COMPANY BOARDS OFTEN LACK THE KNOW-HOW TO FIGHT CYBERCRIME

Posted on 18/02/2016

Category: In-house news

Knowledge of cybercrime among company directors is improving, but many board members are 'technologically challenged' and don't act on information

Sophisticated global fraud has become a major threat but detecting cybercrime is difficult and many boards of directors lack the knowledge to properly guard against such risks, attendees at an Iberian Lawyer In-House Club event in Madrid heard.
According to session panellist Cristina Coto, a partner at CMS Albiñana & Suárez de Lezo, protecting a business against cybercrime "starts by protecting the company both from external threats and from internal fraud". She added that, while companies are implementing compliance structures to prevent and detect such crimes, whether an effective internal investigation is possible without the support of IT teams was questionable.

Bruce Goslin, executive managing director for EMEA at K2 Intelligence, highlighted one of the most frequent sources of cybercrime. "We often detect that an attack comes through a third-party vendor engaged by the company, and this is how the breach occurs," he said. "There are generally two types of companies, those that have been attacked and those that do not yet know they have been attacked." Goslin referred to the results of an international study by Ponemon Institute that revealed it takes an average of 256 days to discover a system data breach caused by a malicious attack. "Imagine you've had someone living in your house for nearly a year and you had no idea about it!" he concludes.
The event was attended by heads of compliance and legal of the major Spanish companies.
In terms of differentiating between sectors, financial institutions and global banks are, by and large,

ahead of everybody else in terms of tackling the threat, as they are vulnerable to losing a lot of money very quickly, and because they can dedicate large teams to such a task, the event heard. While some boards of directors are becoming more aware and understand the cybersecurity risk because they are being educated about it, attendees were told that it is a slow process partly because many board members, due to their advanced age, are “technologically challenged”. In addition, the information sent to boards is often too technical, while some boards do not use or act on the information provided to them.

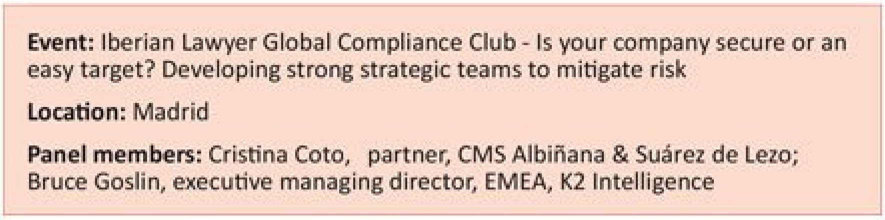
Intelligence is the best defence

When it comes to preventing and combating cybercrime, intelligence is the best defence, attendees were told. While it used to be the case that cybercrime was always committed with the complicity of an internal employee, that is no longer true. Consequently, there is a need for in-depth protection to safeguard data and critical assets because, as one participant commented, “a major cyber attack means that your company is ruined”.

Detection of cyber crime one of the biggest challenges companies face. “The problem with electronic assets is that people don’t even know they have been attacked,” one attendee remarked.

Meanwhile, the event also heard that companies are exposed to greater risk when entering into new markets – therefore, they need to incorporate protection against such risk into their budgets.

Regulations aimed at countering cybercrime vary across sectors. The payment card industry, for example, has very specific regulations that have evolved, but most regulations in many countries – particularly governing banking or healthcare – are too general and when regulations are insufficient, that is when the industry needs to come in and set the standard.



Event: Iberian Lawyer Global Compliance Club - Is your company secure or an easy target? Developing strong strategic teams to mitigate risk

Location: Madrid

Panel members: Cristina Coto, partner, CMS Albiñana & Suárez de Lezo; Bruce Goslin, executive managing director, EMEA, K2 Intelligence