CYBERCRIME: RISKS IN INTERNATIONAL PAYMENT TRANSACTIONS

I. BUSINESS ACTIVITY IN THE DIGITAL WORLD: CAUTION IS ADVISED!

Today, more and more business activities and professional activities are shifting to the digital world. The coronavirus pandemic has contributed significantly to this trend, as it has forced us to adapt to new realities. This situation, as well as the efficiency and convenience of remote work, has created a new working reality, which in turn brings new risks of which many of us were previously unaware. We are talking about cybercrime, which companies in particular can suffer. While we think this issue will certainly never affect us, we should not underestimate it too much, especially as we have seen an increase in this type of crime lately.

II. CYBERCRIMINAL MODUS OPERANDI

A common method used by perpetrators is trying to pretend to be a regular business partner of a company through fake email addresses to change account numbers to which payments related to transactions are transferred. In most cases, only one letter of the original (correct) email address is changed during falsification, so that the change is not easily recognisable. The relevance of this topic must be highlighted: If a company is the victim of such a criminal offence, the criminal proceedings often last for years. This is not only due to the difficulty of identifying the perpetrators, but in many cases also the need to initiate proceedings in cooperation with authorities in other countries. This need arises from the fact that perpetrators of this type of crime are usually criminal groups operating in and out of multiple countries. If a cybercrime is committed within the EU, this can be seen as less problematic. However, if this is an incident involving third countries, serious problems may arise because collaboration between the competent public prosecutors seems practically impossible.

III. BETTER TO PREVENT THAN TO SUBSEQUENTLY LIMIT DAMAGE

Precautions can be used to minimise the risk. The mere fact that precise bank details are recorded in contracts with the contractual partners is enough. Consequently, changes to this information could only be made on the basis of an addendum. A situation that can lead to a change in the account number should be checked closely as to whether, for example, the new bank account of the business partner is managed in the country in which it actually operates.

If the bank account is changed, additional controls are recommended, in particular by management, to determine the authenticity of such changes. In any case, the importance of having in-house procedures, including work regulations and other internal regulations, in the event of an attempt at fraud, and the importance of training for employees must always be pointed out to prepare and raise awareness of possible cyber threats.

IV. RESPOND QUICKLY TO CYBER INCIDENTS

If you have been the victim of such a crime, it is crucial to act immediately.

Experience shows that employees who are involved in such cyber fraud often experience a kind of shame about their own behaviour and try to contact the perpetrators directly. However, since every hour counts here, employees should be made aware that they should not act on their own, because in such a case it is not only important to proceed quickly, but also appropriately. First of all, the bank with which the business account is held must be notified as quickly as possible in order to stop (if still possible) transfers to the fraudulent bank account. If the funds transferred can unfortunately no longer be collected by the bank, legal steps must be initiated immediately.

If you have any questions about cybercrime or need legal support in a cyber incident, please consult our experienced experts.

CONTACT

Austria
Philipp Leitner
P.Leitner@scwp.com

Bulgaria
Cornelia Draganova
Cornelia.Draganova@schindhelm.com

China
Marcel Brinkmann
Marcel.Brinkmann@schindhelm.com

Czech Republic/Slovakia
Monika Wetzlerova
Wetzlerova@scwp.cz

France
Maurice Hartmann
Maurice.Hartmann@schindhelm.com

Germany
Rüdiger Erfurt
Ruediger.Erfurt@schindhelm.com

Hungary
Beatrix Fakó
B.Fako@scwp.hu

Italy
Tommaso Olivieri
Tommaso.Olivieri@schindhelm.com

Poland
Konrad Schampera
Konrad.Schampera@sdzlegal.pl

Romania
Stefan Pisargeac
Stefan.Pisargeac@schindhelm.com

Spain:
Axel Roth
A.Roth@schindhelm.com

Turkey
Gürkan Erdebil
Gurcan.Erdebil@schindhelm.com

Publisher, media owner, editorial office: Lozano Schindhelm SLP | Conde de Salvatierra 21 | E-46004 Valencia | VAT. No.: ESB97548135, registered in the Commercial Register of Valencia, T. 8034, L. 5327, H. V-101900 | Tel: +34 963 28 77 93 | valencia@schindhelm.com | Lozano Schindhelm SLP is a member of Saxinger Schindhelm Services SE, Alliance of European Commercial Law Firms. | All information is subject to correction in spite of careful processing and cannot replace individual advice in individual cases. The liability of the authors or the publisher is excluded.