campos thomaz
advogados

INFORMATION SECURITY INCIDENTS

PRIVACY AND DATA PROTECTION SERIES

1. Concepts

A. What is information security?

Information security is a set of practices to protect information and information systems against unauthorized access, use, disclosure, interruption, modification, and/or destruction.

This concept covers a wide range of areas, strategies, technologies, policies, and procedures aimed at safeguarding what we call the Information Security triad [1], namely:

Confidentiality

is the protection of confidential information from unauthorized disclosure or access. Organizations may achieve confidentiality by implementing access controls and encryption on their systems. By not guaranteeing the confidentiality of information, the organization may expose information (in general) and personal data to unauthorized third parties, causing contractual and financial damages and even harming their image.

Availability

is the guarantee that an organization's information systems and information will be accessible and usable when needed. The blocking of information or information systems may interrupt the organization's internal procedures and, thus, cause damage to the continuity of the organization's business. An organization may guarantee the availability of its information and information systems by implementing backup and information recovery systems.

Integrity

is the protection of information against unauthorized modification, destruction, or corruption, guaranteeing that the information will always be accurate, complete, and reliable. Organizations may achieve integrity by implementing information validation procedures and access controls. Therefore, the lack of integrity of the information stored by an organization may lead to the commitment of crimes of false information and, therefore, cause material and reputational damage to it.

Therefore, information security aims to prevent unauthorized access to information, guarantee the accuracy and integrity of the information, and maintain the availability of the information systems of a specific organization.

[1] Please note that there are other information security models and structures in addition to the triad above, which establishes that information security has other additional grounds, such as responsibility, authenticity, and non-repudiation (which we will not address in this material for didactic purposes).

B. What is an information security incident?

Given the concept of Information Security discussed above, an information security incident is an event that results (or may result) in the compromise, violation, or undue or unauthorized disclosure of confidential, sensitive, or protected information.

An information security incident may occur when there are:
(i) data breaches.
(ii) a cyberattack.
(iii) unauthorized access to confidential or sensitive information.
(iv) a theft or loss of devices containing confidential information.
(v) improper or accidental disclosure of certain confidential information.

Information security incidents occur routinely within organizations. This is routine because situations such as the theft of a laptop and interruption of access to a system are security incidents. After all, from a technical point of view, this exposes confidential information to a threat.

The impact of an information security incident may vary according to the facts related to the incident, from a minor inconvenience to severe consequences, such as financial losses, damage to reputation, and legal penalties.

In view of the foregoing, organizations should have adequate information security incident response plans to refrain and mitigate the impact and damage of an information security incident.

- **Situations that may trigger an information security incident**

Cyberattack

a malicious attempt by an individual or group to disrupt, damage, or improperly access (without authorization) a computer system, network, or device. It may take many forms, including, but not limited to, malware, phishing, and ransomware.

Physical security breaches

occur because of a violation of an organization's physical breach security measures. For example, it may happen when an organization's devices or storage media are stolen, an organization's physical facilities or data centers are unauthorized accessed, or in case of any other physical security violation that risks its information.

Human error

is one of the most common causes of information security incidents[2], often resulting from unintentional mistakes or lapses in employee judgment. For example, an information security incident due to human error may occur when an employee deletes information accidentally; or sets up a wrong system, or sends an email to the wrong recipient.

[2] IBM Security and Ponemon Institute. 2022 Data Breach Cost Report . Available at: < 2022 Data Breach Cost: Full Report (ibm.com)>. Accessed on Feb. 15, 2023. Page 32.

C. What is an information security incident involving personal data?[3]

In Brazil, the General Data Protection Law (Law No. 13,709/2018, aka "LGPD")[4] sets forth that an information security incident involving personal data is any unauthorized access or accidental or unlawful situation of destruction, loss, alteration, communication of personal data, or any inappropriate or unlawful processing of personal data[5].

Additionally, the Brazilian Data Protection Authority (the so-called "ANPD") understands an information security incident involving personal data as a confirmed adverse event that compromised personal data's confidentiality, integrity, or availability[6].

Therefore, organizations should take measures to prevent and respond to information security incidents involving personal data to mitigate possible reputational and financial damage resulting from such incidents and protect individuals' privacy.

