Hi Ben Zapka,

I appreciate your insights on data protection. It's very impressive. Regarding PII data protection, you raised some excellent points. It's an intriguing problem that you have posted.

You have emphasized the confidentiality of personal data and the need for data encryption and authorized personnel access as a solution.

The problem raised with data uploads to other websites and the corporation-binding regulations' transfer of personal data outside of the EU (Allé, 2023). Examining the terms and conditions of the contracts and ensuring that the necessary protections are in place to comply with transfer regulations may be of interest to you (Irwin, 2020).

Do you believe that the issue might be resolved by implementing an approved code of conduct with legally enforceable commitments made using the required contractual clauses and administrative arrangements?

References

Allé, N. (2023) Processing of personal data, Novo Nordisk. Available at: https://www.novonordisk.com/science-and-technology/research-technologies/processing-of-personal-data.html

Irwin, L. (2020). *IT Governance Blog: data transfers outside the EU - the GDPR rules*. [online] IT Governance UK Blog. Available at: https://www.itgovernance.co.uk/blog/transferring-personal-data-under-the-gdpr.

Hi Panagiotis Mourtas,

You have highlighted some excellent points and pointed out the problem that is prevalent in today's organizations. You made a compelling case for the use of data by the various organizational divisions and the potential issues that may occur.

The issue that has been highlighted is widespread and generic in today's IT industry. Nevertheless, the study omits several particular MDM solutions that might be used to address this problem.

By employing some of the ETL tools, data consistencies can be integrated with the metadata framework in the MDM solution, ensuring that the required transformations (Arnaud, 2023) are taken care of before changing the final data.

When updating data, departments can use ETL tools like Informatica to standardize the data translation to master data (Walia, 2022). This will help to enhance data quality and prevent issues.

Do you still believe that, in consideration of MDM solutions, this is an open issue that cannot be addressed if the organization is going to invest in strategizing data management?

References

Arnaud, F. (2023) Part 2 - Build Your Own Master Data Management Solution for Seamless Integration and Strategic Insights. Available at: https://keyrus.com/be/en/insights/part-2-build-your-own-master-data-management-solution.

Walia, A. (2022) Master data management strategy: Key steps for success, Informatica. Available at: https://www.informatica.com/gb/resources/articles/master-data-management-strategy.html#3.

Hi Yuji Watanabe,

I appreciate you sharing this post, and I agree that you've pointed out that security risks are typically the result of employee error.

As you rightly mentioned, ninety percent of cyberattacks are caused by information that employees unintentionally supply. For this reason, it is critical to raise security awareness within your department and to ensure that staff receive proper training (MacKay, 2018).

Nonetheless, considering additional avenues for cyberattacks, the systems must be sufficiently maintained to identify any gaps in the product. The Global Threat Report's analysis revealed an increase in attacks resulting from OS design flaws that can only be identified by exploiting the weakness (Kulkarni, 2023).

Do you think that maintaining and updating the security landscape to handle the latest security issues should be a continuous process rather than just a one-time activity when building security compliance?

References

MacKay, J. (2018). How to Promote Cyber Security Awareness in Your Organisation | MetaCompliance. [online] www.metacompliance.com. Available at: https://www.metacompliance.com/blog/cyber-security-awareness/how-to-promote-cyber-security-awareness-in-your-organisation.

Kulkarni, A. (2023). 10 takeaways for CISOs from the 2023 Global Threat Report. [online] Elastic Security Labs. Available at: https://www.elastic.co/pdf/elastic-10-takeaways-for-cisos-from-2023-global-threat-report.pdf.