INDEPTHFEATURE

CYBER SECURITY & RISK MANAGEMENT

2021

FINANCIER WORLDWIDE corporatefinanceintelligence

Published by
Financier Worldwide Ltd
First Floor, Building 3
Wall Island, Birmingham Road
Lichfield WS14 0QP
United Kingdom

Telephone: +44 (0)121 600 5910
Email: info@financierworldwide.com

www.financierworldwide.com

FINANCIER WORLDWIDE corporatefinanceintelligence

INDEPTHFEATURE

CYBER SECURITY & RISK MANAGEMENT

April 2021

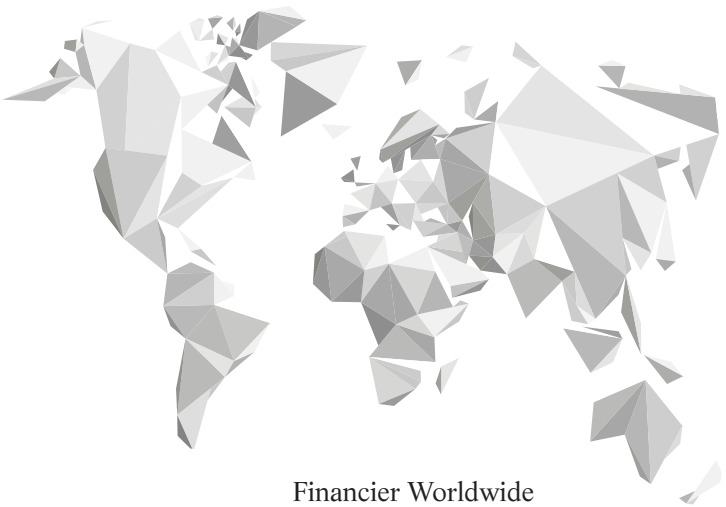
Introduction

While the profile of cyber security has certainly increased in recent years, the events of the last 18 months have reinforced the importance of properly staffed and sufficiently funded cyber security programmes. The COVID-19 pandemic has greatly increased the attack surface for malicious actors, both internal and external, and companies must be prepared to evolve as quickly as cyber criminals.

The means of cyber crime and data exploitation remain largely unchanged – malware and phishing attempts, for example, are not new. But cyber criminals are becoming increasingly sophisticated and bold, and companies that do not up their game not only risk a breach, but also run the risk of falling foul of regulators. The European Union's (EU's) General Data Protection Regulation (GDPR) was a game changer, and many other jurisdictions are following suit. In the US, the California Privacy Rights Act, when it is fully enforced in 2022, will be a watershed moment – and a number of other states are considering privacy-related legislation.

Going forward, companies cannot bury their heads in the sand when it comes to cyber security and data breaches. While none are safe from attack, organisations must take all possible steps to protect themselves and their stakeholders. A comprehensive cyber security framework, an incident response plan and cyber insurance should be key items on the agenda, regardless of a company's size or industry.

CONTENTS



Financier Worldwide canvasses the opinions of leading professionals on current trends in cyber security & risk management.

PORTUGAL

Morais Leitão, Galvão Teles, Soares da Silva & Associados

Respondent

DAVID SILVA RAMALHO
Senior Associate
Morais Leitão, Galvão Teles, Soares da Silva & Associados
+351 210 091 720

David Silva Ramalho joined Morais Leitão in 2016. He is a member of the firm's litigation and arbitration team. His practice, initiated in 2013, is focused on the areas of criminal and misdemeanour litigation and compliance, particularly in the economic and financial areas, as well as in information technology and data protection. In criminal litigation, he has significant experience in cyber crime and digital evidence, representing clients and providing legal assistance in those areas.

Morais Leitão, Galvão Teles, Soares da Silva & Associados

Q. In your opinion, what are the major cyber threats to which today's companies are vulnerable?

A. The major cyber threat to most companies today lies in email – more specifically, in employees' use of company email accounts. This is the gateway for most cyber attacks, ranging from unsophisticated 'Nigerian prince' scams, to the most sophisticated malware, phishing, chief executive fraud and ransomware attacks. The reason is simple: IT departments can more easily prevent risky employee behaviour than react to an outside attacker actively searching for human failure. The former is more or less preventable by blocking access to certain websites, monitoring threats arising from unadvised web usage or imposing restrictions on the download of certain files. The latter faces serious technical difficulties in preventing certain emails from entering a company's mailboxes, and the challenge of training employees to assess its malicious origins and avoid opening suspicious emails.

Q. Given the risks, do you believe companies in Portugal are placing enough importance on cyber security? Are board members taking a proactive, hands-on approach to improving policies and processes?

A. Portuguese companies, particularly small and medium sized enterprises and those not in IT-related sectors, still have a long way to go when it comes to cyber security. This is mostly because a serious investment in cyber security – both from a legal and technical point of view – is often regarded as an unnecessary expense compared to the perceived probability of facing an attack. It has been this way for quite some time. Just when it was getting better, coronavirus (COVID-19) made things worse. Due to the pandemic, companies have been forced to cut back on expenses that are not immediately essential to keeping them afloat, which too often has included any investment in cyber security measures. Incidentally, the pandemic has also amplified the necessity for cyber investment, mostly due to employees working from home and accessing their company's servers remotely, frequently on personal and insecure devices.

