Cyber attacks – preventive measures and notification obligations in Switzerland

Dr. András Gurovits, andras.gurovits@nkf.ch

In this paper we would like to discuss the measures that may be considered in the prevention against cyber attacks and the duties a Swiss company may have if it has become the victim of a cyber attack. This paper is based on the presentation made at a customer event of Niederer Kraft Frey Ltd on 27 February 2020.

1. How does Ransomware get installed?[1]

When turning to preventive measures and looking at what can be done to protect against cyber attacks it is important to understand how cyber attacks take place. Cyber attacks can take different forms. For the purpose of this paper, this question will be discussed using the example of ransomware attacks. Crafting and implementing preventive measures against cyber attacks is, of course, primarily a technical question and the details in planning and implementation must be left to the technical specialists. However, since the failure to take appropriate preventive measures can ultimately have legal consequences, the author of this paper is venturing into this area. The technical specialists among the readers will hopefully forgive if the following discussion only addresses a few fundamental points.

The central elements of a ransomware attack can be summarized as follows: Everything usually starts with a malicious email sent to different recipients within an organization. This e-mail contains a link to a malicious website or an infected attachment. Clicking on the attachment or the website opens an access to the company's network. And this access to the infected computers is then offered for sale in corresponding Internet forums. Criminals then buy these access points through which they then import ransomware that encrypts the data and systems of the affected company. This paralyses the IT infrastructure of the affected company. When the culprits knock on the door of the affected company and demand the payment of a ransom, the pressure on the affected company to pay the ransom is naturally very great. Whether or not the company concerned should pay such a ransom is something we do not wish to discuss further in this paper. In any case, the position of the criminal prosecution authorities in Switzerland is clear: they strongly advise against paying a ransom because such a payment would of course motivate the perpetrators to carry out further cyber attacks.

2. Precautionary measures

2.1 Organizational measures

The preventive measures can be divided into organizational and technical measures. The laws, especially data protection laws, contain a number of references to this, e.g. Art. 7 of the Swiss Data Protection Act

[1] Some of the technical parts of this paper have been inspired by information provided by the Swiss Reporting and Analysis Centre for Information MELANI, accessible at www.melani.admin.ch

and Art. 8/9 of the Swiss Data Protection Ordinance as well as Art. 32 of the General Data Protection Regulation (GDPR). What all these laws have in common is that they refer to the state of the art. As far as the current state of the art is concerned, a comprehensive description of relevant processes can be found in the ISO regulations, in particular in ISO 27001. In order to give data security the necessary weight and also to gain the trust of their business partners, more and more companies are having themselves certified under ISO 27001.

In the following we will briefly summarize the measures we have identified in our practical work as being effective in order to be best prepared for a cyber attack or to be able to react to it. The focus should now be on this alone, and not on a comprehensive analysis of appropriate data security measures as a whole.

Appropriate organizational measures include carrying out a basic assessment of the effects an IT failure can have on the entire business of a company. This also includes defining those IT assets that are critical to the ongoing business. Building on this, it is advisable to define the possible work around solutions that should be available in the event of an IT failure. At the organizational level, it is also important that an incident response team is formed that can start work immediately in the event of a cyber incident. This also means that the company's employees must know where to turn in the event of a cyber attack. An incident response plan should also be defined, which specifies the relevant processes if a cyber attack occurs. It should also define the processes that employees must follow if they notice something suspicious. In order to be ready in case of an emergency, the incident response plan should be implemented and tested regularly. It is equally important that employees are trained in terms of breach awareness, employee responsibility and reporting process. In the author's opinion, this also includes carrying out targeted intrusion tests. For IT managers in particular, it is then important to build up a real knowledge base about cyber incidents in order to be informed about the current threat situation. The regular cyber incident releases from MELANI are also helpful in this context.

Another important topic is the design of the company website. Here, one should be careful about what information about the company actually wants to make publicly accessible and always consider whether the information is potentially security-relevant. Another practical measure is to ensure that security is guaranteed throughout the entire life cycle of IT assets, from procurement to disposal. And it is actually a matter of course today that systems, especially if they are remotely accessible, are checked by an appropriate password policy and two factor authentication.

