The 4th issue of the survey on the state of information security in Poland

Protecting Business in a Digital Transformation

or 4 steps to a more secure company

pwc

pwc.pl/stanbezpieczenstwa

Dear Reader,

In the digital world the digital transformation puts trust to a test. Effective protection of one's IT systems, data, and information is now a key element of ensuring a stable business. CEOs in 61 per cent of the world's largest organizations have said that cyber threats belong to the greatest risk areas in their businesses.[1] One of the most sensitive issues is the brand's market confidence, especially as the interconnectivity between people and devices continues to grow.

The results of this year's fourth edition of the survey on information security in Poland show that business is facing big challenges related to the stable trust in the network and to the sense of security experienced by its employees and customers.

Polish companies have only started to prepare for GDPR and to implement new regulations, starting from the simplest solutions available. The readiness of companies' process seems to be at the lowest deployment stage: a program to identify sensitive resources has been implemented by as few as 11 per cent of companies, while 58 per cent have got no plans to implement it at all.

The results of our survey indicate that 96 per cent of companies have experienced more than 50 incidents in the last year. Financial losses and exposure to legal or judicial risks were listed among the most common negative effects (by 35 per cent of the respondents). One other common response was a loss of clients (30 per cent), and the leak of business correspondence (25 per cent).

Also, the inter-permeation of the IT and OT (operational technology) environments requires a new approach to the security and production monitoring issues among Polish companies. More than 60 per cent of the respondents said that processes which support OT systems for the management of security breaches need to be changed.

Having analyzed the trends, challenges and directions of the development of global companies, we are pleased to present four steps which aim to help Polish companies to comprehensively prepare for the upcoming regulatory changes, strengthen or complement security elements which they have already implemented and finally, add value and help attain a level of the competitive advantage in the market.

Piotr Urban
Partner, Risk Assurance Leader for Poland
Cybersecurity and Privacy Leader for CEE

[1] *PwC CEO Survey 2017*

Protecting business in the digital transformation

Step 1

Focus on trust – get ready for the change

page 4

Step 2

Awareness first – be sure

page 9

Step 3

Monitor results – check performance and draw conclusions

page 14

Step 4

Analytics, automation, the Internet of Things – see more

page 18

Step 1

Focus on trust – get ready for the change

20 million euros

penalty for an infringement of the GDPR rules

72 hours

for reporting a cyber attack to the regulatory authority

The stage of preparedness for the new regulations on data protection (GDPR)

One of the most important events of the past year in the area of information security was when the European Union adopted the General Data Protection Regulation (GDPR), which in May 2018 is expected to replace all national regulations and introduce uniform rules across the entire European common market.

As for Poland, the Regulation changes the provisions of the Act of 29 August 1997 on the protection of personal data. The Regulation will be applied directly which means that it will become a binding law for all entrepreneurs. We are currently in a period of time which has been set aside for entrepreneurs to implement the Regulation, which is to be fully applicable from 25 May 2018. An infringement of the rules may result in a financial penalty, making a company to pay up to euro 20 million, or 4 per cent of its worldwide annual turnover.

GDPR introduces a number of important changes to the approach on how the requirements of securing personal data should be met. Rather than detailed principles, which might not be always tailored to technical solutions, the GDPR requires from administrators and data processors to implement appropriate technical and organizational measures, which they are to choose themselves.

Most importantly, incidents involving breaches of personal data security will have to be reported to the regulator within 72 hours. Also, any business which processes such data will have to at least carry out appropriate risk analyses and to implement adequate security measures. This may mean a change to the existing data management strategy, or having to devise a new one, or a need to implement processes and technologies to effect inventories and ensure protection of the personal data.

This year's edition of the survey shows that in terms of the preparedness for GDPR, Polish companies are only at the beginning of the process for compliance.

When we look at the measures implemented so far, what has been incorporated most effectively are the mechanisms to protect personal data in the design stage of the new systems *("Privacy by Design")*: 42 per cent of respondents declare that while implementing new systems they have already taken into account issues related to the proper protection of personal data. The second best-adhered to requirement is the commitment by employees to undergo periodic trainings on data protection policy: 34 per cent of respondents said so, and 27 per cent of respondents mentioned the implementation of personal data protection and compliance audits of third parties (data processors) who process entrusted personal data .

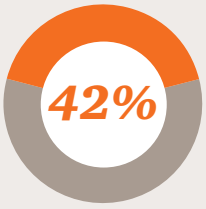
The prospect of implementing data encryption solutions looks promising. As many as 34 per cent of companies declare their high priority to implementing such solutions.

When it comes to the other GDPR-related aspects, business should take swift actions. The most neglected areas are: creation or updating of registers of processing personal data, the assessment of the effects of processing operations, and the reduction of the number of processing operations to the indispensable minimum which is necessary to attain the purpose for which they have been collected. Respectively, only 12, 15 and 12 per cent of companies have implemented adequate solutions. This may mean that they have not yet carried out the analyses which show what required changes in their IT systems and business processes are necessary and actually related to the implementation of GDPR.