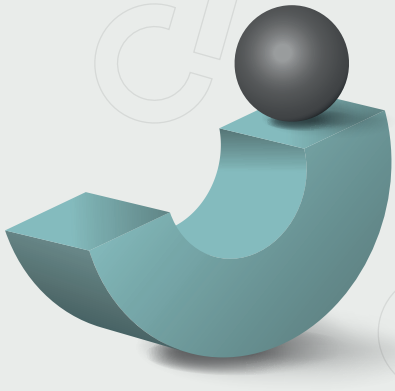
D. Information security incident involving personal data and data breach are they synonymous?

The expressions "information security incident involving personal data" and "data breach" have similar definitions but are not synonymous.

On the one hand, an information security incident involving personal data is any event that affects personal data's confidentiality, integrity, or availability (e.g., when there is a situation of accidental loss, unauthorized access, or intentional (or unintentional) destruction of personal data).

On the other hand, a data breach is a specific type of incident that involves unauthorized access or disclosure of information – including or not personal data (e.g., when personal data is accessed or acquired by a certain unauthorized individual or organization, which may use them for any purposes, including illegal ones).

In other words, an information security incident involving personal data would be the genus of which a data breach would be the species.



[3] LGPD, Article 5, I. personal data: information related to an identified or identifiable natural person.

[4] This is the Brazilian law that governs personal data processing activities in Brazil. It aims to protect the fundamental rights of freedom, privacy, and free development of the personality of natural persons, creating an environment of greater control by individuals over their data and greater responsibilities for the organizations that process them. This law applies to all personal data processing activities, since (a) the processing of personal data takes place in Brazil, or (b) the personal data processing activity intends to offer or provide goods or services or process data of individuals located in Brazil, or (c) data subjects are located in Brazil when their personal data are collected.

[5] LGPD, Art. Art. 46. Personal data processing agents must adopt security, technical, and administrative measures capable of protecting personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication, or any form of inappropriate or unlawful processing.

2. Examples

EXAMPLES OF AN INFORMATION SECURITY INCIDENT

- Malware infection in an organization's computer network.
- Unauthorized access to a database containing confidential or sensitive information.
- Theft or loss of devices such as laptops, smartphones, or hard drives of an organization.
- Social engineering attacks (i.e., phishing) to gain access to confidential and/or sensitive information.
- Internal threats, in which an employee or business partner intentionally (or not) exposes confidential or sensitive information.

EXAMPLES OF AN INFORMATION SECURITY INCIDENT INVOLVING PERSONAL DATA

- Theft or loss of devices such as laptops, smartphones, or hard drives that contain unencrypted personal data.
- Accidental or intentional disclosure of personal data to unauthorized individuals.
- Hacker attacks on an organization's computer systems that result in the theft or compromise of personal data.
- Social engineering attacks where an attacker impersonates a trusted individual or organization to obtain personal data.
- Unauthorized access to personal data by employees who are not authorized to access such information.

EXAMPLES OF A DATA BREACH

- Hacking attacks that allow criminals to access a certain organization's database that contains confidential customer information.
- Ransomware attacks that encrypt an organization's sensitive information and demand payment in exchange for the decryption key and later discloses the data publicly.
- Accidental or intentional sharing of confidential personal information by employees to unauthorized individuals.
- Exposure of confidential information due to a security vulnerability in a third-party vendor's system.
- Theft or loss of devices such as laptops, smartphones, or hard drives that contain unencrypted confidential information.

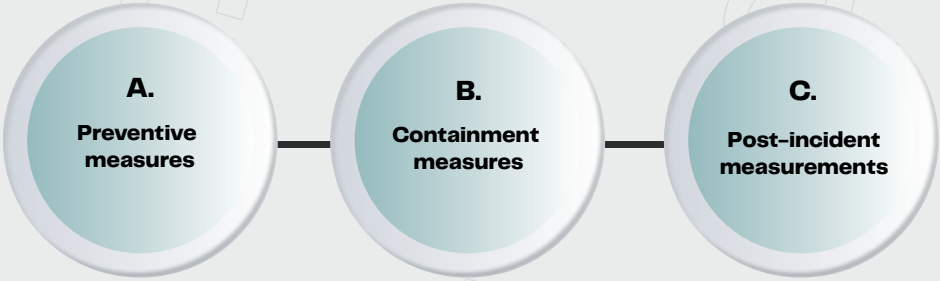
[6] ANPD. Security Incident Reporting. Available at: <https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis#:~:text=A%20comunica%C3%A7%C3%A3o%20of%20incidents%20of%20safety%C3%A7a%20%C3%A0%20ANPD,by%20middle%20of%20completion%20of%20form%C3%A1rio%20available%20below>. Accessed on: Feb. 16, 2023.

