Lack of confidence in data security can cost you more than you think

By Jason Hart, Chief Technology Officer (CTO) of Data Protection at Gemalto

The European Union's General Data Protection Regulation (GDPR) came into effect almost two months ago. Leading the way to a new era of data protection, the long-awaited GDPR has emphasized the importance of data security more than ever before. Besides tarnishing their reputation, businesses face the risk of encountering large fines if they don't align with the regulation.

Although cybersecurity is top of mind for most organizations with the new law, they still feel uncertain about their data protection practices. Recent research from Gemalto, its fifth-annual Data Security Confidence Index, which surveyed 1,050 IT professionals and 10,500 consumers globally, revealed that businesses differ in their capability to study data that has been collected. Shockingly, two in three companies (65%) admit they don't have the proper resources to analyze data and therefore are unable to do so.

This finding forces me to think – the majority of companies don't understand the value of their data, because they aren't taking the necessary steps to study the information they are gathering from customers. That's why organizations are stunted in the process of applying appropriate security controls to protect the valuable information they possess. Unsecured data is a hacker's dream. Attackers can offer it up to the dark web or use ransomware, causing financial loss and reputation damage. It can take years to uncover data manipulation, which can put everything from an organization's business strategy to product development at risk. In today's digital world, data informs everything, so its value cannot be underestimated. We've all seen our fair share of breaches this past year that illustrate how detrimental they can be to an organization.

Organizations have gaps in confidence levels

Almost half of IT professionals say perimeter security is effective at keeping unauthorized users out of their networks. However, two thirds of them believe unauthorized users can access their corporate networks and less than half are confident in the security of their data once cyberhackers are inside. With that being said, more than half of companies don't know where all of their data is stored. Moreover, more than two thirds admit they don't carry out all the processes aligned with data protection guidelines such as GDPR.

This gap in people's confidence in their organization's data protection policies indicates the reason for continuous breaches: twenty-seven percent of organizations reported their perimeter security was breached last year. Of those that had suffered an attack, only 10% of the compromised data was protected by encryption, leaving the rest exposed. In order to secure their networks IT professionals need to use encryption, which, paired with other solutions, will provide an essential security base for a robust system needed to guard sensitive information.

Crucial steps for strong security

When it comes to cybersecurity it's a valid question to ask, "*Who's in charge?*" It's crucial for organizations to get their houses in order, starting with determining who will be responsible for overseeing security measures. Every executive board needs to have a Data Protection Officer, a chief individual who leads data security from the top down. Second, organizations must organize and study

collected data to properly protect it and make informed business decisions. Lastly, IT pros need to change their outlook on security as a whole. It's no longer a case of if, but when a breach occurs. Therefore, organizations should implement a comprehensive approach to cybersecurity, using methods such as encryption, two-factor authentication, and key management in addition to perimeter protection.

These critical steps aren't solely for the sake of companies, but also for consumers who have data records tied to these businesses. The vast majority of consumers say it's imperative that organizations comply with data regulations due to their growing understanding of breaches and communications around GDPR. Actually, fifty-four percent of consumers are aware of what encryption is, which shows knowledge of how data should be protected.

Cost of poor data security

Over the years, security experts' predictions about potential costs of a breach have been increasing. Cybersecurity Ventures estimates the costs related to cybercrime damages to reach $6 trillion by 2021. From upgrading IT infrastructure to paying legal fees and government fines – many costs are either tangible or intangible. We've now reached the tipping point on the implications of data breaches, that can negatively affect company's market value and ruin the reputation of the corporate and management teams.

With pressure to ensure consumer data is protected and the risks and costs of breaches growing, organizations need to take immediate steps to transform their approach to data security. Companies need to have confidence in how they gather, analyze, and store their information. Only having this understanding and ensuring compliance, they will be able to adopt effective security measures.