VOLUME 2 (2016) ▪ ISSUE 1

EUROPEAN CYBERSECURITY JOURNAL

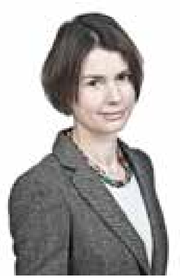
STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES

ANALYSES ▪ POLICY REVIEWS ▪ OPINIONS

THE KOSCIUSZKO INSTITUTE

ANALYSIS

HOW SHOULD PRIVATE COMPANIES DEAL WITH CYBERSECURITY?



AGNIESZKA WIERCIŃSKA-KRUŻEWSKA

Agnieszka Wiercińska-Krużewska - LL.M. – advocate, senior partner at WKB Wierciński, Kwieciński, Baer. Head of the intellectual property and TMT team, also closely co-operates with the M&A team. She advises clients on all aspects of copyrights, industrial property, consumer law, unfair competition, preservation of confidentiality, privacy and personal data protection, internet domains, press law and protection of personal rights. She also deals with the cases regarding critical infrastructure protection as well as the regulations on the transfer of military and dual-use technologies. Agnieszka represents clients in litigation and arbitration proceedings and she has also extensive experience in the acquisition of companies on the private market.
WKB Wierciński, Kwieciński, Baehr is a leading Polish law firm, providing top-tier end-to-end legal services in key areas of business law. For more details please visit www.wkb.com.pl.

Many people wonder what "cybersecurity" means exactly and whether it is applicable to private entities. This is mainly due to the fact that cybersecurity is mostly discussed in the context of terrorist attacks, state security or the functioning of critical infrastructure. Cybersecurity is rarely discussed in relation to small or medium sized companies. As result, some people expect that safeguards should be provided at the state (or European) level rather than at the level of businesses enterprises. According to PWC report [Secured Information – Secured Future – The Global State of Information Security – December 2014[1]], the number of cybersecurity incidents against private companies rises every year by around 25%. The authors of the report claim that it is almost certain that each company will have encountered an IT security attack, but some may still not be aware that it even happened.

In the early days of interconnected computers, most attacks were done for fun or the notoriety of hackers. These days, attacks are often done for money or political reasons. Currently, the global economy loses up to 550 billion dollars due to cyberattacks annually. High profile examples include: "Stuxnet" – where more than 16,000 computers of Siemens were infected with a virus that allowed to download information (2010); and "LulzSec" – where the data of more than one million Sony Playstation users was obtained. The specialised firms that make attacks to check the IT security of firms in Poland say that only 10% of tested firms are able to discover and isolate an attack.

> "Good cybersecurity practices
>
> 1. Employers – Employee Relationship
> 2. Identifying Protected Assets
> 3. Internal Policies And Written Code Of Conducts
> 4. Bilateral Agreements With Employees
> 5. Training
> 6. Monitoring Software
> 7. Specific Incidents Response Procedure
> 8. Consequences

So what is a cyberattack? A cyberattack is an attack initiated from a computer against a website, computer system or individual computer (in this article, collectively, a "computer") that compromises the confidentiality, integrity or availability of the computer or information stored on it. An attack can stop business for a while or, in some cases, forever.

Nowadays, almost every enterprise is connected to the Internet, sells through the Internet, or stores data in the cloud or on servers located outside of its place of operation, or does business with or otherwise relies on other businesses which do. Consequently, virtually every business is exposed to some sort threat connected with operating in cyberspace i.e. the networks among computers.

1 | Global Cybersecurity Index & Cyberwellness Profiles [online.] https://www.itu.int/pub/D-STR-SECU-2015 (access: 17.11.2015).

The respondents to the PWC survey discussed in the report indicate that the greatest risks for business are: an adverse impact on its reputation and the value its brand, the theft of IP rights (such as reports, data or plans), the theft of personal data (e.g. the data employees or customers), and internal administrative failures of its systems.

Most available information shows that companies in Poland are not prepared for cyberattacks. Moreover, not only cannot they stop an attack, but they often cannot even detect that it happened. In many cases, cybersecurity is the domain of IT departments (often outsourced) which are far from the core business of the company and do not understand the company's most valuable assets and risks. Further, few firms incorporate cybersecurity as an element of their business strategy.

There are various things that can be done by company to prevent or limit cybersecurity events and their consequences. A lot of companies, especially in the recent months, have increased their level security by introducing complex IT solutions to monitor and prevent network failures and data breaches. Such investments in security systems seem to be unavoidable. But such investments cannot be the sole approach to the issue.

Many IT experts say that even the most sophisticated firewalls will not protect companies against their weakest links – human beings, especially employees or ex-employees.