3. How to react to an information security incident?

A recent research published by IBM Security in partnership with Ponemon Institute provides that, in 2022, the average cost of an information security incident was US$ 4.35 million, which represents an increase of 2.6% in comparison to the amount calculated in 2021 (i.e., US$ 4.24 million) and of 12.7% in comparison to the amount of 2020 (i.e., US$ 3.86 million).[7]

However, these amounts do not cover damages regarding the reputation and image of an organization that was the victim of an information security incident because such amounts may be immensurable depending on the facts related to the information security incident. Therefore, organizations should have a systematic and well-coordinated response script to contain the incident and mitigate its damage as quickly as possible.

Our experience in dealing with information security incidents (whether involving personal data or not) shows that an effective response script includes the adoption of: (a) preventive measures; (b) containment measures; (c) post-incident measures (detailed below).



A. Preventive measures

Our experience shows that the implementation of preventive measures for information security incidents not only reduces the possibility of an information security incident from occurring but also can substantially reduce the damage that an incident can cause.

In view of the foregoing, please find below some essential steps (in our view) that organizations should take to prevent an information security incident from occurring:

Physical security measures:
Designed to protect an organization's physical assets and facilities from physical security breaches, which may include security cameras, access controls, security guards, alarms, and other measures designed to prevent unauthorized access, theft, and other physical security incidents.

Network security measures:
Aimed to protect an organization's networks and systems against cyberattacks and other threats to an organization's cybersecurity, including, but not limited to: firewalls, intrusion detection software, antivirus software, antimalware, use of encryption, among other security measures designed to prevent or detect cybersecurity incidents.

Data backup and recovery:
Designed to ensure that information assets may be restored quickly in case of an information security incident; they may include regular information backups, redundant storage of data, and implementation of data recovery plans that outline steps to be taken in the event of an information security incident or another emergency.

[7] IBM Security and Ponemon Institute. 2022 Data Breach Cost Report. Available at: <2022 Data Breach Cost: Full Report (ibm.com)>. Accessed on Feb. 150, 2023. Page 5.

Access and authorization controls:
Designed to ensure that only authorized persons have access to systems, information, and facilities. They may include a combination of user authentication measures (e.g., passwords, biometrics), access controls (e.g., role-based access control), and other information security measures designed to prevent unauthorized access to information assets.

Employee awareness and training:
One of the most effective ways to prevent information security incidents is to make the organization's employees aware of good information security practices (i.e., training on best practices for password management, use of email and Internet and social engineering awareness), as well as conduct information security campaigns (on a regular basis) to keep employees informed about how to prevent the latest threats and vulnerabilities.

Implementation of a privacy and personal data protection governance program adequate to the organization's needs:
Due to the recent regulation on privacy and data protection worldwide, the implementation of a privacy and data protection governance program in the organization is an effective preventive measure. That is because a good privacy and data protection governance program involves: (i) the appointment of a Data Protection Officer to be the interlocutor with internal and external personal data subjects and authorities; (ii) the mapping of the organization's personal data flows and, consequently, its vulnerabilities; and (iii) the implementation of internal policies and procedures that may mitigate information security risks involving personal data.

Implementation of response procedures regarding information security incidents (including those that eventually involve personal data):
Regardless of the efforts implemented by an organization to prevent the occurrence of an information security incident, its occurrence is still possible. Therefore, the organization should have predefined procedures for responding to incidents and notifying relevant parties, including data subjects and authorities, when necessary (i.e., at a minimum, an Information Security Incident Response Plan).

Take out an insurance policy with cyber risk coverage:
The coverage of a cyber risk insurance policy covers amounts of damages due violation of information assets (including personal data), as well as expenses that an organization may eventually incur or pay if it is victim of an information security incident. The prior contracting of a cyber risk insurance policy aims to protect the organization from financial losses resulting from an incident in information security, that is, maintain financial health so that it can reestablish itself with peace of mind after the incident.

Recurrent review and update of the preventive measures adopted:
Since the regulation on information security, privacy, and data protection is constantly evolving, as well as the technologies used by organizations and by cybercriminals, new threats and risks to the information assets of organizations (including personal data) may arise. Therefore, organizations should regularly review and update the preventive measures they have adopted to ensure that they serve their purpose effectively.

B. Containment measures

Follow the guidelines of the information security incident response plan/procedures predetermined by the organization.

Collect as much information as possible about the incident, including the type of incident, the affected systems and data, and the time and date of the incident.

