Develop a Data Breach Response Plan

Bookmark this page

Although many companies haven't developed a breach response plan yet, such a framework has an important role in dealing better with cybersecurity incidents, as well as limiting damages and restoring public and employee trust. The main aim is to set the roles and responsibilities for people tasked with managing a breach; including a draft notification and summarising the process of investigation is also vital.

The importance of a response plan is highlighted by regulations as well.

For example under GDPR requirements, organizations have to respond to data breaches within 72 hours of detection; this includes gathering all related information, reporting the breach to the relevant regulator and informing impacted individuals. As technology continues to drive businesses, it also continues to make them vulnerable to cybercrime. In order to reduce the risk of enriching the ever-growing list of breach victims, cybersecurity should become a priority for every organization.