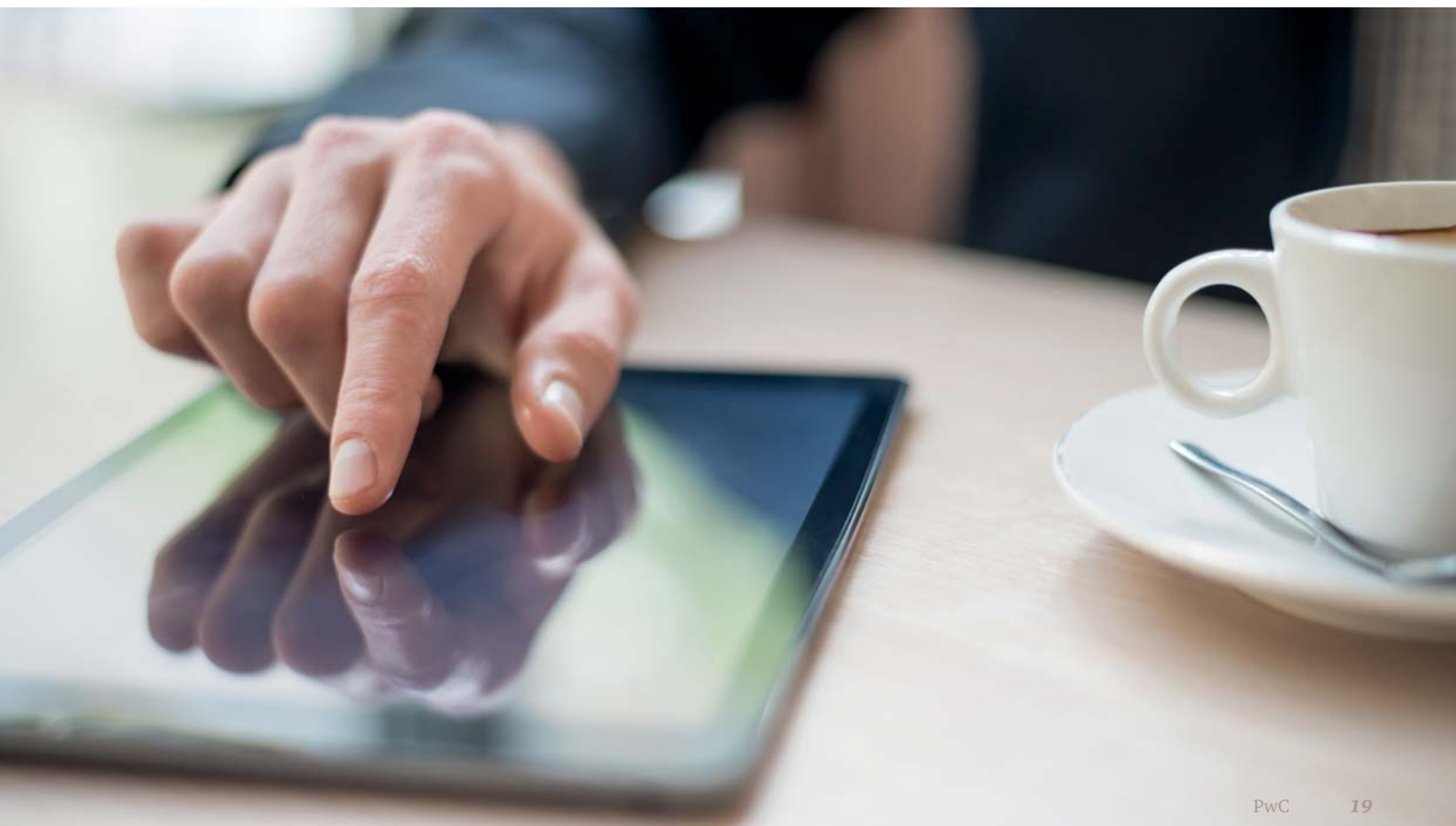
What is the most common type of a loss for which insurance companies have to pay out compensations? According to 47 per cent of the respondents it was the loss of identification data, 41 per cent said that the compensations had to do with the loss of data regarding payment cards, 38 per cent said that the

compensations were a consequence of the theft of intellectual property or trade secrets, and 36 per cent was related to a damage to the brand’s reputation.