> Many IT experts say that even the most sophisticated firewalls will not protect companies against their weakest links – human beings, especially employees or ex-employees.

So, what else can be done? The answer is not necessarily to throw more money at the IT security systems or improve the training of the IT staff or external provider. In many cases, the IT system and staff are adequate. Rather, the vulnerability might arise principally through organisational reasons. For example:

- Employees may not truly understand the key assets of the company and, consequently, they might not know what needs to be protected.
- Employees may be careless and not pay enough attention to the assets to which they have access;
- Employees may not be properly trained and have inadequate access to clearly defined policies on how to deal with valuable assets and the devices on which such assets are stored;
- The company may not have compliance programs, internal policies and staff contracts which clearly cover cybersecurity events;
- Similarly, the contracts with commercial partners quite likely do not mention issues relating to cybersecurity;
- The company might not have insured against cyberattacks, despite such insurance being readily available;
- The company may have no risk management policies on how to react if an IT security breach occurs.

From the legal point of view, while compliance programs in this area are increasingly popular, they still are not especially common. The absence such programs often leads to the failure to prepare internal policies regarding security or, even if prepared, the failure to routinely revise and update them or communicate, or remind staff about them. Also, staff contracts are surprisingly vague on this topic. Often even key personnel have no confidentiality undertakings, no competition clauses or no clearly defined responsibilities as far as access to information is concerned.

Therefore, it is crucial to introduce good practices in the field of cybersecurity, that is:

1. Employers – employee relationship

Cybersecurity events caused unintentionally by employees can be effectively limited by building strong relationship between employees and employers, based on the employees' loyalty and awareness of the risks and consequences of breaches. The best results are achieved if employees associate themselves with the employer and treat the valuable assets as if they were their own. On the flip side, some severe security events are caused by unhappy employees or ex-employees.

2. Identifying protected assets

Before starting work on the legal framework for mitigating cybersecurity risks, the company has to define (map) its key information assets. These can include confidential information such as customer lists, pricing policies, strategic plans, designs, etc., as well as communications with business partners, and personal data kept and processed by the firm. The organisation has to be able to ascertain where the valuable information of the company lies, who has access to it and, finally, what part of this information is stored in the cyberspace. Once the key assets have been identified, in most cases, the number of employees who have to have access may be limited. For this purpose, it is important to categorise employees according to their requirements for access. The exercise should be conducted on different levels of the company and should involve as many of the personnel as possible.

3. Internal policies and written code of conducts

Critically, employees have to also be made aware what they are required to protect and why. They also have to understand, familiarise themselves with and respect policies which often involve consuming procedures. However, assuming that people in the organisation understand the importance of cybersecurity, they will generally follow and comply with policies in this respect. The implementation of the policies has be strict and non-compliance should be a subject to disciplinary penalties, termination of employment contracts or even liability for compensation.

Many companies provide employees with equipment such as a company computer or mobile phone. Moreover, some businesses allow employees to use their private devices for business purposes. In either case, not just the employer, but also the employees may be exposed to cyberattacks and may easily become victims of cyber events. For example, it is common that attacks are made by sending emails employees that links or attachments for the purpose of gaining companies' trade secrets or infecting companies' devices with unsafe software. Moreover, companies should be aware that despite the numerous advantages of providing employees with mobile devices, such practice exposes them to risks connected with loss or theft of the device which may result in unwanted disclosure of important information including trade secrets. A company's data may also be threatened by the unintended activities of employees on the Internet e.g. downloading data and saving it on mobile devices, or downloading software on the company's devices without appropriate permission. Additionally, the increased activity of employees on social media should also be taken into account. Cyberattacks are sometimes based on guesswork in respect of passwords which may be words commonly used by employees in social media.

These are just some of the reasons for implementing robust security policies, with special attention to the IT security policy and the data safety policy. Generally, the implementation of such policies does not require substantial financial resources, but the value may be significant.

An IT security policy has to be prepared on a case by case basis. Samples of such documents can be found on the Internet, but these should be used with caution because they are unlikely to apply to the specific circumstances of a given business.

The internal IT documents usually have one of the three forms: a policy (a binding document that is usually incorporated into the terms of employment), workplace standards or guidelines (each being documents that describe certain technical procedures or suggest certain behaviours). The IT security policy should have the form of a binding document that is approved and announced by the governing body of a company rather than being a mere guideline issued by the IT department. The IT security policy has to be easy to read and understand, and has to be adapted the organisation in terms of subject matter, the IT system used, the size of the company, etc. The terms of the policy should be enforceable and should stipulate requirements on a "do it" / "don't do it" basis. Before being announced, the document should be broadly discussed and subject to comment. The staff of an organisation are often the best critics and may have valuable suggestions. All policies should spell out consequences for non-compliance. However, in order to take account of the variety of situations in which breaches may occur, the employer should always reserve the right not to impose them against a violating employee. Furthermore, each organisation still has to focus on doing its core business. For that reason, each and every policy has to be reasonable and should avoid imposing onerous limitations in a blanket manner when such requirements are only applicable to extreme situations.

