HealthManagement
Promoting Management and Leadership

Securing the Future: Essential Data Protection Strategies

The digital age has brought unprecedented business opportunities but has also introduced significant risks. With the cost of data breaches reaching an average of €4.22 million ($4.45 million), protecting sensitive information is no longer just a technical challenge but a strategic imperative. The threat landscape is increasingly complex, fuelled by advancements in cybercrime techniques, the proliferation of digital collaboration tools and the rapid adoption of cloud and AI technologies. In this context, organisations must prioritise a comprehensive approach to data security. An annual report by Metomic explores three critical pillars of data protection: managing high-risk data, addressing the challenges of data sprawl and stale data and enforcing robust access controls to safeguard sensitive information.

Managing High-Risk Data

Not all data carries equal risk. Specific categories, such as Personally Identifiable Information (PII), Payment Card Information (PCI) and passwords, are particularly vulnerable to breaches. Exposing these data types can have severe consequences, ranging from financial penalties under regulations like the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS) to significant reputational damage. Organisations must, therefore, implement strategies to identify and prioritise these high-risk data points.

Modern workplaces increasingly rely on platforms such as Slack, Google Drive and ChatGPT for collaboration, where sensitive data often resides. Unfortunately, these environments can become repositories of risk if not properly managed. Organisations can use AI-powered tools to classify data based on its sensitivity and assign risk levels to each asset. This categorisation allows security teams to focus their efforts where most needed, such as ensuring the protection of files containing customer payment details or employee identification numbers.

The importance of prioritising high-risk data cannot be overstated. For instance, while only a small percentage of files may contain financial information, the ramifications of their exposure are often catastrophic. Similarly, passwords stored insecurely can compromise entire systems. By addressing these vulnerabilities proactively, organisations meet compliance requirements and create a more secure digital environment that supports long-term growth and resilience.

Tackling Data Sprawl and Stale Data

Data sprawl, the uncontrolled spread of information across various platforms and applications, has become one of the most pressing challenges for security teams. The adoption of collaborative tools has made data sharing easier than ever, but it has also led to sensitive information being scattered across numerous locations. Files stored in cloud platforms, shared in open communication channels or downloaded for personal use create an expanding attack surface that is difficult to monitor and protect.

Compounding this issue is the problem of stale data—information that has not been accessed or updated for extended periods but continues to exist within the organisation's systems. According to recent analyses, as much as 86 per cent of data remains untouched for over 90 days, with nearly half of it remaining stagnant for more than two years. Such data represents a compliance risk and provides an attractive target for cybercriminals. Malicious actors often exploit stale data as it is less likely to be actively monitored or protected.

Organisations should conduct regular data audits and implement retention policies that automate information lifecycle management to combat these challenges. For example, files not accessed in 90 days could be flagged for review, while those dormant for over a year may be securely archived or deleted. These measures reduce the volume of sensitive data and ensure that information critical to operations remains properly secured and easily accessible. By tackling data sprawl and stale data, organisations enhance their ability to detect, monitor and mitigate potential security breaches.

Strengthening Access Controls

While understanding where sensitive data is stored is critical, knowing who has access to it is equally essential. Poor access management is one of the most common causes of data breaches. Freelancers, contractors or former employees often retain access to company systems long after their association with the organisation has ended, creating a significant vulnerability. Similarly, files shared publicly or with overly broad permissions, such as Google Drive files set to “public,” amplify risks.

Access control challenges are further complicated by human error. Employees may inadvertently share sensitive files in public or external channels, exposing them to unauthorised users. The rise of collaborative SaaS tools has made such mistakes more frequent. For instance, sensitive data shared within team communication platforms like Slack can quickly proliferate if users are unaware of proper sharing practices.

Addressing these risks requires a combination of education and technology. Building a “human firewall” is an essential step in which employees are trained to understand the implications of poor data-sharing practices and are diligently equipped to follow security protocols. Tailored training for departments handling high volumes of sensitive data, such as HR, finance and engineering, can significantly reduce errors. Beyond training, automated solutions are invaluable. Tools that monitor sharing permissions, flag unusual access patterns and automatically revoke access for inactive users ensure higher security. Moreover, enforcing policies such as limiting external sharing by default and implementing strong password protocols can further minimise risks.

Data security demands a proactive and multifaceted approach. Organisations must focus on managing high-risk data, addressing the challenges posed by data sprawl and stale data and enforcing robust access controls. These strategies are essential for regulatory compliance and protecting an organisation’s financial stability and reputation in an increasingly interconnected digital world.

Organisations can effectively mitigate risks by leveraging technology, such as AI-driven risk assessments, and fostering a culture of security awareness among employees. As cyber threats evolve, staying ahead requires continuous adaptation and vigilance. The stakes are high, but with a comprehensive strategy, businesses can secure their most valuable assets and thrive in the digital age.

Source: Metomic

Image Credit: iStock

Published on : Sat, 30 Nov 2024