JONES DAY

JUNE 2014

COMMENTARY

The Fight Against Cybercrime: A Major Issue for European Companies

The fight against cybercrime constitutes an economic and legal challenge for companies. The digital revolution and the development of new technologies have significantly increased the risks to which companies are now exposed. Furthermore, the amount of damages caused by cyberattacks has literally exploded over the last few years. It is estimated that the cost of cybercrime has reached €750 billion per year in Europe.

In addition, although companies are potential victims of cyberattacks, they remain no less responsible for protecting their own data. Only a comprehensive policy of "cybersecurity" can raise the awareness of companies and provide both a technical and a legal response to cybercrime. In this respect, a strong emphasis should be placed on data protection considerations.

The Development of Cybercrime

A Criminal Activity Experiencing Significant Growth. If cybercrime initially originated from isolated individuals or small groups, it is now also the result of criminal organizations, often with a strong international dimension. Cybercrime has become professionalized notably through the creation of highly structured networks specialized in drug trafficking, prostitution, money laundering, and industrial espionage.

Cybercrime is the fastest-growing type of criminality both nationally and internationally. The figures speak for themselves: In 2012, almost one in two French company claimed to have been the victim of cyberattacks in the past 12 months (compared with 29 percent in 2009).

By becoming professionals, cybercriminals have found a way to become profitable with almost no effort: for a minimal investment, the loss can be huge. For example, losses due to the "I Love You" virus in 2000 amounted to more than €4.7 billion with just a few clicks.

A Protean Concept Covering a Wide Variety of Offenses. Cybercrime takes various forms that companies need to understand in relation to their area of work.

Because no legal definition of "cybercrime" is clearly established, the Organization of the United Nations has adopted a particularly broad definition of cybercrime: "Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network."

Cyberattacks may include the following:

- Fraudulent access to or within all or part of an automated data processing system, obstruction of or interference with the functioning of the system, fraudulent introduction of data, fraudulent deletion or modification of data.
- Breaches of personal data, such as unlawful processing of personal data, collection of data without the knowledge of individuals or companies, identity theft.
- Damage to the company's reputation and dissemination of illegal contents, defamation and public abuse on the internet.
- Trademark and work infringement, software counterfeit (i.e., cybersquatting, which is the registration of, trafficking in, or use of a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else).
- Ordinary law offenses committed on the internet, such as theft, breach of trust, fraud.

Such criminality is diverse, complex, and very often international. Furthermore, cybercriminals are driven by different motivations (financial gain, technical challenge, defense of an ideology, industrial espionage, etc.). Worse still, 80 percent of cyberattacks are carried out by internal company employees.

A Wide Range of Risks for Companies. In the event of a cyberattack, companies are facing significant risks.

First, such an attack could have significant financial implications for a company. Thus, the interruption—even temporarily—of an IT department would inevitably result in a production slowdown and could lead to substantial operating losses for the company. In addition, the leak of trade secrets or loss of strategic intangible assets would likely be seriously detrimental to the company.

Cybercrime could also create a significant "reputational risk" for companies. In the event of an attack, their personal data as well as that of their business partners or customers could be stolen or disclosed. The impact could well be devastating not only for the company's reputation but also for its credibility.

Finally, companies must also be aware that they could be held criminally liable, especially if they were connected through their computer network to any kind of illegal actions such as spamming—sending emails indiscriminately to multiple mailing lists, individuals, or newsgroups. A company may also be held liable for not complying with regulations relating to the security of information systems.

Toward a Global Cybersecurity Strategy

With regard to cybercrime, cooperation at the national and international levels has grown steadily over the past decade. If the advent of the digital age has led to the implementation of national policies, the fight against cyber threats obviously requires coordinated international responses.

The Existence of Specialized Services at the National Level. Given the increasing number of cyberattacks, France has adopted a defense policy to protect its information systems. It has set up various bodies and services specifically dedicated to fighting cybercrime at all levels:

- The *Agence nationale de sécurité des systèmes d'information*, established in July 2009, implements guidelines related to the protection of national information systems. It is also in charge of the continuous surveillance of sensitive networks and provides reliable advice and support to private companies to help ensure the security of their information systems.
- The *Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication* is designated to deal with any offense related to the misuse of new information and communication technologies (hacking, identity theft, fraud, etc.) and to coordinate, at the national level, law enforcement operations.
- The *Brigade d'enquêtes sur les fraudes aux technologiques de l'information* primarily deals with intellectual property issues, especially when information systems are undermined (hacking, fraudulent access to a computer network, counterfeiting software, telephone-related frauds, etc.), and assists various investigative services on cybercrime cases.
- The *Service technique de recherches judiciaires et documentation* is responsible for centralizing and coordinating legal information forwarded to it by law enforcement

units, including the dissemination of illegal content on the internet. The "*Cyberdouane*" service introduced a monitoring system to detect and track offenses on the internet, including counterfeiting.

Although the institutional framework has been reinforced, it is also necessary to develop a judicial framework dedicated to punishing cyberattacks. In this regard, we are calling for the creation of a European prosecutor and a digital hub within the Ministry of Justice to ensure the effective implementation of a criminal policy against cybercrime.

Enhanced Cooperation at the European and International Levels. Cyberattacks cross borders and can be directed against several countries simultaneously.

Such transnational character requires the implementation of concerted actions to establish policies for European and international cooperation against cybercrime. It is within this framework that the European Parliament adopted the 2013/40 EU Directive on August 12, 2013 that will become domestic legislation by September 4, 2015. This new Directive aims to tackle the increasingly sophisticated and large-scale forms of attacks against information systems, to harmonize national legislations and enhance cooperation by implementing a coordinated monitoring of infringements.

The creation of the European Cybercrime Centre ("EC3") in January 2013, whose main goal is to protect European companies against illegal online activities and information system attacks, constitutes a recent high point of this cooperation. EC3 centralizes expertise and information and provides operational support in joint investigations conducted across the European Union. Upstream, the Centre prepares reports assessing the risks of cyber threats and, if needed, publishes early "alerts." EC3 also provides a Cybercrime help desk for EU countries' law enforcement units in case of cyberattacks.

Finally, a Cyber Crime Investigation Cell has been established within INTERPOL, promoting the exchange of information on potential cyberattacks, detecting new threats and providing Member States with the information collected. This group also assists Member States in their investigations relating to cyberattacks.

Conclusion

Cyberattacks now pose a substantial threat that business managers must understand and anticipate. Enhanced vigilance is necessary at all levels of the hierarchy within companies in order to ensure internal control and protect their own assets. To preserve the confidence of their investors and partners, companies must also improve their IT security policy as part of a comprehensive cybersecurity strategy.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Bénédicte Graulle
Paris
+33.1.56.59.46.75
bgraulle@jonesday.com

Emmanuel G. Baud
Paris
+33.1.56.59.39.18
ebaud@jonesday.com