LACCA

(http://laccanet.com/features/article/682/lacca/your-weapons-cyber-war/)

Your weapons in the cyber war

24 March 2014

Alison O'Connell

As governments and the private sector across the globe look for ways to deal with the rising threat of cybersecurity, Latin American general counsel are being placed on the front line to protect their organisations

As any general counsel worth their salt knows, risk and opportunity are intimately intertwined. So while organisations are happily and fully exploiting the business benefits of society's move online and increased connectivity, so too are they faced with increasingly significant risks by those who exploit such benefits to attack organisations.

"Information is the life blood of any organisation – it's a cliché, but true. And increasingly we are sharing that information via our own systems, knowingly, and via third parties or mobile systems, or perhaps unknowingly," says Steve Durbin, vice president of the Information Security Forum, an information and risk management think tank.

And the numbers associated with that risk are growing. The Ponemon Institute, which conducts research into data protection and information security policy, estimates that the average annualised cost of cybercrime incurred by organisations in 2013 was US$11.56 million, ranging from anywhere between US$1.3 million and US$5.8 million. This marks a 26 per cent increase from 2012, where annualised average costs were around US$8.9 million. On top of this, it is estimated that most multinational organisations experience an average of 122 successful attacks per week, up from 102 attacks per week in 2012.

With such breaches posing a significant, and potentially devastating, impact on a company's reputation and financial position, it is no surprise that businesses globally are waking up to the risks. In fact, the same report by The Ponemon Institute stated that 41 per cent of large organisations said they now consider cyber risk to be more important than other insurable business risks. In addition, nearly a third of those surveyed in Consero Group's General Counsel Survey in 2013, acknowledged having experienced a corporate cyber breach in the previous year.

“In short, if you operate in cyberspace then you are at risk. If you handle sensitive data, then you are at risk. If you share your data with third parties, then you are at risk. The management of risk has become a key component in operating effectively in cyberspace and we have seen a move away from information security to cyber security,” says Durbin.

As a result, measures against cyber-attacks are becoming an increasingly critical part of overall risk management and with everything from corporate reputation to long-term financial viability on the line, it is becoming more and more evident that general counsel should play a significant role in protecting their company’s if they are first—rather than last—on the cybercrime scene.

“Legal counsel can play a vital role in helping the business understand and manage the complex landscape of legal and reputational risks relating to cybersecurity. The role of counsel is to help the business develop a strategy for reducing these risks and for having an effective response in the event of a cyber-related incident,” says Harriet Pearson, partner in Hogan Lovells' global privacy, information management and data security practice group in Washington DC.

Some ‘phishy’ goings-on

Until relatively recently, many of the risks associated with cyber breaches have not been seen as a big local problem, with Latin American GCs being much less worried about the protections they should be putting in place than those in the US or Europe. However, that is changing, as the region originates more and more of the kind of critical threats to sensitive company, customer and employee data which keep GCs up at night.

According to a report by security company Norton released last year, the cost of cybercrimes stood at US$8 billion for Brazil, home to the largest internet user population in Latin America. In addition, the country is listed among the top 10 countries globally for cybercrime attackers and victims by a Trustnet study conducted in 2013. The cost of attacks was also significant in Mexico, reaching US$3 billion in 2012, while in Colombia the figure stood at around US$464 million, with costs continuing to rise across many other parts of the region.

“Latin America is a new, emerging threat region - if you’re in government, finance, or energy and doing business in Latin America, be prepared to be the target of sophisticated attacks that have seen a dramatic evolution in capability,” says Tom Kellermann, managing director for cybersecurity at global professional services consultancy Alvarez & Marsal in Washington, DC.

The use of malware, the type of software used to infect computer systems, has risen steadily over the past few years, with such programmes being developed in countries such as Brazil, Mexico, and Guatemala. In fact, last year Peru was the source of the region's first ever corporate espionage virus, and others such forms of attacks are posing an increasing threat to businesses throughout the region.

Attacks involving phishing, a technique used to acquire information such as usernames, passwords, and credit card details from users, are also increasing at a higher average rate in Latin America than elsewhere in the world, according to Argentine cybersecurity researchers, and it is estimated that bank users in the region lose around US$26 million each year due to phishing.

Companies are without doubt on the frontline when it comes to battling these threats. While Latin American governments have certainly begun to recognise the risk posed by cybercrime, with various new agencies created to monitor and combat online criminals, they continue to struggle to keep pace with the rapidly-changing landscape and often impose backwards-looking legal frameworks.

"While well-intentioned, the challenge is that given the rapid evolution of technologies and the complex nature of the actions needed, legislation is a blunt instrument that nearly always produces unintended outcomes," says Hogan Lovell's Pearson.

Indeed, even the private sector struggles with a general lack of awareness or clarity. "Unfortunately, a great many organisations do not fully understand cybersecurity risks, or how best to address them. This is true even of some large, multinational organisations that are otherwise quite sophisticated," says Jason Gonzalez, partner at Nixon Peabody in the US.

It is no surprise therefore, that 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. And the outlook does not seem set to change anytime soon. "The future is dark," says Alvarez & Marsal's Kellerman. "Corporations cannot rely on law enforcement to save them from cybercriminals. They must begin to build their own gated communities in cyberspace." So just what should Latin American companies and their GCs be doing to ensure they are protected?

Ignorance is risk

Today, companies are faced with the dual challenge of understanding current trends in security threats as well as identifying inherent vulnerabilities within their industry and

existing internal systems.

