Cyber insecurity

Thursday, 21 February 2013 • Hugo Coelho • Compliance and ethics

http://www.laccanet.com/features/article/338/lacca/cyber-insecurity/

The Latin American Corporate Counsel Association

Guy Fawkes mask *(Credit: Justin Ling / Wikicommons)*

General counsel are being called to the front line of the battle for cyber security and data protection. They must stay one step ahead of the game, as governments in the region enter a race to enact regulations after the US and the EU

The annual meeting of the world's financial elite at Davos is shrouded in secrecy, with the commercial world's powerbrokers discussing risks and opportunities behind closed doors. But even there, cyber

security is a taboo topic - no prominent business executive could be persuaded to take part in a panel discussion on the topic, and the word was spread during the meeting that to discuss the matter openly one would have to go outside, to the corridor. People seemed afraid of talking about cyber attacks on their businesses.

Silence has been companies' preferred reaction to cyber threats for a long time, but that strategy no longer works. Cyber security is a buzzword, with news about security breaches, data and financial losses and impending legislation overhaul hitting the headlines regularly.

"It is clear that cyber security has become a matter of grave concern," says **Lisa Sotto,** head of global privacy and data protection at the New York office of Hunton & Williams LLP. "Trade secrets and personal data are being sucked out of the companies' systems. It costs tens of billions of dollars and is an enormous embarrassment."

Cost and reputation: two words that start alarm bells ringing in corporate legal departments. A recent survey by the Association of Corporate Counsel listed "data breaches and protection" as one of the issues of major concern for chief legal officers. An annual survey by consulting firm Consero Group has shown that almost one in three general counsel think their companies are not prepared to defend against cyber attacks. Another 28 per cent admitted they have experienced a cyber security breach in the past year.

Carol Elizabeth Conway, director of regulatory affairs at UOL, the biggest internet service provider in Latin America, says awareness has been building up over time, but admits it is a risk which is becoming more prominent for companies. "Cyber security is not a recent concern at UOL, as we practically started commercial internet in Brazil. It has always been on top of our agenda, but we can see it growing as an important concern for regular business."

"Nowadays we see our credit cards, accounts and even money passing by cables in a virtual way. If in the past we had to create

strongboxes to keep it in safe, now it´s important to protect the data inside our cables, and this is what this growing concern about cyber security is about. It is important to keep in mind that crime follows people and money, and if they are migrating to the cyber world, then crime is going to do the same."

The value of data

This growing apprehension reflects the increasing value of information, says **Jacobo Cohen Imach**, vice president for government relations and general counsel at Mercado Libre, the biggest e-commerce website in Latin America.

"At the end of the day, it is all about data - users and consumers' data, trademarks and trade information. It is all about protecting data from third parties and your own. More than ever before, data is one of the most valuable assets companies have. I agree most companies are not ready to protect against this threat."

One of the reasons why businesses are so helplessly exposed to cyber threats is the rapidly changing technological landscape. The increasing use of mobile devices poses a particular threat, and in this Latin America is growing rapidly - economists from the Inter-American Development Bank forecast that mobile telephone access in Latin America and the Caribbean will reach the levels of member countries of the OECD in nine years.

Jody Westby, chief executive officer of Global Cyber Risk, which advises corporations and governments on such threats, points out the risks posed by a new working environment dominated by cloud computing, social-networking, web-based applications and a bring-your-own-device culture.

"If you have personnel carrying around laptops and accessing company data through public wireless networks… this is a significant concern. If you are an oil company, for instance, who operates in dangerous areas, the geo-positioning data from their mobile devices

can reveal their location. This is a different kind of threat, but no less real and is a result of connectivity."

This sense of vulnerability may be holding back some companies from moving forward with web-based businesses. "Our experience shows that cyber security is one of the main aspects companies take into consideration when establishing, operating and expanding corporate IT environments and web-based businesses," claims **Fábio Pereira**, head of IT Law at Veirano Advogados.

"The security of cloud services, for instance, is a top priority for companies interested in cloud computing services in Brazil. A number of companies have assessed the possibility of using cloud solutions, but only a few have implemented them so far. Thus, we believe that cyber threats and the lack of effective protection and uncertainty about the systems' security is hindering the implementation of cloud and internet-based services."

Closing the net

Not only are companies trying desperately to protect their data from more and more sophisticated cyber attacks, they must also keep up with legislation overhauls at a global level.

This month, within a week of each other, the US and the EU have unveiled their plans on cyber security. US president Barack Obama issued a long-awaited executive order and addressed the topic in his State of the Union Speech. The order focuses on information sharing between government and business and standard-setting for critical industries.

After that, the European Commission launched a cyber security strategy along with a draft directive to make sure businesses are not skimping funding for cyber security and do protect their data. Brussels calls for each member state to pass legislation and set up Computer Emergency Teams to deal with major incidents. It also makes it compulsory for private companies to disclose any major breaches of security.

New legislation still has to be fully implemented, but once that is done it will loom large over the rest of the world. “Many companies operate globally so they will have to address US and EU standards anyway,” says Hunton & Williams’s **Sotto**. “It would be foolish not to take a worldwide approach [to compliance policy]. If you are implementing standards in the US, it may be necessary, because of the systems’ integrated nature, to implement them overseas.”