Identify and isolate affected systems/devices/networks to prevent further damage or loss of information assets to contain the incident.

Determine the extent of the incident and the type of information assets affected, which includes, for example, the risk of damage to personal data subjects and business partners, as well as the likelihood of recurrence of the incident.

Mitigate damage suffered by restoring information assets using backups, removing malware, and repairing affected systems/devices/networks.

Assess whether the incident needs to be reported to regulatory authorities or affected individuals according to the applicable regulations in force.

C. Post-incident measurements

Investigate the cause of the incident:
After the organization has contained the incident and the authorities and other affected parties have been notified, the organization should conduct a deep investigation to assess the cause of the incident and identify any vulnerabilities exploited for the incident to occur.

Review and improve procedures:
After the organization has contained the incident and investigated its cause, it is time to analyze the effectiveness of the previously established procedures to implement improvements and mitigate the risks related to new incidents. In this regard, we believe it is essential that the organization conduct further training and awareness campaigns with its employees on this matter.

4. What should an organization know if an information security incident affects its business in Brazil?

A. Communication duties

In Brazil, there is not a single regulatory body responsible for receiving notifications of all types of information security incidents. Thus, the requirements for reporting an information security incident will depend on the specific circumstances and the type of data affected.

However, there are some authorities that the organization victim of an information security incident must notify, depending on the nature of the incident, namely:

Agência Nacional de Aviação ("ANAC")
in case the organization is regulated by ANAC (aviation sector organization) and if an information security incident involving personal data occurs.

Agência Nacional de Energia Elétrica ("ANEEL")
if the organization is regulated by ANEEL (electricity sector organization) and the cybersecurity incident is relevant and substantially affects the safety of the facilities, operation, or services to users or data.

Agência Nacional de Telecomunicações ("ANATEL")
in case of organizations regulated by ANATEL, and if the incident is relevant and substantially affects the security of telecommunications networks and user's data.

ANPD
if the incident involves personal data and represents a relevant risk or harm to the data subjects, involves many data subjects, affects sensitive personal data, or involves personal data of vulnerable individuals.

Banco Central ("BACEN")
by banks, financial institutions, payment institutions and PIX participants, in any event of an information security incident involving personal data on the PIX infrastructure, regardless of the severity of the incident and how it affects data subjects..

Comissão de Valores Imobiliários ("CVM")
if the organization is subject to regulation by the CVM (a publicly held organization) and if the cybersecurity incident is material.

Superintendência de Seguros Privados ("SUSEP")
if the organization is subject to SUSEP (insurance sector organization) and if the information security incident is considered relevant.

Personal Data Subjects
in addition to notifying the ANPD and the regulatory authorities, the organization may be required to notify affected data subjects and business partners if the breach is likely to result in a risk of damage to their rights or interests. As an example: banks and financial institutions are obliged to notify the data subjects involved in any information security incident involving personal data on the PIX infrastructure.

B. Sanctions

Suppose an organization suffers an information security incident in Brazil. In this case, it may suffer penalties, fines, or other legal consequences, depending on the nature and severity of the incident. Additionally, suppose the incident involves criminal activity. In this case, the organization could face criminal charges, and the individuals or organizations involved could be held criminally liable.

However, the severity of the consequences will depend on the specific circumstances of the incident, such as the type of data involved, the measures taken to protect the data, and the measures taken to deal with it.

Suppose the organization has implemented adequate data protection and information security measures and adopts prompt and effective measures to deal with any information security incidents. In this case, the consequences might be less serious.

Furthermore, failure to notify the competent authorities of an information security incident may result in fines and other penalties by current Brazilian regulations applicable to each case.

Our recognitions

Análise Advocacia (2021)

Chambers & Partners Brazil (2021 & 2022)

Leaders League (2021 & 2022)

Transactional Track Record (2021 & 2022)

The Legal 500 (2022)

Meet our Partners

Alan Campos Thomaz

Partner

Technology & Digital Business, Privacy and Data Protection, Fintechs and Intellectual Property

at@camposthomaz.com

+55 11 9 8375.2627 +1 (650) 6436652

Filipe Starzynski

Partner

Litigation & Law Enforcement, Civil, Real State, Labor and Family

filipe@camposthomaz.com

+55 11 9 7151.9639

Juliana Sene Ikeda

Partner

Intellectual Property, Technology, Contracts and Life Sciences

juliana@camposthomaz.com

+55 11 9 8644.1613

Follow us

campos thomaz advogados

Subscribe to our newsletter