2.2 Technical measures

As regards technical measures, it should be a matter of course today to equip the company's systems and networks with appropriate virus protection, firewalls and spam filters. As far as the back-up processes are concerned, it must be ensured that these are carried out regularly. The back-ups must then be stored or kept offline to prevent them from being infected in the event of a cyber attack. It should also be ensured that regular tests are carried out to ensure that the back-ups can be properly installed in the event of a system failure. Another important technical measure is to store the log files of critical systems. In addition, the log files should also be checked regularly to see if there are any suspicious entries that could indicate an impending attack.

With regard to the networks, it should be examined to what extent they can be separated within a com-

pany or group of companies in order to prevent the spread of malware. It goes without saying that all system security updates should be installed regularly, as this is the only way to ensure that the security systems can react to the latest developments. Another measure is to define the system settings in such a way that every user can access the systems on a need-to-know basis. Only those user rights that are absolutely necessary for the execution of the respective tasks are to be assigned. It should also be checked whether and to what extent the data should be stored in encrypted form. This applies in particular if sensitive data is stored or made available on mobile devices. In the case of remote access systems, it must then be ensured that proper authentication processes are used.

3. Notification duties

With the above, the topic of organizational and technical measures shall be left and in the following the question of which obligations arise when a company is affected by a cyber attack shall be discussed. For purposes of the present paper, this discussion shall be limited to the question of notification duties. These notification duties are primarily to be found under the applicable data protection laws.

3.1 Does ransomware attack trigger "data breach" that is to be notified?

In the case of a cyber attack with ransomware, the fundamental legal question arises as to whether such a cyber attack leads to a data breach at all, which must be reported to the authorities in accordance with the data protection laws, for example Art. 33 GDPR.

In our practical work we could establish that ransomware usually "only" encrypts data and systems. This encryption then leads to a loss of availability of data and to business interruptions. But the question is whether such an attack also leads to unauthorized access to personal data and/or misuse of personal data that must be notified. In our experience, this is not necessarily the case, which is why the question can be asked whether in the case of a ransomware attack one should even take the effort to notify the authorities, where there is an obligation to notify in the case of a data breach. And indeed, in one specific case we received the answer from the UK ICO that in the view of the ICO, the reported ransomware attack did not constitute a data breach in the sense of the GDPR. The unpleasant thing about such an attack is, however, that the further course of the attack cannot be predicted and the possibility of a data breach within the meaning of the GDPR cannot be excluded. For this reason a notification on a precautionary basis seems always to be recommended.

3.2 Notification duties

3.2.1 In general

Depending on the area of activity of a company, there may be far-reaching notification duties. A further preventive measure in the event of a cyber attack is, therefore, to make the company ready in case of a cyber attack. In the author's view, this also means that the company should clarify in advance where and what notification duties exist, so that it can then react quickly in an emergency. If there is a cyber attack that paralyses the system, the stress is already great enough, so it is an advantage to know already where you have to notify when and how. When making these assessments, it is important to bear in mind that the effects of a cyber attack are not necessarily limited to data breaches that must be reported in accordance with the applicable data protection laws. Against this background, a distinction must

be made between notification duties under the data protection laws and other laws. A distinction must also be made between notification duties in Switzerland and possible notification duties abroad.

3.2.2 Notification in Switzerland

Under the Swiss Data Protection Act as it stands today, there are no mandatory reporting requirements. What does exist is the possibility of reporting a data breach to MELANI, and reporting to the Federal Data Protection and Information Commissioner (FDPIC) is also possible and recommended. But, unlike in the EU, there is no obligation to notify under the current Swiss Data Protection Act. However, the Data Protection Act is currently being revised and it remains to be seen whether Switzerland will also introduce such a notification duty in the future.

In addition, there are also possible sector-specific rules that require notification. These notification duties are generally not limited to cyber attacks, but relate in a general way to disruptions or problems. Some examples of such notification duties can be found on the slide. These are reporting obligations to the relevant supervisory authority under the Aviation Act, the Nuclear Energy Act, the Electricity Supply Act or the FINMA Act.