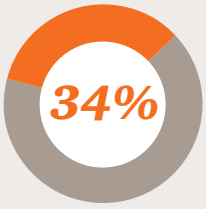
Businesses have started implementing new regulations by applying the simplest solutions first, which makes a good foundation for any further tasks. However, one ought to keep in mind that the time to implement the GDPR rules is limited. From the perspective of the personal data protection, the most critical seems to be how companies approach the Big Data issue. 80 per cent of companies do not consider introducing solutions which would ensure security in this area. Since the GDPR regulations also looks at the mass processing operations, any processes which ensure security of personal data should also encompass the area of the Big Data.

Polish businesses are at the beginning of the road in their preparedness for the new regulations. The level of readiness of large and medium companies is generally low. Some rules which have been the simplest to effect have been implemented, data protection specialists have been hired, and technical solutions are in place to ensure data security. The readiness of companies' process seems at the worst stage: the program which identifies sensitive resources has been implemented by only 11 per cent of companies, and 58 per cent do not plan to have it at all.

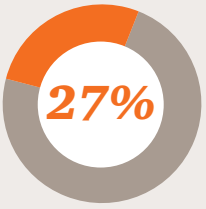
The level of preparedness of Polish companies for GDPR



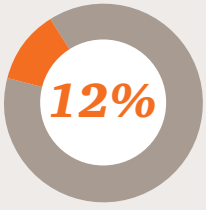
Mechanisms of protection of personal data have been incorporated into the new IT systems



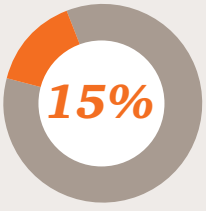
Employees are committed to periodic trainings regarding the personal data protection policy



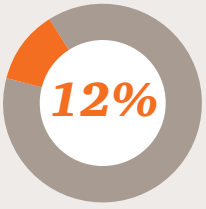
Personal data protection mechanisms and external audits which look at the personal data are in place



Registers of personal data processing operations have been created/updated



Impact assessments of processing operations have been carried out



The number of processing operations necessary to attain the goal for which they were collected has been cut down to the minimum

Above: percentage of companies which have implemented appropriate solutions.

Preparation for GDPR calls for an analysis

"One should bear in mind that the style of implementing the GDPR requirements may differ for each administrator and processing entity. It is also admissible that one entity will have to apply different ways of fulfilling this requirement. Each decision on what data protection measures to apply should first be analyzed in depth, in order to select the best solution. The requirements of the General Data Protection Regulation affect many areas of the company's operations. They relate not only to the work of the legal department but also of the marketing, HR or customer service departments. For this reason, in order to ensure an adequate implementation of the requirements of the GDPR rules, setting up an interdisciplinary team of experts is advisable, particularly in the legal, business, IT and information security areas".

Anna Kobylańska – *advocate, counsel in the PwC Legal*
Łukasz Ślęzak – *manager, Cyber Security Team*

Collaboration for cyber security

Cyber threats affect all businesses with no exception. We have undertaken to check whether businesses do decide to cooperate in order to jointly increase cyber security. The issue is topical since, as our study shows, most respondents are not really convinced whether the activities undertaken by their business partners or providers are sufficient to ensure the IT security. Only 25 per cent of the respondents said that they were rather or firmly convinced that this was the case.

The issue of cooperation and coordination of activities is high on the agenda also in the public administration. At the end of 2016 the Ministry of Digital Affairs released a draft of the "Cybersecurity Strategy of the Republic of Poland for the years 2017-2022" where one of the main objectives is: "to achieve the capacity for nationally coordinated actions which will prevent, detect, combat and minimize the effects of incidents which compromise the security of ICT systems which are vital to the functioning of the state."[2] This does not imply however the various actors' desire to tighten ties between them. Like a year ago, the respondents were skeptical about cooperation and information exchange with other stakeholders. Only 31 per cent of the respondents to our survey have confirmed that their business collaborated with others to improve safety and to reduce future risks. About 27 per cent of the respondents have said they do not do it, while 42 per cent were not able to answer this question. But what is the factor which makes this kind of collaboration so unpopular?

The main obstacle is the distrust towards external sources of information. Another reason is the reluctance to discover the weaknesses in one's own company.

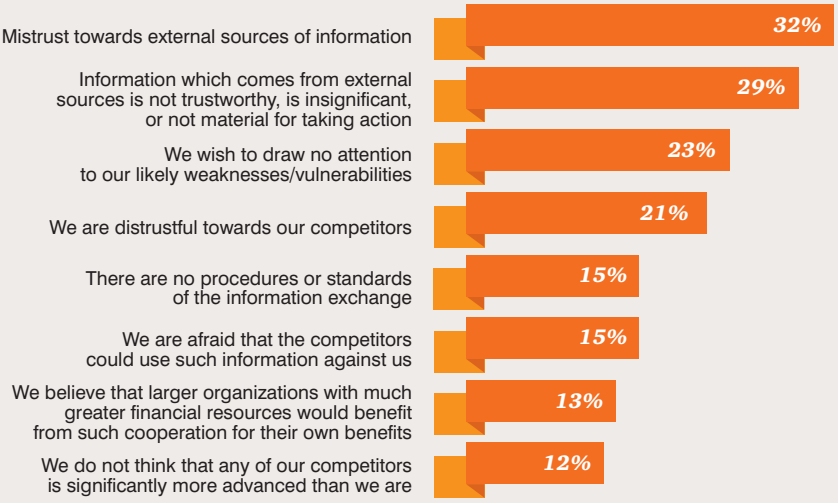
The respondents' replies indicate that they find it difficult to notice positive aspects of cooperation, and that they rather tend to concentrate on threats.