An insurance policy comes in a lot of options to choose from. They can include a destruction of data, attacks

which result in rejections of service, and thefts and extortions. Optionally, they can also include costs of reacting to incidents, repair costs, as well as the investigation and cybersecurity audit costs. Some insurance companies will expand their range of cover to include compensation for the lost intellectual property, damaged reputation, image and brand and for the infrastructure failures. We should however bear in mind that it is very hard to estimate the insurance level and a likely scale of a damage inflicted by a cyber attack. It is a very important aspect because purchasing an insurance policy requires substantial allocations from the budget, and thus to accurately estimate company’s needs is of topical importance.

Interestingly, such insurance policies are the world’s fastest growing insurance segment. As shown in the PwC’s “Global State of Information Security 2016” survey, their value will increase from 2.5 billion dollars in 2015 to 7.5 billion dollars in 2020.



Compensations related to cyber attacks:



An additional effect of purchasing an insurance policy is also a better recognition of the existing threats and a possibility to better deal with them. This is a result of the requirements posed by the insurers, which put on obligation on companies to analyze their ability to prevent cyber attacks and to permanently monitor the risk level. We ought to keep in mind that insurers are not likely to offer favorable policy terms if they rank an event as highly probable, unless certain security measures have been applied, most often in a manner of an independent verification.

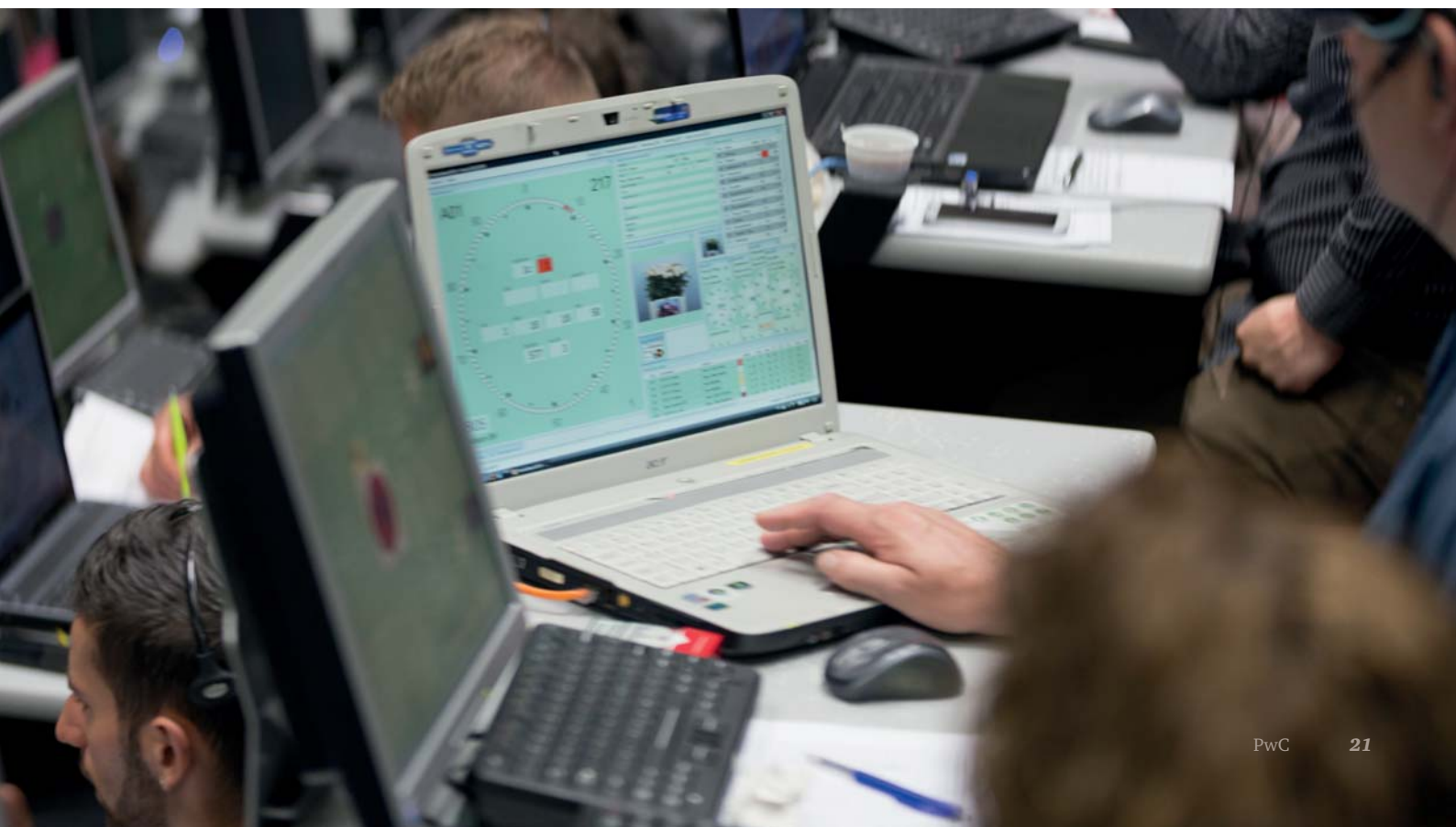
A factor which facilitates cooperation between enterprises is the creation of government agencies which collect data on the attacks performed and facilitate exchange of information. An important role can also be played by trade organizations which form platforms of sharing information on risks. Such an exchange also helps raise awareness of the existing risks. International cooperation between companies gets more complicated as discrepancies in their legal systems may cause difficulties in the areas of e.g. protection of personal data, and even in the interpretation of what personal data in each country is.