Morais Leitão, Galvão Teles, Soares da Silva & Associados

Insurance is gaining traction as a viable mitigation tool, with a market better prepared to meet the increase in demand for products that include cyber risk coverage.

Q. How does the judicial system usually handle cyber crime cases in Portugal?

A. There are two main problems with cyber crime cases and they usually arise in different stages of the criminal procedure. The first is insufficient resources in the investigation phase. Though we have highly skilled police officers and public prosecutors in charge of several of these investigations, it is clearly not enough considering that technical analysis of a given device takes two to three years and that sometimes when evidence is requested and collected, all the relevant deadlines for collecting further information, such as traffic data, have passed. The second problem is a general lack of IT knowledge in the judicial phase. Courts must deal with all types of complex criminal cases, often requiring knowledge of subjects not of a legal nature, which of course include cases of cyber crime. However, though the law allows it even for highly sophisticated cyber crime it is still rare to see courts request technical assistance from IT professionals to interpret digital evidence and understand what information they

should seek to confirm in the prosecution or the defence's narrative.

Q. In your experience, what steps should companies take to avoid potential cyber breaches – either from external sources such as hackers or internal sources such as rogue employees?

A. The solution lies in a balance between the legal and technical sides of cyber security. While the legal side should focus on compliance with labour and data protection legislation, establishing transparent and fair internal procedures that allow for a legally admissible level of monitoring, the cyber security side should focus on implementing technical measures that mitigate cyber risk and trace evidence of possible attacks. It is always important to protect the company against external cyber breaches with measures including intrusion detection, email filtering and independent vulnerability assessments. But companies should not forget that many cyber breaches originate from within the organisation.

Q. How should firms respond immediately after falling victim to cyber crime, to demonstrate that they have done the right thing in the event of a cyber breach or data loss?

A. The first step is to make sure that the crime is no longer taking place. Then the company should assess the level of damage the attack has caused and whether any sensitive personal data has been compromised. The first assessment should be made by independent legal and technical specialists, working closely with the company's IT department. It is the purpose of this analysis to identify how the attack has happened, to collect evidence in a forensically sound manner and to consider any legal action. The response will vary depending on the outcome of the legal and technical analysis. Possible outcomes may include a legal obligation to notify a particular authority of the data breach, or a strategy for presenting a formal criminal complaint with evidence.

Q. In what ways can risk transfer and insurance help companies and their D&Os to deal with cyber risk, potential losses and related liabilities?

Morais Leitão, Galvão Teles, Soares da Silva & Associados

A. Awareness among companies of the importance of taking different actions to mitigate cyber risk is becoming increasingly widespread, mainly due to the spike in cyber threats and data protection laws. Despite being relatively recent and with limited supply, insurance is gaining traction as a viable mitigation tool, with a market better prepared to meet the increase in demand for products that include cyber risk coverage. As the market currently stands, such protection may be found in traditional commercial insurance, by taking out a standalone insurance policy, or via endorsement policy already in place. The latter are usually the safest options as traditional commercial policies often exclude cyber risks or include wording that casts doubt on such protection. Cyber risk protection may include first-party coverage, such as cover of direct losses from a breach or business interruption, third-party claims, such as liability arising out of data breach claims or harm to third-party systems, or defence costs and regulator fines.

Q. What are your predictions for cyber crime and data security in Portugal over the coming years?

A. If we have learned anything from cyber crime predictions it is that they are usually wrong. Taking this into consideration, if I were to risk any predictions, I would have to say that the more serious offences will continue to be ransomware, hacking through vulnerability exploitation, phishing and chief executive fraud, with intent to steal money, information or intellectual property. The more serious changes will not be felt on the criminal side, but instead on the investigative side, due to the increase in data security. The advent of secure communication apps, increased access to the dark web and to online illegal markets, and new ways to launder proceeds from crimes, particularly with digital currencies and the increasing use of the Lightning Network, will seriously hamper investigations. What worries me the most is how far lawmakers will go to address these challenges. ❑

Morais Leitão, Galvão Teles, Soares da Silva & Associados

www.mlgts.pt

MORAIS LEITÃO, GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS is a leading, full-service law firm in Portugal, with a solid background of decades of experience. Widely recognised, the firm is a reference in several branches and sectors of the law on a national and international level. The firm's reputation among both its peers and clients stems from the excellence of legal services provided, characterised by unique technical expertise, combined with a distinctive approach and cutting-edge solutions that often challenge some of the most conventional practices.

DAVID SILVA RAMALHO Senior Associate
+351 210 091 720

INDEPTHFEATURE

CYBER SECURITY & RISK MANAGEMENT

2021

FINANCIER WORLDWIDE corporatefinanceintelligence