Surprisingly, despite the deficiencies of trust, most respondents think that their companies have got no plans to implement monitoring programs or audits by external partners and service providers to ensure adherence to the security and data protection policies. Only as few as 8 per cent of organizations have implemented such activities.

It is also worth noting that there exist areas where the exchange of information does take place: it is the banking and the telecom industries. What prevails, however, is the information exchange via informal channels. The Ministry of Digital Affairs promotes the Computer Emergency Response Teams (CERT), a question is whether they can become a remedy and overcome the distrust which exists.

[2] *Ministry of Digital Affairs "Cyber-Security Strategy for the Republic of Poland for the years 2017 to 2022"*

Reasons for not cooperating with other businesses in order to improve security



Consumers online

The issue of trust is not only about relationships with business partners, but it also concerns individual clients. According to the PwC Total Retail 2017 study, companies do not want to abuse the trust of their consumers. More than half of the companies said that in the coming year their organizations do not plan to ask their customers for any additional personal information (such as demographics or contact information), which could help personalize services which they provide.

Given the mood among customers, it looks like a good decision to take. People are reluctant to share information about themselves, mainly because of the fear of fraud. Consumers use the Internet primarily to get services from the companies which they trust: this is true for about 52 per cent of respondents from Poland and 59 per cent globally. Similarly, 54 per cent of consumers in Poland and 63 per cent worldwide declare that they use only trusted websites. 25 per cent of the respondents to the survey in Poland said that they were familiar with the data protection policies, and the percentage worldwide was only slightly lower.

More and more Polish customers do their shopping via social media: 21 per cent of respondents said that they do. This fact is important as companies have to take action to protect the data which they gain through such processes. Any online activity is connected to decisions which involve a requirement to leave behind one's identifying data, either personal or for payment purposes. Therefore, increasing sales through this process requires secure means of data processing in the cyberspace. Consumer concerns also relate to the use of mobile devices. 71 per cent of respondents are afraid of hacking attacks on their smartphones or tablets, while only 29 per cent believe that mobile payments are secure.

The level of customer trust in these areas is still quite low, which is an important piece of information for companies. If they want a greater willingness from the customers to entrust them with their data or a bigger level of online shopping, they have to enhance security and to communicate to customers what activities they undertake. This information is valuable for companies which want to single themselves out, as taking special care about security issues is a great asset.

25%

of Polish consumers read privacy policy when sharing personal information online

Step 2
Awareness first – be sure

Allocating budget for defensive actions is essential. In our survey more than half of the respondents have said that their budgets for IT/information security for 2016 were between PLN 500,000 – 1 million. It seems, however, that it is only a beginning of investments in this area, given the context of the medium and large companies preparing for the GDPR. The dynamics of expenditure has also changed: the implementation of investments is now point-wise, that is targeting selected areas. Although globally the level of expenditure on security issues has not changed, its distribution has shifted between economy sectors.

In the budgetary context, most respondents declare that they have got an overall IT security strategy in place, but as many as 72 per cent of these companies do not actively seek to identify sensitive resources, and most of them have got no specific strategies regarding areas such as social media, mobile devices, or cloud computing (respectively: 63% per cent, 86 per cent, and 63 per cent). It is quite puzzling, given that under the current market trend companies let their employees use their private electronic devices (smartphones or tablets) for corporate applications. As of today, 46 per cent of the surveyed companies allow this, while another 14 per cent plan to allow such activities in the future. Only 17 per cent of companies say that they do not allow such activities. At the same time, only 16 per cent of companies require MDM (Mobile Device Management) solutions to be installed on the devices before users are allowed to use their company's applications.

of companies spend less than PLN 1 million per year on IT security

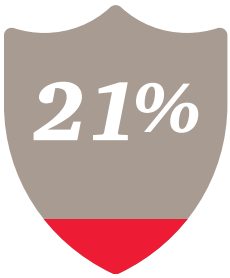
46%

of companies allow their staff to use company's apps on their private smartphones or tablets

Effective security requires a comprehensive approach

"Having an overall security strategy does not guarantee in itself an optimal spending of one's financial resources or the selection of adequate technological and organizational security mechanisms. What enables a proper channeling of an investment is the knowledge about the environment and the threats, understanding what is most important to the organization, and what resources are to be protected. The results of our survey and market observations indicate, however, that spending continues to be targeted point-wise and on technologies rather than on raising the level of security of the entire organization. Often new technical solutions are introduced, but no investments in people follow, which otherwise might help them use the technological solutions more effectively. What is also lacking are investments in processes which might ensure that technology and people work effectively. Such an approach and the lack of appropriate risk management procedures means having to learn by mistakes, which can be very expensive".

