ISACA Now Blog

The Impact of GDPR on Cybersecurity Managers

Anna Vladimirova-Kryukova, certified Data Protection Officer, CSX Fundamentals certificate, COBALT, Latvia
| Posted at 3:04 PM by ISACA News | Category: Security | Permalink | Email this Post | Comments (0)

Around six months have passed since the General Data Protection Regulation (GDPR) took effect. Among many unclear implication of GDPR, the vaguest might be how to ensure compliance with the security requirements, including data protection by design and by default. It has been a tough task for cybersecurity professionals to understand how to interpret the GDPR requirements and probably will be a continuous struggle over the next several years.

However, the interpretation of these GDPR provisions should not be the only aspect to command our attention. The increased penalties (up to 20 million Euros or 4 percent of the total annual turnover) made many companies think not only about how to ensure compliance, but also about what happens if the required measures are not implemented. Thus, the question for many companies is who will be liable for compliance failures regarding GDPR security rules: the company or cybersecurity manager?

There is no single answer and many aspects depend on the laws, regulations and case-law in each country. For example, there are cases in the UK that prove that the issue of employees' responsibility for data protection should be addressed, but the scope of the liability may vary. For instance, in one case an employee was sentenced to eight years in prison, and the company is still in court trying to prove that it should not be liable. In another case, a six-month sentence was imposed only on the employee for unauthorized access to personal data.

Moreover, the scope of responsibility might be a concern for companies that have offices all around the globe, which entails different application of laws regarding the liability of employees. Taking into consideration high stakes and new broad security requirements introduced by the GDPR, it is time for companies and their cybersecurity managers to make their relationship as transparent as possible for both parties. This can be done in the following way:

1. **Define the scope of responsibility.** Cybersecurity managers should have a clear understanding of their specific role regarding the GDPR implementation, the systems that are covered, and their access rights.
2. **Define the territory.** It is necessary to understand the territorial scope of the GDPR compliance that a specific person is responsible for. Is it the place where the manager is physically located or is it broader? This question should be answered especially in cases of international group companies where one person can be in charge of several organizations.
3. **Agree on communication.** If the scope of the responsibility overlaps with other managers or employees, it is crucial to agree on how you work together and how common tasks are distributed.
4. **Prove it.** All of the agreements reached on the scope of responsibility and distribution of tasks should be provable. If it is possible and reasonable to put them on paper, it should be done. Other options (such as communicating the main terms over email) are also relevant if the company and cybersecurity manager will be able to prove, if a conflict takes place that a certain order was accepted by all stakeholders.

It might seem that it is sometimes more beneficial to avoid agreeing on specific things and engaging in unpleasant talk about what happens in case of an incompliance penalty. However, a clear framework addressing the scope of responsibility and liability can be considered a personal incident response plan for cybersecurity managers that will help them to perform their work in transparent and clear conditions.

Comments

There are no comments yet for this post.

You must be logged in and a member to post a comment to this blog.