Cybercrimes and Cyberwarfare are discussed at the "Digital Talk" Roundtable: watch the webinar

12.08.2021 4 min read

Authors

Felipe Palhares

Related areas

Data Privacy and Cybersecurity

Topics

Compliance, Investigations and Regulatory Enforcement | Data Privacy and Cybersecurity | ANPD | Events | GDPR | Home Office | Felipe Palhares | Cybersecurity | Security incidents | Personal data breaches | Pandemic | Digital Talk | Business Crime | Risks management

Any business that wants to remain current and relevant in today's market has to be digital, especially after the covid-10 pandemic, when home-based work and lockdowns were important tools for slowing down the spread of the coronavirus. At the same time, the speed imposed by the pandemic in making digital inclusion a reality gave criminals an opportunity to attack the most valuable asset held by any business in the 21 st century: its data.

Cybercrimes and Cyberwarfare were the topic of discussion at the webinar held on August 10, 2021 within the **Digital Talk Roundtable *(Papo Digital: Mesa Redonda)*** series of webinars led by BMA's Data Protection, Technology and Digital Businesses practice area. Arthur Sabbat, Director of Brazil's National Data Protection Authority, the ANPD, and Rafael Galera, a diplomat and Chief Information Security Coordinator and head of Network Incident Treatment Team for the Brazilian Foreign Service, took part in the conversation, along with Bernardo Weaver, partner in BMA's Business Crime and Compliance, Investigations & Regulatory Enforcement practice areas, and BMA Data Protection partner Felipe Palhares, who moderated the discussion. The webinar can be accessed above and on BMA's Youtube channel (English subtitles).

CYBERCRIMES, INVESTIGATION AND THE PANDEMIC

"The characteristics of these crimes have changed a lot. Cyberattacks used to have political or ideological motivations behind them and were intended to provoke or discredit a certain government authority. Now what we're seeing are attacks intended to obtain personal data, either to be sold on the deep web or to be used in frauds. Because of the pandemic, crimes for financial gain have grown, with many attempted attacks and system break-ins", explains Arthur Sabbat. "It's interesting to see this change in the type of criminal – they used to be people who wanted to show that they could access an official website, that they could get into that place, and now they're attacking for financial ends," adds Felipe Palhares.

Investigating digital crimes also has some differences, since IP masks and encryption can make it difficult to get to the perpetrators, as BMA partner Bernardo Weaver explains. At the same time, "we're seeing this momentary increase during the pandemic, but cybercrimes are still crimes. It's just that life has become more digital and crime is beginning to occur in digital life as well," he says. "They say that data is the new gold rush, the new oil, but not all companies guard their data as carefully as they would guard gold or oil. And during the pandemic, that made it possible for opportunists to succeed. Especially since there's this difficulty in getting proof, even if you know where

to look for it," Weaver adds.

One recent event that will certainly strengthen Brazilian data legislation is the country's accession to the Budapest Convention, [with] a committee of specialists to deal with cybercrime. "This gives us a variety of tools for dealing with these crimes. There are three ways to deal with a cyberattack: the criminal level, the diplomatic level, and the military level, which still hasn't effectively happened," explains Rafael Galera. "On acceding to the Convention, we were required to establish new types of crimes in order to have good coverage for digital crimes," notes Weaver, who believes that the effort invested by Brazil does not necessarily need to be legislative, but rather in "training and resources for the authorities that will investigate" digital crimes.

Diplomat Rafael Galera went on to say that the recent meeting between the heads of state of the United States and Russia seems to have had the effect of mitigating actions by allegedly Russian hackers. US diplomatic pressure is also supposed to be why websites belonging to large hacker groups went offline following the meeting between Joe Biden and Vladimir Putin.

PAYING RANSOMS

What do specialists recommend in cases where data is encrypted or access is blocked? Both Sabbat and Galera are emphatic in saying that the most important thing any organization can do is invest in backups so that they don't risk losing all their information if it is held hostage by cybercriminals. "I believe you shouldn't pay because of the risk that the criminals will not restore all your data. I recommend that organizations guard their data carefully and always maintain a backup because organizations without backed-up data are exposing themselves to enormous risk," points out the ANPD director. Galera agrees: "Making a backup is just basic and, with the advance of cloud computing, it's also inexpensive to make a copy. When people start paying ransoms, we end up providing an incentive for other groups to attack. It might be worth paying for the person that suffered the attack, but it's very bad for public policy.

Weaver, however, believes in a case-by-case approach. "It's a very difficult assessment and has to be made at a very sensitive time. Companies need to have well-organized crisis committees and good advisers to make such a decision. I understand the dilemma over paying, but data is different in nature. Once it becomes public, it can lose value. Its value is precisely in the fact that it is secret, and so having a back-up doesn't help."

› PROFESSIONALS

Professionals who combine legal insight and market perspective

Felipe Palhares