Tomasz Sawiak – *deputy head, Cyber Security Team*



of companies have got SIEM

(Security Information Event Management)

Technology for the security

Maintaining a level of IT security which can match the specific character of a business and noticeable environment-specific risks requires an appropriate set of security mechanisms. Not only organizational resources are required, but also appropriate technological solutions in order to address specific problems and threats. Companies develop and improve their business processes and related IT systems and environments in a strive to gain the most competitive advantage. An increasing level of dependence on technology is decisive for the level of competitive advantage which a company may attain, but it also increases the risk and a possible impact of a cyber attack on their IT environments. This increases the need to carefully select an appropriate set of technical protective measures. Looking at the security solutions which are available on the market and at the specific character of the attacks, one can say that companies are not yet fully prepared to counter the current threats and the likely methods of attacks. Companies in Poland are still to do a lot of work in their technological architecture which relates to their security. Contemporary methods of attacks on business IT environments are often about targeting privileged users' workstations via remote access, for which they employ malicious software (RAT – Remote Access Trojan). Various methods of attacks are in place, including taking advantage of the ignorance on the users' part and fooling them into unintentional infecting of the workstations e.g. when visiting especially fabricated web sites, or opening specially crafted files (documents, spreadsheets, etc.). Only 26 per cent of the companies from our survey utilize specialized solutions to safeguard themselves against such types of attacks (ie. Anti-APT: Advanced Persistent Threat).

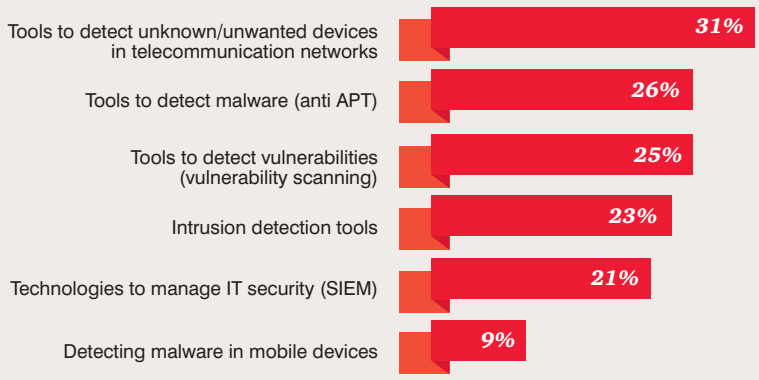
A huge number of systems and technological security measures require a comprehensive look at the entire IT infrastructure as well as a degree of knowledge regarding the work of security mechanisms. This is an indispensable condition which will enable an adequate response and analysis of identified incidents. Only 21 per cent of respondents say that they have got a SIEM-class (Security Information Event Management) system in place in order to addresses this issue. When an attack takes place, it is the known vulnerabilities of the IT components which are abused.Removal of critical vulnerabilities, such as an unauthorized remote access to critical components of the system, is of key importance.

Unfortunately, only 25 per cent of the respondents say that they have got tools to support such processes. The Intrusion Detection Systems (IDS) are solutions which are based on signatures of known attacks and on the attempts to use vulnerabilities. These systems complement the weaknesses of the identification process and of the management of vulnerabilities in infrastructure components, and are used by 23 per cent of businesses.

More and more information is being processed through mobile devices, and modern applications are designed with the purpose of being used by mobile users, who gain an easy remote access to data. Unfortunately, only 9 per cent of companies use malware detection software on their mobile devices. Companies tend to just focus on the security of their workstations and forget to secure their mobile devices in a similar manner. The lack of such protection can result in uncontrolled data leaks which, in the context of the new GDPR regulations, calls for a particular attention.

Also, notwithstanding the proper technical security, what really matters for the IT security is the IT staff and their appropriate qualifications. Even the best security measures will not be fully utilized or developed if there are no right people or if the appropriate tissue of the procedures and the organizational system is lacking. Also, it is important to constantly improve the configuration of the existing systems, basing on the knowledge gained from the resolved incidents and the risks which have been observed in the company's environment.

Security means implemented in the companies

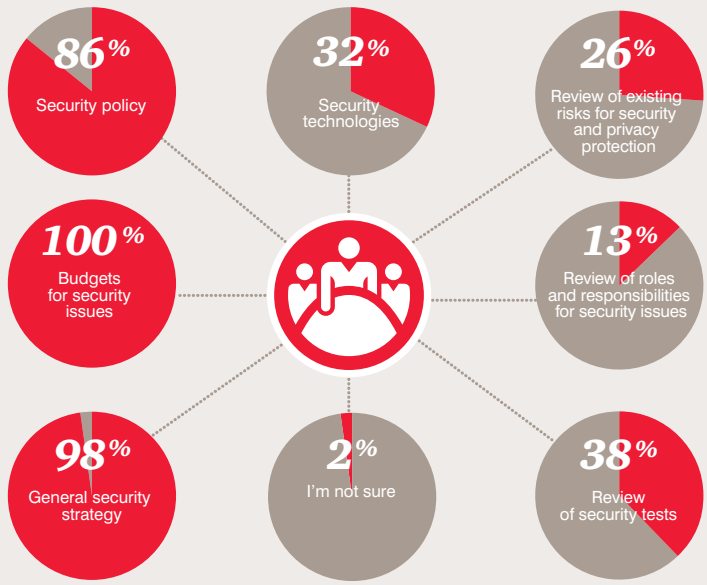


System of information and IT security in companies

ICT security should be supported at all levels, and well-established at the company's management level. We have asked our respondents about their ways of organizing information and the IT security. The good news is that we have noted no cases of an absence of a person responsible for the Information and IT security areas. For the most part, large companies employ up to 10 people in their IT and information security departments. If a company has got a position of a director of the company's IT security, this person directly reports to the CEO; such was a reply from 27 per cent of our respondents.

