Spring 2020

ihl

The In-House Lawyer

BRAND AND REPUTATION MANAGEMENT • CYBERSECURITY • INSURANCE • COVID-19 RESPONSE

Eye of the storm

Insurance GCs brace for impact amid global crisis

Cyber insurance and the silent revolution in Brazil

Pedro Guilherme G De Souza, partner, Rodolfo Mazzini, senior associate, SABZ Advogados

Pedro Guilherme G De Souza
partner, SABZ Advogados
pedro@sabz.com.br

Rodolfo Mazzini
senior associate, SABZ Advogados
rmazzini@sabz.com.br

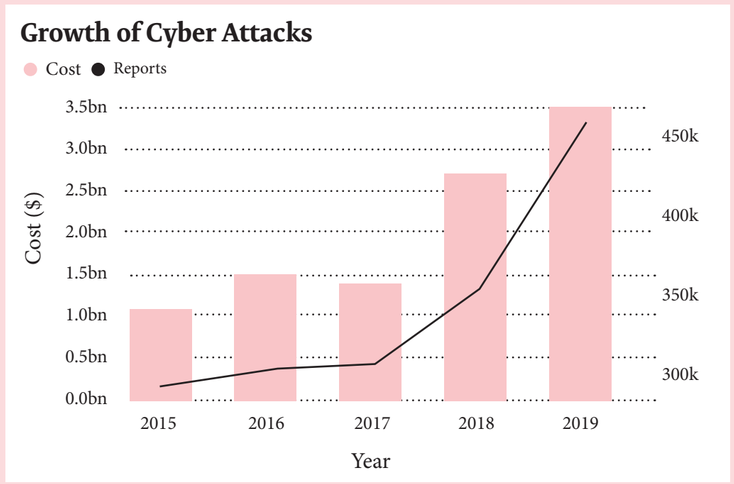
Cyber risks – intensified by the expansion of home working due to the Covid-19 pandemic countermeasures – are one of the most serious worldwide threats nowadays. That doesn't mean the risks themselves are new, but the sophistication and range of modern cyber attacks foretell a dire future. According to Cybersecurity Ventures, the cost of cyber crime is expected to reach a whopping $6trn per year by 2021.

The graph below illustrates the scale of cases and associated costs of cyber attacks reported to the Federal Bureau of Investigation over the last five years.

Despite this scenario, current efforts in Brazil to face these risks are still far from what they should be: recent studies show local companies' lack of preparation in tackling the problem, even though the country is the third largest target for cyber crimes in the world. (It may come as a surprise that human error and inappropriate behaviour are a significant catalyst to cyber attacks. Actions or omissions by employees, such as creating a weak password or inadvertently sharing confidential data, may result in security breaches and/or claims against the company).

Considering Brazil's potential for technological development and the affinity of its population with the internet, the revelation is nothing short of baffling.

The time has come for Brazil to abandon its outdated view – or lack thereof – on cyber risks and move towards cutting-edge cyber security and risk management tools, in order to completely integrate to the contemporary world dynamics.



> **Having noticed the rising stakes related to cyber risks and the worldwide concern about the matter, Brazilian legislators did not remain idle.**

Legislators take action: the LGPD

Having noticed the rising stakes related to cyber risks and the worldwide concern about the matter, Brazilian legislators did not remain idle and, following eight years of studies and debates, passed Federal Act number 13.709/2018 (LGPD), which regulates personal data protection nationwide, and will come into full effect by August 2020.

Drawing inspiration from the European Union's widely acclaimed General Data Protection Regulation (GDPR), LGPD deals with personal data – one of the key stakes protected by cyber security. The new regulation establishes several guidelines, such as: (i) admissible data treatment, sharing and elimination; (ii) rights of data subjects; and (iii) most important to our theme, security parameters. These guidelines are enforced by sanctions ranging from a simple warning to fines of up to BRL50,000,000.

The growth of cybercrime, associated with the rising obligations of LGPD, has jump-started Brazilian companies' cyber security programmes. However, even the most advanced technologies are unable to completely shield companies. Thus, cyber insurance has a prominent role as a tool to fill protection gaps.

The promised panacea: cyber insurance

There is no denying the relevance of cyber insurance: as a gear in a complex risk management mechanism, it provides relief for mild to catastrophic cyber-related events, such as major data breaches or severe network and hardware damages. Yet, is it being 'oversold' by the insurance market? In our opinion, yes. Here are two key reasons why.

The first is related to what cyber insurance is: an insurance product, inherently subjected to the dichotomy of coverages versus exclusions. When it comes to cyber insurance, the insurer is faced with many uncertainties and limits the risk taken through a vast arsenal of exclusions. Even some traditional ones – such as war and terrorism, intellectual property and capital markets exclusions – carry a far heavier weight in cyber insurance (see the argument around the 'act of war' exclusion in *Mondelez Inter, Inc v Zurich American Ins Co* [2018]).

The second is related to what cyber insurance could be: a means to foster synergy between insurer and insured and the development of the cyber security framework. Instead of policies firmly structured upon traditional liability insurance models, insurers should offer policies that support the insured through 'routine coverages'.

It demands a shift from a static to a dynamic view of cyber security. Instead of guarding against the consequences of cyber risks, it is more reliable to address its causes – much like health insurance markets. Unlike a hurricane or earthquake, cyber risks are omnipresent; they constantly threaten companies, chipping away at their defences or lying in wait for some vulnerability. In that case, why not assist the insured in keeping a strong, healthy body?

Given the insurers have 'skin in the game', (cyber risks policies), they could support their clients through value-adding services focused in understanding and preparing for cyber risks, providing security consultants, network and hardware technicians, anti-data leak experts etc. Insurers are not oblivious to the possibility. As an example, AXA and Accenture recently partnered to offer cyber security services to their insureds. Insurance policies could incentivise such demands through pricing and reward mechanisms.

Particularly in Brazil, whose GDP is strongly reliant on small and mid-sized companies, a product that offers immediate usefulness in the form of 'routine coverages' is more prone to attract attention, as it assists in complying with the LGPD and avoids the usual distrust Brazilians have in insurance.

Lessons learned

Cyber risks are a bigger threat now than ever before (mainly after an increase of home working due to Covid-19) and will only grow with each passing day. There is an ever increasing 'cyber gap' and our defences are always one step behind the criminals. Those are further grounds to strive for the best possible cyber security and risk management.

A model of cyber insurance structured by two layers – the bottom with routine, value-adding services, and the top with seldom-used liability (and crisis) covers – would help foster a trusting and symbiotic relationship between insurer and insured, while also revealing the constant – but often unnoticed – usefulness of insurance. ■

Mondelez Inter, Inc v Zurich American Ins Co [2018] L 11008


ihl