The Importance of Security Incidents Plans

24.02.2021 2 min read

Authors

Felipe Palhares

Related areas

Data Privacy and Cybersecurity

Topics

Corporate Governance | Data Privacy and Cybersecurity | GDPR | Felipe Palhares | Cybersecurity | Pandemic

With the coming into force of Brazil's General Data Protection Law, setting up a well-structured data privacy and protection governance program, which establishes processes and procedures to be followed in certain situations, is an essential measure for reducing corporate risks.

Recent months have seen various cyber attacks, aimed both at businesses of every size and at government institutions, such as the recent incidents involving a number of Brazilian courts. In August 2020, Interpol published a report[1] indicating an alarming increase in the level of cybercrimes, including phishing, ransomware and denial of service attacks, all commonly used by criminals.

This dizzying increase in cybercrime numbers coincides with the spread of the covid-19 pandemic and the intense digitalization of organizations, often implemented abruptly in response to the sudden changes imposed by the pandemic, without time to prepare adequately for a migration to remote work. In such a context, technological weak points and vulnerabilities in information security practices can create targets for attacks and potential breaches.

Cyber attacks usually have one overriding objective: to obtain an illegal economic advantage by selling or using data, whether commercial or personal. Where personal data is concerned, the advent of the Brazilian General Data Protection Law (LGPD – Lei Geral de Proteção de Dados Pessoais) has made it necessary to take even greater care, because violations of the LGPD can expose organizations to fines or, worse, serious reputational damage and orders that restrict or prohibit processing of personal data.

To reduce these risks, it is fundamental for every organization to have a privacy program that establishes specific rules on personal data processing. Although it is not a legal obligation, a privacy program is recognized by the LGPD as a good practice in article 50§2(I), and can serve as an attenuating factor in determining administrative sanctions for violation of the Law.

One of the essential points to be addressed in any privacy program is structuring a security incident response plan that sets out the procedures to be followed when incidents occur, and identifies the persons responsible for dealing with the incident, so that the steps to be taken are clear.

In chaotic situations like those created when access to a company's computer systems are blocked by a hostile attack, it is natural that people do

not know exactly how to react and end up lost in the general confusion and lacking clear direction, which can result in even more complex consequences for the organization.

The more time that passes without coordinated action to resolve the problem, the more difficult it is to gain control of the situation. An incident response plan should serve as a map in times of crisis, providing guidance on practical matters such as the identification, containment, investigation and communication of security incidents. Thus, although security incident response plans are not compulsory, they are highly advisable: as the saying goes, an ounce of prevention is worth a pound of cure.

--

NOTES:

1. See<https://www.interpol.int/en/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf>.

› PROFESSIONALS

Professionals who combine legal insight and market perspective

Felipe Palhares