CIA in Action: How Privacy Professionals Help Craft a Secure Information Security Program

by
Brett Cook
&
Samantha Corsey

Privacy professionals play a pivotal role in assisting organizations in the development of robust information security programs. In this article, we will explore several essential principles of an information security program and the integral role privacy professionals fulfil within them. The key security goals of a system are commonly described as *confidentiality*, *integrity*, and *availability*.

Confidentiality refers to keeping sensitive data away from unauthorized users. This includes personal data, trade secrets and other restricted data. Because this data is specific to only authorized users, without the proper safeguards, this information can become susceptible to security incidents (commonly referred to as "breaches") which can result in data loss, financial loss and reputational damage. To mitigate the risk of unauthorized data access, organizations can employ the following strategies:

- Restrict access trusted personnel with a need to know;
- Encrypt data at rest and in transit;
- Implement data retention and information security policies; and
- Utilize non-disclosure agreements.

A failure to protect data confidentiality may also be a failure to protect privacy. Privacy professionals must collaborate closely with security personnel to evaluate data elements within the scope of a potential security incident to identify any regulatory or contractual disclosure obligations that may have been triggered. To effectively manage their data, organizations need to have a clear understanding of its origin, storage location, and the parties with whom it is shared. Further, they should have the ability to locate, tag, and inventory the different data types (i.e., sensitive personal data) across both on-premises and cloud environments during a security incident.

Integrity refers to preventing unauthorized modification of data, which could include replacing a correct value with an incorrect one or deleting data. Privacy regulations like the General Data Protection Regulation (GDPR) explicitly state that data quality is mandatory. This essentially means that the data collected by organizations should be accurate and comprehensive. Data files may not meet this requirement if they contain errors or omissions due to a lack of data integrity maintenance after collection.

One way to protect data integrity is to limit access and control. Privacy professionals can help organizations identify valid business objectives and determine who is required to have access to specific data elements. Moreover, they possess the capability to identify any potential

overexposure of data and monitor data sharing across internal and external access points. By providing regulatory guidance to security teams related to employee surveillance, privacy professionals can diminish the risk posed by insiders, expedite the implementation of the zero trust model (which operates on the principle of not blindly trusting anyone and granting access only after legitimate authorization is established), and enhance the overall data security when leveraging access intelligence technologies.

Availability pertains to ensuring that computer systems are available when needed, even under duress (like a natural disaster) or after suffering intentional cyberattacks. Data availability is critical for business continuity, disaster recovery plans, recovery time objectives, recovery point objectives, and service level agreements.

Furthermore, Fair Information Practice Principles and sector-specific regulations in industries like healthcare and finance may require organizations to provide reasonable consumer access to their data. Security incidents that hinder this access could potentially lead to legal or regulatory consequences. Privacy professionals can help organizations identify these areas, evaluate risk, and develop alerts to accelerate investigations so security teams can quickly investigate, resolve/mitigate, and develop risk reduction techniques.

In today's data-driven landscape, the collaboration between privacy professionals and cybersecurity teams is paramount in establishing a robust data security program. By joining forces, privacy experts can ensure that organizations not only comply with complex privacy regulations but also proactively mitigate potential risks to sensitive data. Working in tandem, these groups strengthen an organization's ability to protect its data, maintain trust with stakeholders, and navigate the intricate regulatory landscape of data privacy and cybersecurity. This collaboration is not just a best practice but a strategic imperative for safeguarding sensitive information and upholding privacy rights.

References:

- Breaux, Travis D. *An Introduction to Privacy for Technology Professionals*

- ***Data Confidentiality: How can Businesses Protect Their Data?***
  https://penneo.com/blog/data-confidentiality/

- **Federal Privacy Counsel- Fair Information Practice Principles**
  https://www.fpc.gov/resources/fipps/

- ***Is The CIA Triad Relevant? Confidentiality, Integrity & Availability Today***
  https://www.splunk.com/en_us/blog/learn/cia-triad-confidentiality-integrity-availability.html#:~:text=Confidentiality%20protects%20information%20(data)%20from,when%20needed%2C%20even%20under%20duress

- ***The Largest Cyberattacks of 2023***
  https://www.splunk.com/en_us/blog/learn/cybersecurity-attacks.html

Brett Cook is Senior Privacy Counsel for Motorola Solutions, Inc. and serves as an Executive Committee Member for CLA's Privacy Law Section.

Samantha Corsey is an Intellectual Property Project Assistant at Foley & Larnder, LLP.

The views expressed in this article are solely the personal opinions of the author and do not reflect the views or opinions of their employers.