Security can be compared to driving: we ought to foresee how a situation on the road can develop, and we must not be taken by surprise. Also, in an event of an incident we must not lose our head. Lastly, we ought to keep in mind that the insurance does not prevent the accident, but it can limit its consequences for our budget.

Let us not be hit by cybercriminals and also let us not shoot ourselves in the foot: we ought to collect information about what is about to come, take care to secure ourselves, and to ensure the good quality of processes, technologies, and personnel who is responsible for the ICT systems. When an incident does take place we ought to remember that we need a technician to take care of the IT side of the problem, a lawyer to look at the legal obligations and implications, and a spokesman to effectively communicate things to the market and shareholders. Yes, all this is going to generate big costs for us, but not as much as the loss of the competitive advantage and the market reputation as well as the loss of customer confidence or our ability to do business.

“The cyber security aspect of our business is just as important as any other type of security. It can be disrupted by international organized criminal groups which seek to finance their criminal activities through the network. This also applies to economic crime, as tax frauds and carousel frauds move to cyberspace. It often happens that apart from cyber criminals, highly skilled IT and network security experts are hired to engage in this. Apart from camouflaging criminal activities, they test the latest vulnerabilities in the systems, and develop malicious software to steal the so called crown jewels. It is therefore necessary to minimize the effects of such incidents, and secure evidence which can identify the perpetrators so that proceedings before a criminal or civil court can be instigated. Also, the state agencies have recognized the need to develop the national cybersecurity system (expansion of the law enforcement and regulations), and that the whole process cannot take place without cooperation between government agencies and entities from the private sector entities”.

Marcin Klimczak – Partner, Forensic Services Team Leader





Methodology

The report was prepared on the basis of the study which involved 126 Polish experts in the field of IT and information security. The study was conducted in autumn 2015 via an online survey. The survey results are based on the aggregation of responses.

Contact details



Piotr Urban

Partner
Risk Assurance Leader for Poland
Cybersecurity and Privacy Leader for CEE
Tel.: +48 502 184 157
E-mail: piotr.urban@pl.pwc.com



Rafał Jaczyński

Director
Cyber Security team for Poland and Central Europe
Tel.: +48 519 507 122
E-mail: rafal.jaczynski@pl.pwc.com



Jacek Sygutowski

Director
Cyber Security Technology Services Team
Tel.: +48 519 504 954
E-mail: jacek.sygutowski@pl.pwc.com



Magda Sarzyńska

B2B Content Manager
Tel.: +48 519 507 153
E-mail: magdalena.sarzynska@pl.pwc.com

The publication has been prepared for general information purposes only and does not constitute advice within the meaning of Polish law. You should not base your actions/decisions on the content of the information contained in this publication without obtaining professional advice first. We do not guarantee (explicitly or implicitly) the correctness or accuracy of the information contained in our presentation. Moreover, to the extent provided by the Polish law, PricewaterhouseCoopers Sp. z o.o., its partners, employees, or agents shall undertake no obligations and assume no responsibility towards you, neither through damages or through any other title, for any losses, damages or expenses that may be a direct or indirect result of action taken on the basis of information contained in our publications or decisions taken thereunder.