Cyber Security: A threat for all businesses

Christophe Szwedo and Laurent Le Pajolec look into the ramifications of the new General Data Protection Regulation (GDPR) on all businesses

CHRISTOPHE SZWEDO
CYLRESC, France

LAURENT LE PAJOLEC
EXCO A2A Polska – INSOL PL

Share your views!

Nowadays, a company, whatever the business sector, relies on an information system which must be protected with specific means.

With a rising number of cyber-attacks, cyber-security is a hot topic and companies are trying to secure their information systems. Though, the sole fact of putting a firewall or using a VPN connection to access your information system is not enough, besides, those must be installed and configured properly by cyber-security experts. Implemented means against cyber-attacks and cyber-criminals should neither be overlooked, nor underestimated.

One often hears things like: "I don't need to audit or strengthen my information system, who would attack my company? I have no enemies and I don't handle any sensitive data".

The part about not having enemies and handling sensitive data might be true, but your company may be an intermediary to the real target and hackers will try to reach any person close enough to it. As a law firm, you may be the perfect target for hackers because, through your company's information system, they can get access to sensitive data about your customers. Moreover, even if you are not their true target, hackers are greedy and if their penetration test succeeds, they might just as well drop a ransomware on your network and ask you to pay if you want to recover your data. Of course, it is NOT recommended to pay: 53% of the companies which pay do not recover their data after paying. The success of the recent attacks known as "Not Petya" and "WannaCry" proved that companies are not spending enough time thinking about how to improve their cyber-security system.[1]

A few figures here: 55% of the French companies declare having been victims of a cyber-attack in 2016. Half of them declare the cyber-attack had an important impact on their productivity. 23% declare having issues maintaining their reputation after an attack. 60% of the small companies attacked close in six months after a cyber-attack.[2]

Cyber-security: How to be protected?

Protecting the company against cyber threats forces the companies to formalise processes, identify sensitive data and sensitive areas in their information system and strengthen them by implementing cyber-security means such as firewalls, a password policy, mandatory Full Disk Encryption (FDE), etc. It is important to understand that formalising processes and strengthening cyber-security becomes essential for a company to exist. Today, the management of cyber-security seems to be reserved for companies handling sensitive data, whereas it should be part of any company's life cycle.

An attacker can easily compromise an unprotected information system by sending e-mails with infected attachments to the whole company. It is called *phishing*. Phishing attacks aimed at an individual will try to steal his/her social media account or bank account credentials. In the case of a company, it can simply send an attachment, which once it has infected one computer will spread through the whole network like a worm. Phishing attacks are

usually paired with ransomware attacks. The amount of phishing e-mails containing a form of ransomware grew to 97.25% during the third quarter of 2016, up from 92% in the first quarter.[3] The form of such an email is realistic (copy of email address / copy of format, for example, false "energy invoice"…)

Security strength is evaluated according to the weakest link in the information system.

Hackers have well understood this concept, and that is why there are growing numbers of phishing attacks. It is true that you can have the most sophisticated security, a state-of-the-art defensive system with strong restrictions on networks streams, but an employee can undo everything just because of one mistake such as opening the wrong file, plugging a USB flash drive found on the parking lot with the name of a competitor on it, and so on.

Experts in cyber-security can do an *audit* of your company, consisting in taking a picture of your information system, analysing it through code reviews, architecture reviews and configuration reviews and thus ensure that it is well secured and compliant with known cyber-security standards.

Penetration testing is also useful, and it consists in testing the security of the company's information system in real conditions. An auditor comes to your premises and acts like an evil employee trying to harm the company, without, of course, doing anything that might impact the productivity, unless the auditor has the company's approval to do so. The audit and the penetration test result in a report that contains all discovered vulnerabilities and the recommendations associated to those vulnerabilities.

Awareness training is also important because one cannot "configure" a human being as it is done with a computer. Employees should feel concerned about the cyber-security of their company and for this, simple gestures, such as locking the computer when away (even for three minutes), using complex passwords or a password manager to access professional and internal web services, are contributing to reinforce the cyber-security of the company.

Becoming "GDPR-Ready"

Nowadays the European Parliament intends to strengthen data protection for all individuals within the European Union through the General Data Protection Regulation (GDPR or the Regulation, in this article), which will be in force in May 2018.

If a company does not meet the requirements defined in the GDPR, it may receive a fine of 20m euros or 4% of the annual worldwide turnover of the company (whichever is higher). 52% of the companies believe they will be fined for non-compliance. (Article 83 from GDPR)[4]. The GDPR aims to the have the following personal data protected by all companies:

- Name, address and ID numbers
- Location, IP address, cookie data and RFID tags
- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation.

The Regulation defines, for example, that the company needs to be able to locate and, if requested, provide all personal data they have collected on an individual. If the company is not able to fulfill that request and an individual decides to file a complaint, it may receive a fine.

Being GDPR-compliant, proves that the company:

- has created processes and is mature enough to locate and protect all stored personal data;
- can identify which application uses these personal data; and
- can identify who has access to it.

A strong principle of the GDPR, is the "accountability". If a hacker succeeds to steal personal data from one of the partners of a company, the company itself is considered just as responsible of that leak as your partner's company, and so even if the company is GDPR-compliant. This is the main reason of why being "GDPR-Ready" is a *pledge of trust*. It means the GDPR could really become a competitive advantage or at least, a necessary means to cooperate with other companies.

Going through the GDPR-compliance process helps every company not only to protect personal data of its employees, clients, suppliers and other stakeholders, but also to strengthen the company's cyber-security (firewall protection, data encryption, least privilege principle …), to implement *basic* security means in order to ensure that no personal data leak or are accessible to unauthorised persons.

Conclusion

- All companies will be attacked directly or indirectly. It is a question of time.
- Cyber-security is a universal topic:
  - for companies and their clients;
  - for small and large businesses.
- Any company processing personal data of European citizens will have to be compliant with GDPR.
- **As a member of INSOL Europe, you should take care to see that your company becomes GDPR-compliant!** ■

Footnotes

1 www.orange-business.com/fr/blogs/securite/actualites/infographie-barometre-cybersecurite-2017-ou-en-est-l-industrie-francaise-
2 www.inc.com/thomas-koulopoulos/the-biggest-risk-to-your-business-cant-be-eliminated-heres-how-you-can-survive-i.html
3 http://cofense.com/wp-content/uploads/2017/10/PhishMe_Malware_Review_2016_Q3.pdf
4 www.privacy-regulation.eu/en/article-83-general-conditions-for-imposing-administrative-fines-GDPR.htm

"AS A MEMBER OF INSOL EUROPE, YOU SHOULD TAKE CARE TO SEE THAT YOUR COMPANY BECOMES GDPR-COMPLIANT!"