- Data privacy / Data breach

Privacy and data security mistakes to be avoided

BusinessMirror · 12 Jul 2022 · A4 · By Henry J. Schumacher

MOST companies lack the experience and resources needed to manage the plethora of security, privacy, and compliance issues inherent in a growing technology-based business. Nevertheless, the legal and business implications of poorly managed privacy and data security practices are too important to ignore. A single error can undermine the trust of investors and customers, attract unwanted regulatory attention or litigation. Here are 7 common privacy and data security mistakes that you must avoid:

Too frequently, company management and boards fail to pay sufficient attention to the significant problems that will arise from a company's failure to provide adequate security or to comply with applicable privacy laws. Litigation involving privacy and security is becoming mainstream.

Too many pay little attention to the fact that businesses are governed by a wide range of laws and standards, and are expected to operate within commonly accepted practices. Among other things, they may ignore the fact that the collection, use, and processing of most personal information is regulated here and abroad. Ignoring these laws may lead to significant errors and may in fact subject the company and its managers to legal and other action.

Some companies may think that their ability to succeed requires that they be nimble. They may believe that policies and processes slow them down and are not a business imperative. However, in the absence of rules defining who is allowed to access certain information or what uses are restricted, employees, subcontractors or visitors might inadvertently access highly confidential or sensitive data and misuse it.

Some companies hire third parties, outsource some of their functions, or locate their operations in the cloud because they do not have sufficient resources to hire personnel or to purchase equipment. In doing so, they may think that they have passed on to those third parties the responsibility for their data.

However, the company that initially collects the data remains primarily responsible for anything that happens to the data. The entity that the customers know—not the obscure service provider—will be the one that will be sued or investigated if data is illegally processed or inadequately protected. It will be the one whose reputation and trustworthiness will be at risk.

Security breaches are to be avoided. They are significantly disruptive. A company that has implemented a well thought through written security program will be less exposed to potential security breaches and to the significant consequences of security breaches. In most cases, a company that has suffered a breach of security might be required to publicly disclose the occurrence of the breach. It may have to send notices to affected parties and regulators, and offer credit monitoring or identity theft insurance, which is usually a significant expense.

Some companies tend to collect too much data just because "we may need it later" and "storage is cheap." The more data a company has in its custody, the more vulnerable it is to legal violations and security breaches. The more data a company has, the more time and data experts it will need to retrieve it. Collecting a massive amount of data also causes significant security risk. The larger the volume of data—the higher the probability that it will be stolen.

When discussing personal data protection, it is common to hear: "We don't have any personal data, our data is anonymized, and it cannot be tied to an individual." This is a significant mistake. While it might have been true, a long time ago, that anonymization prevented the association of a particular individual to a particular data set, this is no longer the case. In the world of data analytics, big data, semantics and other tools, there is no such thing as anonymity. Too often, a competent data scientist will be able to crack the anonymization shell in a short time.

Why am I writing about Privacy and Data Security mistakes? Data breaches are in the news more and more. We strongly believe that a lot of training in data science, data analytics and data management is needed to provide companies and their employees with the capabilities to stay relevant. Consequently, we have developed training in these areas. If support is needed, contact me at hjschumacher59@gmail.com