The US Department of Commerce's National Institute of Standards and Technology (NIST), in order to help businesses fortify themselves from cyber attacks, recently released guidelines on what it believes businesses can do to improve their cybersecurity practices.

According to NIST, companies should begin by prioritising their business objectives and identifying the types of digital threats they face. Companies should then perform a risk assessment and define their cybersecurity objectives. Finally, businesses should determine the gaps that exist between their current cybersecurity profiles and the profiles they want, allowing them to develop their own action plan to identify, protect against, detect, respond to and recover from a cyber attack.

“Businesses put the cart before the horse when they begin securing their information assets without first taking the time to understand the vulnerabilities in their systems and the threats facing them,” says Pearson. Regular risk assessments as well as advance planning are therefore not only essential steps to making thoughtful security decisions, but they are important for compliance purposes, as a risk analysis is often requested by regulators when there is an investigation or audit.

There are no shortcuts - as technology continues to develop and change, so too have attacks grown in sophistication and complexity, rendering the majority of ‘off the shelf’ solutions, such as commercial antivirus programmes, ineffective.

However, just like in more familiar areas of anti-corruption compliance, clear internal policies and training is a powerful tool. Employees are increasingly using mobile devices, which creates a host of security risks. Not only do such devices provide additional access points into a company’s network, they also give rise to complex issues regarding data ownership and privacy between the company and the employee. On top of this, their use can cause the employer to lose some degree of control over the security environment, leading to increased opportunities for hackers to gain entry into the network.

“Protecting a company’s systems implies not only having the most advanced technology for this purpose but also developing clear internal policies for the use of the internet and access to information,” explains Alejandro Anderlic, legal and corporate affairs lead for Microsoft in Argentina and Uruguay.

Alongside keeping pace with shifting technology, training for employees focused prevention can provide a strong foundation on which to build am overall safer business

environment. A company can have the best security system in the world but still be vulnerable if its employees are not trained to prioritise security, to recognise and avoid malware or phishing scams, and to keep track of their mobile devices.

“Companies must pay careful attention to employee training and monitoring, consider appropriate network segmentation and credentialing; and do their best to implement security solutions that are nimble and seamless so that employees will actually use them,” says Gonzalez.

Collaboration is also key. By working together, legal, compliance and IT departments are more able to create a wholesome framework for protection, but can also ensure a prompt and strategic response in the case of a breach.

“Our legal team works closely with the IT department to deploy good security information policies for internal use,” says Andelic. “Microsoft has recently created its Digital Crimes Unit, which is composed of a team of international legal and technical experts who apply cutting-edge tools, technologies and strategies to enhance security, including cloud, and make the internet safer for everyone.”

Again, just like in corruption compliance, looking beyond the company's immediate borders is increasingly important. As companies have become better at identifying and mitigating risk, many cybercriminals have moved elsewhere to obtain the information they want.

“All sectors are at risk, but lately increasing attention has been paid to the risks facing consultants, law firms, and other entities that advise the major industries,” says Gonzalez. "These advisors often have extremely sensitive and confidential information about corporate transactions, research and development, and investigations.” Such organisations have a reputation for being less attentive to cyber-security and hackers have started to realise that it may be an easier route to gaining the same valuable information.

“Enterprising thieves have now found ways to penetrate supply chains and enter otherwise well secured organisations and the increasing use of cloud computing and other forms of outsourced services present further risk management challenges,” agrees Kellerman. As a result, companies are increasingly focusing on third-party compliance to mitigate risk and ensure protection from all angles, particularly for companies with a widespread network of business partners both nationally and internationally.

A particular challenge for Latin American GCs is a cultural one. In the US, the trend both in business and regulation has been for openness and transparency about the risks

companies face. The SEC issued guidelines in 2011which stated that publicly-traded companies must not only disclose instances of breaches or attack, but they must report even when they are at material risk of such an event.

The rules have compelled legal departments to work closely with IT departments to ensure they are aware of cybersecurity issues at every stage - as poor communication between departments can leave a company at risk of violating SEC guidelines. That means that companies have been forced to make budget and resources available, and face up to their obligations in the field.

"Unfortunately, in many Latin American countries, the trend is still for a company to hide a breach affecting their clients and customers' personal data instead of establishing a relationship of trust with them by explaining to them what they are doing to diminish the impact of a breach and notifying them, once a breach has occurred, of the ways to mitigate its impact," says Cédric Laurant, data privacy lawyer and public policy expert, based in Mexico City.

Which means of course, that general counsel have to work harder to get companies to be realistic about the risks and to invest in measures to counter them. In all, that can mean that for companies in Latin America, the risks posed by cybersecurity are sometimes taken into account too late, and companies and their legal teams need to do more to make sure they invest in prevention to ensure a future of cyberpeace.

General counsel can also work together to find the right solutions. Continued legislative and regulatory focus on these topics worldwide is inevitable; however, the implementation of effective legislative measures will also need direct collaboration from industry leaders.

"I always advise industry leaders concerned about these issues to engage with government officials so they can inform and help shape the standards and laws that will continue to emerge in this area. If a company has international interests, it is even more important to do so, given the challenge of complying with inconsistent and potentially conflicting requirements," explains Pearson.

Now is the time to be proactive, as Laurant points out. "Data breaches will inevitably occur one day or another. Companies can no longer bury their head in the sand waiting for the storm to go by, but should proactively work to establish incident response and risk mitigation strategies."