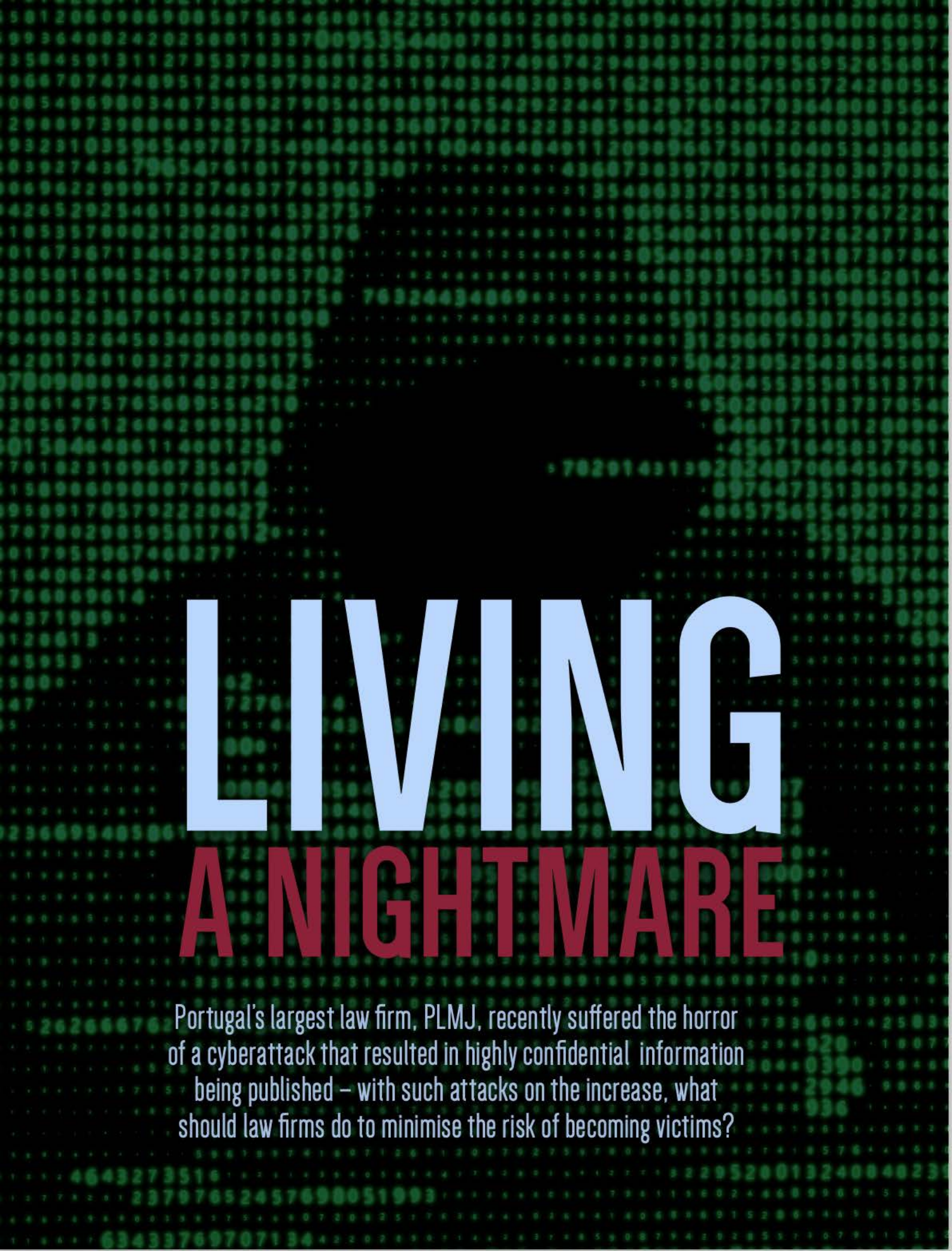

LIVING A NIGHTMARE

Portugal's largest law firm, PLMJ, recently suffered the horror of a cyberattack that resulted in highly confidential information being published – with such attacks on the increase, what should law firms do to minimise the risk of becoming victims?

It must be a nightmare scenario for any law firm. Hackers break into your firms' computers, access confidential information about your clients and the correspondence you have had with them and then publish it. But for leading Lisbon law firm PLMJ, this nightmare became reality. In January, the firm's systems were hacked and information was published on the "Mercado de Benfica" blog. Prior to the newspapers getting hold of the story, PLMJ went through the drama and anxiety of trying to obtain an injunction, but the efforts failed. The secrets were out. The stress for those involved must have been unimaginable. What clients want when they appointed a lawyer is a trusted adviser, but in this case that trust had been broken, though it is hard not to feel sorry for PLMJ, which was the victim of a crime perpetrated by some very sophisticated hackers.