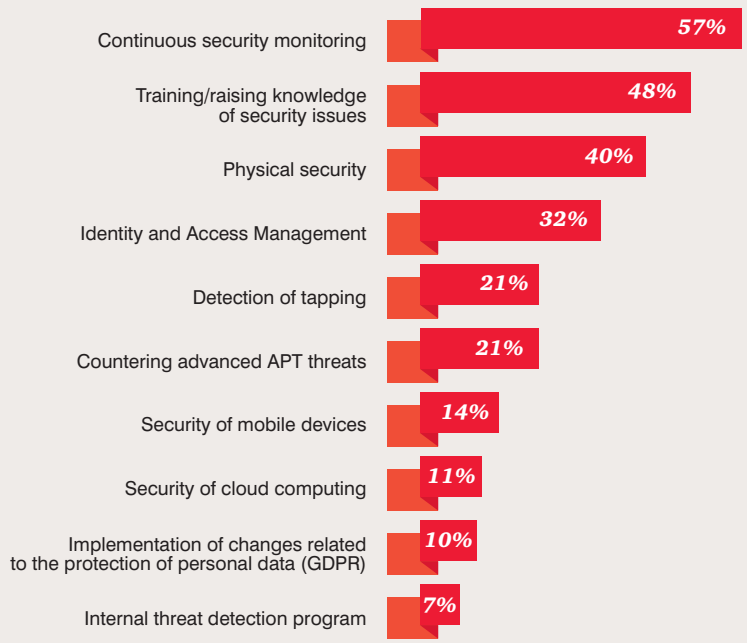
The company's management can play a very important role in providing IT security. In all the companies under our survey, their management takes part in shaping the budget for the security issues. 98 per cent of respondents said that their management contributes to the overall security strategy and 86 per cent said that it was actively shaping the security policy. Only a small number of boards gets involved in reviewing the roles and responsibilities in their organizations, as this is the case of only in 13 per cent of the companies surveyed. It is comforting to see that there is an involvement of the boards in these issues. However, the low position of the security managers in the company's hierarchy indicates that the issues of data protection, privacy and security are not high enough on the agenda of large and medium-sized businesses.

Areas in which the Board gets involved



While researching the strategic level in organizations, we decided to see what the organizations' priorities for the next 12 months were. Our findings show that the largest group of companies, that is 57 per cent, plan to conduct a continuous monitoring of IT security. The second top priority was providing training with a view to increase the level of knowledge on security issues, and the third top priority regarded physical safety. Large organizations have begun to appreciate the importance of security monitoring and of their employee awareness. It was surprising to see, however, how little emphasis was put on implementation of GDPR-related changes. This trend seems to have to be changing in the months to come, as awareness of the very regulation and of its impact on the organization is going to grow.

Companies' priorities in security for the next 12 months



Cyber security management on the CEO's agenda

"In Poland the cyber risk management still makes it to the agenda of only very few boards. Only mature organizations recognize the benefits of receiving a constant feedback on this and of the potential of being able to use them in business decisions. In large companies in the United States or Western Europe, cyber security is one of the key topics, which is systematically discussed and analyzed at board meetings. However, in order to do this, an organization has got to have the right tools to acquire, analyze, track and report on the environment and on the risks involved. It is worth noting that such tools do exist: they are the SIEM or DLP (Information Leakage Protection) systems. What is often missing however are the processes and the knowledge of the systems, which prevents them from being utilized to their fullest. A good example are the Governance-Risk-Compliance (GRC) systems, which enable data analysis and automation of multiple security, audit and compliance processes, and provide managers with clear information about their companies' risk profiles".

Patryk Gęborys – *Deputy Director, Cyber Security Team*

Step 3

Monitor results – check performance and draw conclusions

Security measures implemented by businesses build their security architecture, and reduce the risk of attacks and potential losses. However, due to the complexity of the IT environments and the continuous evolution of the risks and attacks, they do not guarantee a hundred per cent effectiveness. Drawing conclusions from the noticed incidents allows planning and directing one's actions for a further development of the security level, as well as the identification of potential vulnerabilities and an ability to carefully address them. Businesses report an increasing number of incidents, a phenomenon which is connected to a higher awareness of the problem and to the monitoring processes: 96 per cent of companies have experienced more than 50 incidents in the last year.