Even businesses operating at a country or regional level should prepare for new and stricter rules, as Latin American governments are expected to follow the lead from developed economies. **Cédric Laurant**, a global data privacy attorney and public policy expert based in Mexico, believes that Latin America will be the next big region after Asia to see a major overhaul in its data protection regulatory landscape. “The two very different models [US and EU] are being pushed on Latin American governments. In the next three to five years, most countries will have a specific law on data protection and they will come up with regulations, gradually.”

Laurant predicts data protection laws and regulation will be enacted in an effort to promote business and trade and attract investment – not so much for protecting individual rights. “The highest motivation for Latin American governments to push for data protection laws is to foster commerce with other countries and attract foreign investment in call centres or the outsourced IT industry, to name a few.”

The time lag in imposing local regulations could actually make doing business riskier for local companies. Global Cyber Risk’s **Westby** thinks most Latin American countries will follow the European model, which is more regulatory than the rules from the US. “I think they will take a close look at it, but they lag behind in connectivity, so they will be somewhat slower to reach the same level of sophistication in their security programmes.”

“People – hackers and insiders – will realise this and take advantage. So, in a sense, Latin American [companies] need to be more

conscious of security and have better programmes to prevent criminals from taking advantage of them."

In the meantime, in-house lawyers in Latin America have to navigate through a maze of rules and requirements. **Laurant** says that most big countries in South America have already enacted some form of data protection legislation, but haven't implemented them through regulations yet. Another common feature is poor enforcement mechanisms.

"Argentina and Uruguay offer 'adequate protection', demonstrating that they have been considered as having a legal framework offering protections at least close enough to the EU data protection framework. Colombia has started to demonstrate strong enforcement through its new data protection authority, while Mexico is a bit slow to enforce the law in the same way," he adds.

Brazil, by far the largest online market in Latin America, with more than 40 million online consumers and 80 million internet users, is stuck in a legislative limbo. Cyber security and the relevant laws became a hot topic in the country when government websites were attacked and hackers published private pictures of a famous Brazilian actress, years ago. But no specific law on data protection has been approved yet.

Evy Cynthia Marques, partner at Santos Neto & Montgomery Advogados, explains that there are data protection provisions in Brazil's Constitution and in its comprehensive consumer laws. Last year, Congress approved some amendments to the criminal code, imposing penalties for cyber crimes of up to two years in jail. However, an EU-inspired and comprehensive bill addressing data protection and cyber security – Marco Civil da Internet – stalled.

Nonetheless, courts have been penalising companies that fail to prevent consumer data leaks. Veirano's **Pereira** points out to one ruling against Mercado Livre – Mercado Libre's Brazilian subsidiary – in 2008. The company had to pay compensation to one user that

posted a mobile phone to a hacker, who broke into the company's system and sent him a sham message confirming payment.

Prevention is better than cure

Within a confusing regulatory picture, being one step ahead of the game seems to be businesses' best strategy, as consumers increasingly choose where to spend based on their trust in companies' ability to protect their data. "We are reviewing our policies to make sure everything is in line with Marco Civil," says UOL's **Conway**. "But people should note that what Marco Civil and also the recent cyber-crime law do, is turn current practices of users and online providers into law, in a kind of statement of principles about the internet."

Mercado Libre's **Cohen** designs the compliance strategy based on the highest global standards. "As a listed company, Mercado Libre has to comply with strong security requirements and have an internal audit. We have a one-size-all-fits-all approach to our cyber security policy, so we set the bar by the strictest requirements and go beyond local regulation."

Complying with laws and regulation is just the first part of the job, though. General counsel must ensure everyone in the company is engaged and is sticking to internal rules. "It has to be a coordinated effort between different company departments: the legal department leads, but we also work with people from IT and human resources," says **Cohen**.

"[Legal] know about the requirements and penalties and can develop compliance policies. The IT team must implement these measures – building up the firewall and setting permissions to access information. There are two kinds of threats, internal and external. When it is internal it is for the human resources people to make sure employees comply with the rules."

Conway talks about the importance of keeping staff updated and providing training about cyber attacks and ways to avoid

confidentiality breaches. “People are the most important item when you try to guarantee your information protection, as they are vulnerable to one of the most dangerous cyber-attacks, social engineering, which consists of manipulating people in order to get confidential information. This is all part of our compliance programme.”

Third-parties pose another challenge to corporate lawyers, especially if they are law firms. “There is a lot of whispering about breaches at law firms, which scares them to death,” says Global Cyber Risk’s **Westby**. “Law firms are managing lawsuits of great importance to their clients. If someone hacks into their system and steals sensitive data on a case, it could cost them the case, the client, and their reputation.”

Conway admits it is more difficult to protect information when you are sharing it. “But if this sharing is part of your job or a project, then you should face it,” she adds.

“The first thing to do is to determine which information can be shared and which information cannot by classifying documents. After that, companies must establish confidential agreements before starting to share any kind of information or document in order to guarantee that third parties are going to keep these information with the same care they provide.”

Most importantly, policies and structures must be constantly reviewed, as companies fight to keep pace with the cyber criminals as they develop new ways to attack data and infiltrate systems. Legislation is important, but will always be several steps behind the trends of consumers and most importantly hackers. General counsel are at the front line of defending their companies against these attacks.