Perhaps unsurprisingly, PLMJ was unwilling to provide any official comment when asked for an update on the fallout from the attack. Lawyers at the firm will want people to stop talking about it in the hope that the story, and the negative publicity that surrounds it, will go away. Meanwhile, partners at rival law firms are breathing a huge sigh of relief that it wasn't their organisation that had its name tarnished by such a worrying security breach.

WARNING CLIENTS

Despite the absence of official comment from PLMJ, sources close to the firm say that the management took a series of steps when they realised their systems had been compromised. "The firm found out just before the press did, all the IT guys were called and a specialist US cybersecurity specialist was instructed to analyse everything," says one source. There is speculation that an employee from a specialist IT company that provides services to the firm may have allowed, deliberately or unwittingly, a password to fall into the hands of a hacker, though this is unconfirmed and police are investigating. "It's a very sensitive issue," says another source. "Clients were warned, the firm took the lead on that and contacted all the clients, it was taken very seriously. However, there are issues, and the firm does not want to talk openly about the matter."

It's no real surprise that it was a Portuguese law firm that was the victim in this case. Data shows that, when comparing EU

countries, Portugal is the third biggest victim of cyberattacks (see table). In light of the horror experienced by PLMJ, firms are being warned that they have to face up to this new threat and act now. "Law firms of all sizes should be worried," says *SRS* Advogados partner **Luis Neto Galvão**, who specialises in advising companies on data protection. "Even small law firms can be vulnerable to cyberattacks – acquiring a cybersecurity culture takes time and resources," he says. "Therefore, law firms should start immediately addressing the matter."

In one of the most famous law firm cyberattacks, the "Panama Papers" scandal in 2015, 11.5 million documents – containing detailed financial and attorney-client information – were leaked from a Panamanian law firm in an event that shook the legal world. **Martim Bouza Serrano**, a partner at CCA Ontier, says such attacks represent an unsettling window into the future when hackers will become much more sophisticated and be able to carry out attacks on a larger scale. "We have been seeing an increasingly number of cyberattacks and I am certain that during 2019 we will see bigger and more damaging threats than in previous years," he says.

LUIS NETO GALVÃO

"LAW FIRMS OF ALL SIZES SHOULD BE WORRIED"

SRS Advogados partner Luis Neto Galvão

BIGGEST CYBERCRIME VICTIMS IN THE EU

		Percentage of population who have experienced cybercrime	Annual average malware encounter rate	Cybercrime Victimhood Rating
1	Romania	18%	28%	23%
2	Netherlands	27%	14%	21%
3	Portugal	15%	24%	20%
4	Poland	16%	23%	20%
5	Italy	17%	21%	19%

Source: www.websitebuilderexpert.com (based on data from European Union, ITU Global Cybersecurity Index, Microsoft and Rapid7)


MARTIM BOUZA SERRANO

"I AM CERTAIN THAT DURING 2019 WE WILL SEE BIGGER AND MORE DAMAGING THREATS THAN IN PREVIOUS YEARS"

CCA Ontier partner Martim Bouza Serrano

ENORMOUS DAMAGE

Given that they handle large volumes of confidential information, law firms are an obvious target for hackers, and once an attack has happened, the results can be devastating. "There is one feature that everyone expects from a priest, a doctor or a lawyer and that is confidentiality," says Bouza Serrano. He adds: "The damage caused by a cyberattack to a law firm is enormous and it may cause irreversible consequences to the trust between firms and their clients."

It is unclear how often cyberattacks really happen, because businesses often handle them discreetly. Culprits are hard to trace and motives often unclear. It may be criminal organisations with a focus on extortion, or whistle-blowers, according to **Cláudia Martins**, a senior associate at Macedo Vitorino. Meanwhile, on rarer occasions, hurting the firm, or its clients, could even be the primary goal, according to Galvão.

Whatever the reasons behind a cyberattack, there are various steps firms can, and should, take to minimise the risk. Martins recommends evaluating systems for weak points before preparing formal cybersecurity policies, incident response plans, backup and restoration procedures. She also advocates the use of two-factor authentication, and encryption. Meanwhile, Galvão says formal cybersecurity policies are essential, while also stressing the importance of training and specialist outside support. However, he acknowledges that there is no "definitive formula" for effective cybersecurity.

HUMAN ERROR

Raising awareness of cybersecurity policies and procedures across organisations is vital, according to Bouza Serrano. He also says sensitive information should only be accessible to the lawyers working on a given case. "Cybersecurity by itself is not enough to keep information safe," Bouza Serrano says. "Many of the security breaches come from mistakes made by people."

So, what should firms do if a cyberattack is successful? Firms must be ready for action, with cybersecurity insurance, a detailed action plan, and a crisis communication plan in place. Clients and the relevant data protection authority must be notified immediately, and firms should consider making a public statement – in this instance, pre-prepared draft media statements and client letters could prove useful, lawyers say. Meanwhile, external cyber professionals should work alongside internal IT teams to stop any active threat and also protect against future attacks using the same method. With any luck your law firm will never have to put such an action plan into practice, but with cyberattacks on the increase, it's best to be prepared.