3.2.3 Notification duties in the EU

If a Swiss company or group of companies is also active abroad, it is advisable to have clarity as to whether reporting obligations also exist abroad. The reporting obligations under data protection legislation, i.e. the GDPR, are also a priority. The obligation to report to the data protection authority is found in Art. 33 GDPR, and the obligation to notify the data subjects is found in Art. 34 GDPR. In addition, however, it should also be examined for the EU whether there are any other reporting obligations under other laws.

3.2.4 Notification duties in other jurisdictions

And of course the same scheme also applies in other countries. For example, Canada also has reporting requirements under Canadian data protection legislation. And in Brazil, for example, there is an obligation to report to the tax authorities under certain circumstances.

4. Do Swiss companies have to notify in the EU?

4.1 Introduction

Following these general remarks, we would now like to examine more closely when a Swiss company is actually obliged to make a notification in accordance with the GDPR regulations if a data breach has occurred. The main question here is whether and when the GDPR is applicable to a Swiss company at all. The answer can be found in Art. 3 GDPR. According thereto, the GDPR applies to the processing of personal data in the course of the activities of an establishment of a controller or a processor in the Union, whether or not the processing is carried out in the Union, if the processing is directed at a data subject in the Union. The GDPR also applies to the processing of personal data of data subjects located in the Union by a controller or a processor not established in the Union where the processing activities are related to the provision of goods and services to data subjects in the Union or to the monitoring of the

conduct of data subjects in the Union.

4.2 Specific issue for group of companies headquartered in Switzerland

For a Swiss company or group of companies that wants to comply with the GDPR, the specific problem of where to report in the EU arises, especially if the group is represented in several EU countries. The main question here is whether the Swiss company could also benefit from the one-stop-shop principle under Art. 56 GDPR. If the company could benefit from this, it would only have to report in one country. This raises the difficult question of which would be the lead supervisory authority within the meaning of Art. 56 GDPR. The lead supervisory authority is defined as the authority of the "*main establishment*" of the company. And the main establishment is defined in Art. 4 (16) GDPR as the "*place of the central administration in the Union, unless the decisions on data processing are taken in another establishment in the Union*". The main establishment is therefore the unit within the group of companies in which the essential decisions on data processing are taken. According to the provisions of the GDPR, this unit should not be confused with a European head office, which the group of companies has in the EU.

The French data protection authority, Commission Nationale de l'Informatique et des Libertés CNIL, has clarified this in a landmark decision. On 21st January 2019 the CNIL ordered that the company Google LLC be fined 50 million euros for breaching the GDPR. The French data protection authority acknowledged that Google's European headquarters are located in Ireland. However, the CNIL did not consider this European headquarters to be a "*principal place of business*" within the meaning of the GDPR. In particular, the CNIL did not consider the European headquarters to be the place where decisions on data processing within the group were made. As the CNIL considered that the European headquarters did not have the power to take decisions on data processing, it rejected the Irish Data Protection Authority as the lead authority and considered itself competent to impose a fine on Google LLC.

4.3 Conclusions for group of companies headquartered in Switzerland

The consequences of this decision for a group of companies with headquarters in Switzerland are serious. If the decision-making power on data processing operations lies with the Swiss headquarters, there is no lead authority in the Union in the sense of the GDPR. For this reason, the one-stop-shop privilege under Art. 56 GDPR is not available to a Swiss company. This conclusion is also confirmed by a legal opinion from leading UK firm available to the author.

This means that in case of a data breach notifications must be made in all countries of the Union where the data breach has an impact. This also exposes the company to the great risk of being fined several times in the event of a breach of the GDPR. For this reason, the CNIL's decision has been criticised on several occasions, but it must still be respected. The question that might arise in this context is whether a different conclusion should be drawn if the company has appointed a representative in the Union within the meaning of Article 27 of the GDPR. In my opinion, however, this is not the case, because Article 27 and Article 56 of the GDPR regulate different situations.