What are the main areas that the employer should focus on in the policy?

Use of private equipment: In the event that employees use their private equipment for business purposes, there should be a policy covering such arrangements. The policy should allow the use personal devices for business purposes only under certain conditions e.g. only if such device is protected by special programs which effectively detect and remove viruses. In some companies, especially where trade secrets require strong protection, it is justified to prohibit the use of private devices for business purposes. Use of the company's equipment for private purposes: Due the common availability of IT devices, the use of company's equipment for private use is less frequent than a couple of years ago. Still, it constitutes a major risk to IT security. Some basic restrictions should be imposed such as prohibition on using the same logins and passwords as for privately used devices, a prohibition on providing a company email address to privately used services, a prohibition on making a company device accessible to third persons, and a prohibition on visiting certain types of risky websites on Internet. The employees should also be made aware which programs can be installed and kept on their company devices. Moreover, they should be instructed about spam filters and how to use them to prevent the impact of harmful spam. Password policy: The policy should also include provisions concerning requirements regarding passwords for IT devices. In particular, employees should be obliged to set a password which consists of a required number of characters, including lowercase and uppercase letter, numbers and special characters. Furthermore, in order to give greater security, employees should change their passwords regularly, and important data should be backed up frequently. Unknown email policy: The policy should prohibit opening any suspicious email and should require that such emails be forwarded to a specialised IT department for assessment. For clarification, all policies should include examples of prohibited or desired actions. Furthermore, even the best IT security policy is useless if employees are not aware of its existence or are not trained on its proper application.

4. Bilateral agreements with employees

Another form of protection against cybersecurity events which is a common and recommended practice is to conclude non-disclosure agreements with employees. Such agreements oblige the employees not to disclose any confidential information covered by the contract. Apart from employees, non–disclosure clauses should be included in all types of contracts with people who may have access to the enterprise's trade secrets. A non-disclosure undertaking can be concluded not just for the period of employment or other access, but also for a period after the termination of employment or other contracts. In such cases, the undertaking may even stipulate contractual penalties or liability for compensation for any breach. However, a provision on liquidated damages may not be valid in every jurisdiction.

5. Training

An important security measure is to expose employees to fake targeted cyberattacks and follow up with training. Nothing works better to focus the minds employees than to become aware that they were the weakest link. The employer should inform employees that such attacks may be performed without notice and failure to obey the policies may be a reason to impose disciplinary action.

6. Monitoring Software

Employers should consider whether to monitor employees' work. This is becoming an increasingly common method of protection. For example, it is possible to install software such as keyloggers on employees' computers that enables employers to track all activity. Within certain groups of employees, this should be considered a justified form of protection.

On the other hand, most European labour legislation imposes a duty on employers to respect employees' privacy. For this reason, employers should inform employees in advance about using such software or other monitoring measures.

7. Specific Incidents Response Procedure

Every company should develop a plan (cyber incident response plan) that identifies possible cyberattack scenarios and sets out appropriate responses. The plan has to be customised for each company's particular circumstances. Such plan should address the following basic areas: define the response team composed representatives of different departments such as IT, legal, information security, PR, insurance; provide for reporting channels, define the scope and manner of investigation, designate a recovery and follow-up plan and management of public relations and law enforcement.

> Every company should develop a plan that identifies possible cyberattack scenarios and sets out appropriate responses

8. Consequences

If an employee does not comply with the required procedures, such behaviour may be treated as a breach of its obligations as an employee. Pursuant to most European labour legislation, employees who disobey IT security policy are responsible for the resulting damage to the extent of a material loss sustained by the employer although, in some jurisdictions, during the term of an employments contract, the employee cannot be obliged to pay contractual penalties. Moreover, employers may apply disciplinary penalties with respect to employees who do not observe the rules. In some cases, a breach of duty provided for in the company's IT security policy may lead to termination of the employment contract without notice because it constitutes a violation of basic duties. However, what if the employer has no policies or other measures in place? In most cases, the lack of awareness means that there is limited exposure for and fewer consequences that may be imposed on the employee. In short, it is the employer's duty to define the scope and means of security.

In summary, the policies should give a roadmap of tasks and responsibilities to manage the risks and to make employees aware that each of them has a role and should strive not to be the weakest link. ■