96%

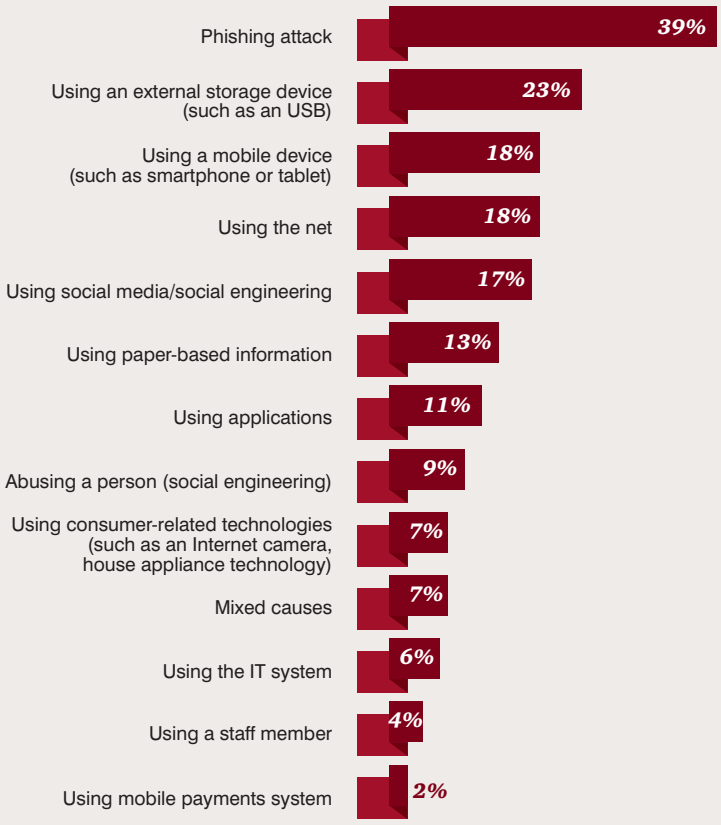
companies have experienced more than ***50*** security breaches in the last year

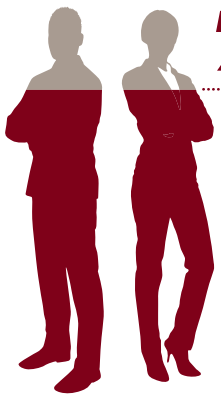
Ways, sources, and consequences of security breach incidents

Our survey has established that the most commonly used method was a phishing attack (intended to mislead the user and to induce them to perform a certain operation), such has been the reply by 39 per cent of the respondents. The second most often breach was the use of external storage media, which meant infecting components of the infrastructure and a possibility of data leakage. The third top breach was using mobile devices and networks: 18 per cent of respondents have said so. Many of the incidents could have been avoided if appropriate security systems had been implemented, or the staff members had been more aware of risks and if there had been adequate policies and procedures to follow.

a phishing attack is the most common security breach in a company.

Reasons for security breach incidents:





79%

of security breach incidents in companies are made by current staff members

In comparison with the previous survey, the primary source of threats has not changed and remains to be one's current employees: 79 per cent of the respondents said so. However, the number of respondents who have indicated hacker attacks has gone down from 67 to 62 per cent. A fairly big share of organized crime is worth noting, but even though it has gone down from the previous 41 per cent to the current 38 per cent, it is still at a high level. The count of one's current service providers, consultants or contractors was only 1 percentage point less. When we discuss the sources and the number of incidents, we ought to keep in mind that each incident can bring about serious consequences.

As the results show, 55 per cent of the respondents were unaware of the impact of the attack on the data in their business organizations. In part, this probably means that they caused no harm, but some respondents may just not realize the effects of the breaches, as they may be difficult to estimate without an appropriate methodology. This is a reason why risk management systems should be developed, including collecting information on operational events and security incidents, so as to ensure a consistent collection of information on the costs, impact and the incident handling.

The consequences of security breaches

A significant group of respondents (29 per cent) reported that cyber attacks resulted in a data loss or damage, 6 per cent reported leakage of their customer data, and 5 per cent spoke of data leakage pertaining to staff members. About 3 per cent said that they had experienced data and information leakages which could identify their customers or contractors, and in 2 per cent of the organizations such leakages enabled identity thefts. This last one may potentially bring about particularly negative consequences, ranging from a damage to the reputation to serious financial losses.

In comparison to our previous survey, the number of responses which indicated the staff members leakage has gone down from 13 to 5 per cent, but what is more important is a reduction of leakage of customer data (down from 18 per cent to 6 per cent). Unfortunately, at the same time we have noted a significant increase in the data loss or data damage, from the level of 16 per cent last year to 29 per cent this year.

The most commonly reported adverse consequences were financial losses and an exposure to legal or judicial risk (35 per cent). Other frequently reported responses were a loss of customers (30 per cent) and a leakage of corporate correspondence (25 per cent). In the view of the respondents, such incidents rarely cause financial frauds, losses of business partners or suppliers, or thefts of "soft" intellectual property (5 per cent).

Insurance against cyber risks

Awareness of the cyber risks does encourage some companies to buy out insurance policies against them. As our survey shows, 7 per cent of companies have taken such a decision. 40 per cent of companies which have got cyber -insurance have also undertaken steps to improve security in the organization in order to reduce insurance premiums.

