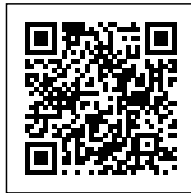


# LIVING A NIGHTMARE

*Posted on 11/04/2019*



Category: [Archive](#)



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. 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 (pictured), 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.

To read the article in full, please download the magazine [here](#)