CYBER-COMPLIANCE IN THE SHADOW OF THE PANDEMIC A CYBERFRAUD CASE-STUDY

Running a business in the pandemic era, including switching to remote working, has opened multiple doors for cyberattacks. Cybercriminals become more skilful in using new technologies and social engineering to their advantage. They know that human error is the key to success. A cyberattack may cause severe losses, including financial ones, for the company. To minimise potential losses, cybersecurity guidelines adopted by organisations should be given a closer examination.

Cybersecurity in the pandemic era

Since the beginning of the pandemic, the number of cybercrimes has increased significantly, including:

> **hacks into security systems, data breaches** and confidential information theft;

> **blackmail through ransomware**, i.e. computer software programmes that block access to data owned by the blackmailed company or disable the company's usual operation. The latest example of such an attack is the case of the highly digitized Colonial Pipeline, USA;

> **money transfer fraud**, pursued by rerouting a payment originally intended for the business partner to the fraudster's bank account in another bank.

The latter category of incidents employs cyberspace and IT tools, in particular those used to interfere with electronic communication (business e-mail compromise), combined with social engineering, resulting in the impersonation of e.g. a contractor or an insider (e.g. director of the organization).

Caution is often not paramount during the pandemic. With the attention of entrepreneurs focused elsewhere: on maintaining business profitability, compensating for losses, and maintaining good relationships with the clients, criminals can get the upper hand. **Ending pandemic restrictions and the accompanying enthusiasm can also be a critical moment facilitating cyberattacks**. In such circumstances, the entrepreneur should pay special attention to cyber-security issues in its organization.

Disregarding the company's current guidelines (procedures) or the lack thereof may result in detrimental financial, legal (e.g. due to a personal data breach) and reputational consequences. These may in turn be borne by individuals within the organization.

For these reasons, let us have a closer look at how cyber-compliance guidelines are used in practice to eliminate the risk of payments for the benefit of cybercriminals. We present a typical scenario below.

A (common?) case study

Two business partners (for the study, we assume that they are foreign business partners) maintain long-lasting business relationships under which Business Partner 1 purchases from Business Partner 2 goods necessary for production purposes. Payments for the delivery of goods are based on invoices forwarded in electronic form, via bank transfer to the bank

account indicated on the invoices. The bank account has remained unchanged for years. Correspondence regarding payments is exchanged by e-mail,. Persons who are responsible for financial matters on both sides stay in touch on an ongoing basis and their communication has a friendly tone.

Due to a significant order, a high-amount invoice is issued. The due date is near and Business Partner 1 receives a message from what seems Contractor 2' legitimate email address. The alleged Contractor 2 wants to know when the payment will be made **and requests that it be made to a different bank account**. The reason is an audit which the usual bank account is currently undergoing.

The indicated bank account is maintained (again for the study) by a bank based in Poland, a country unrelated to the economic relationship between the Business Partners. The style and linguistic correctness of the email informing about the change of the bank account do not raise doubts as the latest correspondence is not different from previous emails. The e-mail address from which the messages are sent is seemingly legitimate and does not raise any doubts, either.

Once the number of new bank account has been sent, Business Partner 1 receives a series of enquiry messages requesting information on when the transfer will be made as well as asking for confirmation of the transfer.

Business Partner 1's bank receives an order of payment and the transaction is made.

Whether Business Partner 1 sustains damage depends on how quickly they will become aware that they have fallen victim to fraud, as well as on the reaction of the bank keeping the account to which the money has been transferred.

The scenario may occur in many variants. How credible and genuine the misleading narrative has been may result from i.a. to what extent and for how long the company's IT system has been compromised.

Diagnosis: how did that happen?

Common as it may seem, the implementation of the above scenario is a result of an array of mechanisms that lead to decisions harmful to the company.

First of all, cybercriminals break into the security software of the IT system. It enables them to monitor the organization's activity from the inside, learning how it operates and obtaining data about its crucial transactions. Criminals can also obtain sensitive information about critical moments of the organization's activities, such as the regional CEO's visit or closing of the financial year. Such events may exert pressure, which may, in turn, result in **lower vigilance** concerning other spheres of the company's operations. A security breach also enables cybercriminals to monitor the communication between the company and its contractor in terms of transactions settlements.

Such knowledge allows fraudsters to interfere at the right moment with the email correspondence on payments. They take control of business communication, including email forgery and interfere with the content of the correspondence.

Manipulation of e-mail correspondence is often carried out using **e-mail addresses created for fraud, confusingly similar to those used by real contractors**. Differences in e-mail addresses can be difficult to notice. For example, a capital “i” is replaced with the letter “L” written with a minuscule; a dash between two elements of the e-mail domain may be removed; one character may be added to the last element of thee-mail domain; and “.com” may be replaced with another TLD, e.g. “.eu” or “.pl”, depending on the context.

These changes are hardly discernible, especially in fast-paced business relationships. Quite often, as a result of interference with the IT system, cybercriminals take control of the e-mail address used by the contractor.

Cybercriminals are also capable of circumventing the requirements that may result from e.g. internal accounting procedures such as the issue of an invoice including information of a new bank account or confirmation by the contractor's management that the bank account has been changed. Practice shows that such documents can be easily forged in the digital era, especially if cybercriminals have been carefully monitoring the company's activities.

In addition to new technologies, fraudsters skilfully use **social engineering techniques**, knowing that their success depends on **human error**. Insider knowledge of the organization enables them to impose pressure on the decision-maker responsible for financial settlements or taking advantage of friendly communication between persons responsible for settlements on the part of the contractors. The pandemic itself creates fertile ground for manipulating reality.

Thus, features of communication such as style or language are important. In one case, the fraudster impersonating a contractor's financial director called the financial director of a company obliged to make a payment to “confirm” the change of the bank account. According to the director who was the victim of the fraud, the person's voice on the phone sounded like the actual voice of the financial director employed by the contractor.

All these measures aim to render the narrative about changing a bank account credible, even if the new bank account is maintained by a bank in an “exotic” country from the perspective of the business relations between the contractors. Internal payment processing procedures are also often breached (e.g. although paper invoices are required, the payment is made based on an invoice sent in electronic form).

Preventative measures

Often companies that have been attacked realize that the attack occurred only after a long period, whilst the more time passes from the unauthorized interference, the more harm it can cause.

In today's world, the question of whether you might be subject to a cyberattack is rhetorical. The key question is when and how you will be attacked. **To minimize the effects of cyberattacks, it is vital to implement and rigorously follow a few basic principles**:

- **cyber-compliance, including trainings,**
- **verification of the effectiveness** of IT security systems,
- **crisis management** in the event of a cyberattack.

If a transfer is made, the money is blocked by the bank and law enforcement authorities are notified, the authorities may decide to initiate criminal proceedings. It is advisable to join the proceedings as an aggrieved party. Joining the proceedings and starting a dialogue with the law enforcement authority may contribute to the faster release of funds and their return to the company. However, it should be taken into account that the funds may return to the victim only after a few months; in the same cases, it may take a year or longer.

Thus, following cyber-compliance guidelines and common sense, we should remember the golden rule: if something seems suspicious, it probably is and needs to be checked.

———

If you have any questions, contact me at my email address below.

Aleksandra Stępniewska – counsel, advocate
aleksandra.stepniewska@wkb.pl