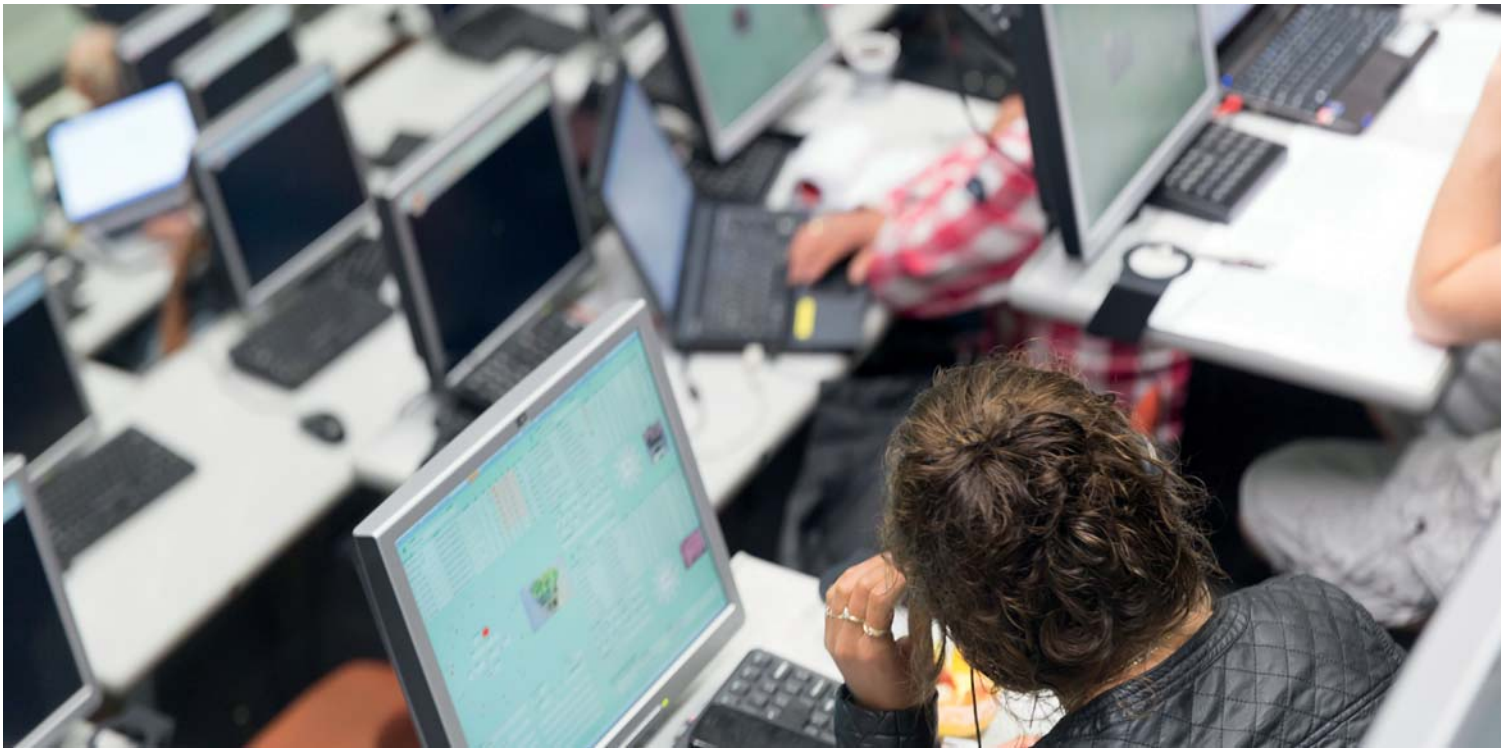
Step 4

Analytics, automation, the Internet of Things – see more

58%

of the respondents worldwide use private clouds

Almost half of the organizations under our survey use some form of cloud computing. The most common was the use of public clouds, as indicated by 54 per cent of the respondents. The private and hybrid cloud models were less used. Globally, 58 per cent of the respondents use private clouds, 33 per cent use public ones, and 30 per cent use hybrids. Moreover, 47 per cent of the respondents globally indicated that their companies have developed cloud data protection strategies; 29 per cent of the companies commissioned such documents from outsourced providers. The use of cloud solutions is quite widespread across the world. A question remains, however, as to the level of stability of such services. The spectacular failures of the Amazon and Microsoft clouds in 2016 and 2017 show that, despite great efforts employed, such solutions are not completely reliable.



Analysis of large data sets

In Poland, 13 per cent of organizations under our survey use their own or external tools to analyze big sets of data, and 7 per cent say that it is their priority for the next 12 months. Overall, it is worth noting that a number of such companies is small and that 41 per cent of companies do not plan to implement such solutions at all. Poland looks rather poor against a global background. 43 per cent of the companies surveyed use this type of solution worldwide, while 24 per cent plan to implement them in the course of the next 12 months. Only slightly over 11 per cent of companies do not intend to implement such tools at all.

As in the case of large data sets, Polish companies are not very advanced when it comes to the Internet of Things (IoT). 53 per cent of the respondents have indicated that the IoT solution is not used in their companies, and only 5 per cent have declared it is used. In this situation it comes as no surprise that most companies do not have security strategies regarding the Internet of Things. Such a distribution of answers allows us to put forward a thesis that the IoT security topic is in principle non existent for Polish enterprises.

Security of industrial systems (OT – operational technology)

The OT systems are responsible for sustaining key technology processes in companies. Cyber attacks can have serious and far-reaching consequences for this environment. In addition to causing financial losses, they can cause prolonged interruptions in the delivery of critical services, environmental damages, and even posing danger to people's health and lives.

