## Anticipating Crisis: Preventing Information Leaks

Wojciech Wandzel, Maciej Truszkiewicz

"Better safe than sorry!" Despite the fact that this proverb is well known, lawyers often fail to apply this rule with respect to data protection. They seem to forget that information is the most valuable asset and that their law firms are susceptible to cyberattacks. Therefore, lawyers should be adequately prepared to secure data and address information leakage incidents. The first step of this preparation is crisis anticipation, which helps avoid the crisis in the first place and also gives necessary confidence to react effectively.

### Change Your Attitude

First of all, without changing their approach to the issue, lawyers will not effectively anticipate the crisis. Only the fulfillment of this factor allows lawyers to address the problem comprehensively and understand its importance. Moreover, lawyers are advised to keep in mind that the issue at hand is a subject of concern not only to IT staff, but also to the whole law firm. Thus, it is essential to secure the cooperation between IT employees and nontechnical staff. With that cooperation, it is possible to collaborate and determine potential threats, countermeasures, and funds that can be committed to reduce the risk level.

### Deploy Internal System

When lawyers are aware of the issue, they may then take appropriate steps to address the risk. One of step is to deploy an internal system that identifies events causing the crisis. It is also desirable to divide potential causes of the crisis in different groups and prepare scenarios to deal with the crisis caused by the distinguished events. Primarily, decisions required to be taken in case of the crisis should be identified—for instance on the basis of past events or experience of other entities.

Furthermore, the internal system should be able to alert about the crisis immediately and to address the issue. Law firms should hire IT specialists and deploy and maintain proper software and hardware. It is highly recommended, however, not to use cloudbased filesharing, as it may result in data leakage, usually due to unintended mistakes committed by users. Some firms actually block access to such software.

The deployment of the aforementioned systems alone are not sufficient to prevent data leakage. It is also required to maintain them in good condition by performing system updates regularly.

### Use Proper Technology

Nowadays, the circulation of information between lawyers and their clients is almost solely dependent on the use of technology. Therefore, it is crucial to use devices and methods that provide security. The first proposition is to deploy appropriate software to detect and counteract data leakage. Secondly, in terms of internal and external communication that contains privileged information, lawyers are urged to use only encrypted laptops, cell phones, or other mobile devices. It is also highly recommended to deploy a system that would automatically encrypt all emails sent both to the clients and other workers. Encrypting internal messages is not necessary if the messages are sent using an intranet system, which is advisable to have inside the firm to store privileged information. On the other hand, using tracking technology systems is undesirable because they may download information that the owner may not want to share.

### Educate Your Workers and Have Written Policies

One of the most common causes of data loss are inadequate training of employees. Data theft often requires some activity or inactivity of an employee who, if educated, would recognize the attack and react properly. Similarly, data leakage is usually caused by minor employee mistakes, such as addressing a message to a wrong entity. For this reason, it is crucial to educate staff about types and methods of

attacks and how to act against them. Trainings in this matter may be conducted by IT staff because their knowledge is the most comprehensive. However, lawyers are advised to provide for IT staff some external training, enabling them to have uptodate information. Finally, having written policies for employees would help them know their rights and duties, as well as who is supposed to and how to react in various situations.

**Conclusion**

As one of the most valuable assets, information is desirable by everyone. By taking the aforementioned steps, lawyers may accomplish a high level of data protection. However, they must be aware that these actions are just the beginning of establishing a comprehensive security program. Last but not least, it cannot be forgotten that anticipating crisis and preventing information leaks are always preferable to addressing such problems once they have occurred.

Pierwotnie tekst ukazał się: www.americanbar.org/publications/litigation-committees/commercial-business/practice/2017/preventing-information-leaks.html