Highly qualified and well-motivated criminals actively seek to exploit security vulnerabilities in the OT networks, process control systems, and in critical infrastructure. Their motives range from economic benefits and espionage, through to a desire to disrupt work in a malicious way.

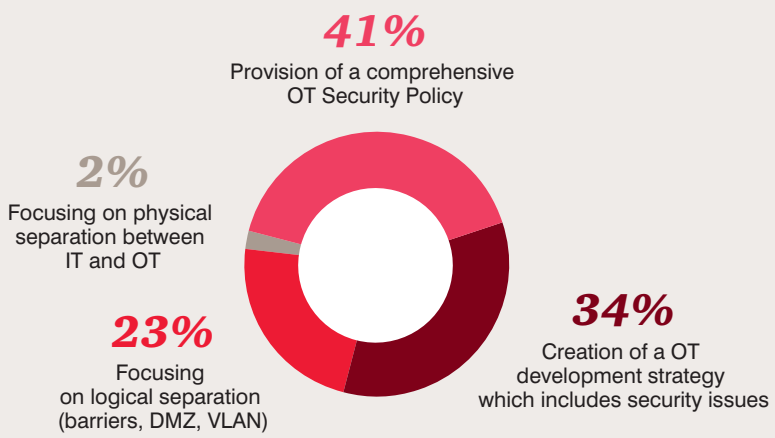
As the results of the in-depth interviews with large companies indicate, respondents are well aware of the serious implications which lurk behind OT incidents. 64 per cent of the respondents have indicated that an OT incident could break technological processes, 43 per cent have said that such incidents may leak sensitive information, and 41 per cent are concerned that they could result in damages to the infrastructure, which would entail significant costs.

As for the source of such incidents, 68 per cent of the respondents have pointed to an unauthorized access from the inside of the organization. This means that, as in the case of the IT, the greatest threat (although it is worth noting that often unintentional) comes from the staff members themselves.

68%

of incidents in the OT systems is an unauthorized access

Key elements for preventing OT security breaches



According to more than 60 per cent of the respondents, processes which support Operational Technology systems for the management of security incidents in the enterprise do require changes. This is due to the low maturity of the OT environments for monitoring security incidents, and the existence of architecture and services which are ill-prepared to handle such events. The OT systems were often designed in order to sustain technological processes, focusing mainly on the issues of accessibility. Current maintenance services face the risk of threats which in the IT world have already been taken care of in a systemic way, following the principle of the *"Security by Design"*. The security of the OT systems used to be ensured mainly through a galvanic disconnection from other computer networks. Today's business requirements and environments which inter-penetrate one another do not allow this.

A remedy for this problem may be to look at the OT systems in the context of a logical separation and monitoring security breaches, which requires a change in approach.

One can still see that companies manage their IT/OT access management locally and that they lack uniform standards for dispatching stations. As a rule, such an approach used to make sense in a single plant, but no longer now, when systems of individual units make up whole entities, or exchange information. What is currently recommendable, is to introduce central management of permissions and event monitoring, which requires significant changes in the architecture of the OT systems. The lack of a global approach across the enterprise results in a fact that access management policies are not consistent and they are repeatedly untested (monitored).

Any such change requires financial resources and, more importantly, a skillful design so as not to interrupt the technological process (some of this type of processes require supervision and control 24/7).Also, the group of specialists who both understand the OT and are familiar with the IT security issues is very small, which adds to the slow pace of the changes.

For 53 per cent of the respondents the safety considerations are a driver of changes in the OT environment in their companies. The OT safety requires a holistic approach across the enterprise and a roadmap of changes. The changes are meant not for a few years only, as in the case of IT, but for a decade or even longer. This is due to the fact that in some cases the work can be done only when there is a technological gap, and when other work is being done in conjunction. The costs of switching off and re-commissioning the equipment are huge, and many times it is just not possible. 72 per cent of the respondents have said that security-related implementations for the OT were going to be introduced by the OT teams, 51 per cent pointed to the IT departments, while 44 per cent spoke of specialized advisors or consultants (respondents could choose multiple answers).

When it comes to the OT security aspects, Polish companies are going to focus on monitoring and analyzing information tools (such as SIEM) – this is what 76 per cent of the respondents said. The second top aspect, as indicated by 42 per cent of the respondents, is the need to raise awareness and competence of staff members. Also a tighter cooperation with the IT and building multidisciplinary teams is very important.

Protecting business in the digital transformation

Research Methodology

The report was prepared on the basis of a study which involved 100 large and medium-sized Polish companies. The study was carried out in autumn 2016, via an online survey. The security aspects of operational technology (OT) were examined via in-depth interviews. The survey results are based on the aggregation of the responses.

The Polish study is part of an international project of *The Global State of Information Security® Survey 2017*, which looks at 133 countries in terms of the state of information security.

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

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

Tomasz Sawiak
Deputy Director, Cyber Security Team
Tel.: +48 519 504 234
E-mail: tomasz.sawiak@pl.pwc.com

Patryk Gęborys
Deputy Director, Cyber Security Team
Tel.: +48 519 506 760
E-mail: patryk.geborys@pl.pwc.com

pwc.pl/stanbezpieczenstwa