Don't Overlook Email When Planning for GDPR Compliance

Table of Contents

As cyberattacks escalate in volume and sophistication, data protection is more vital than ever. The European Union (EU) General Data Protection Regulation (GDPR) is one of the most demanding compliance mandates to date, aimed at ensuring that any organization working with European consumers or enterprises use all the necessary means to protect the personal data of individuals.

With the May 25, 2018 deadline for full GDPR implementation and compliance less than a year away, enterprises around the globe need to focus on one of their most essential and mission-critical applications—email—to ensure they meet a key principle of the legislation: accountability.

Given the sheer number of emails created, sent, received, stored and managed every day, the potential for compliance violations is substantial. So are the potential economic penalties for non-compliance, as discussed in this paper.

mimecast®

TechTarget® | Custom Media

Email is mission-critical, there can be no compromise on data protection

GDPR is a broad legislation spanning all data types, but it's essential to keep in mind that significant personal data is held in email communications. According to Radicati Group, the number of business-to-business emails will reach a staggering 124.4 billion per day in 2017.[1] Organizations must deploy a data privacy and security strategy for email that encompasses people, processes and technology to meet the stringent requirements of the GDPR.

There is plenty of work to be done. Osterman Research estimates that a majority (58%) of midsize and large organizations are unprepared for the impact of the GDPR, including its potentially crippling fines and core principle of privacy by design.[2] Although many organizations are familiar with data protection, security and privacy, they are not transforming their business architecture in terms of how GDPR mandates are handled.

Personal data includes names, telephone numbers and location information that can identify an individual. In the U.K., the current Data Protection Act allows for a maximum fine of £500,000 for a breach. However, that magnitude of fine is minuscule compared with the tough, new €20 million, or 4% of global revenue, under the GDPR.

This threat is helping to focus minds at the board level, and many companies have recruited a data protection officer to coordinate efforts for a GDPR compliance strategy. The GDPR emphasizes the principle of accountability and the need for organizations to demonstrate they have taken reasonable measures to protect personal data.

1 "Email Statistics Report, 2015-2019," Radicati Group, March 2015

2 "GDPR Compliance and Its Impact on Security and Data Protection Programs," Osterman Research, 2017

GDPR challenges for email

Personal data about individuals is shared extensively within emails, and these emails must be produced by an organization if a subject access request (SAR) is made by individuals exercising their right to see their personal data. Considering the daily volume of emails, and the fact that some sectors, like financial and legal, must retain emails for six years, the GDPR will have a huge impact on how emails are processed, archived and accessed in relation to ease of accessibility in the event of a SAR. Such requests must be fulfilled within a month, and at no cost to the individual—another one of the GDPR's precise mandates.

The number of SARs is set to increase, but IT managers can't afford to have their time taken up with these requests and call center agents are better focused on ensuring customer service. This administrative burden can be handled only by effective technological solutions and business processes. Secure email archives that can be searched flexibly and quickly are essential in dealing with the demands of an escalating number of SARs.

Criminals are intent on devising sophisticated email phishing attacks to steal money, credentials, customer data and other valuable intellectual property. When it comes to security, people are often the weakest link, meaning organizations must educate employees to inculcate security and privacy best practices for email-based data.

Using weaponized attachments and impersonation emails designed to look as if they are from friends or colleagues, attackers lure unsuspecting victims to click on malicious links and unleash paralyzing malware and viruses. Deploying advanced email security, data loss prevention and encryption mechanisms can reduce the risk of attacks and help mitigate breaches of GDPR mandates. Recent ransomware attacks such as WannaCry and Petya that impacted many organizations globally underlines the importance of implementing and maintaining up to date security.

Preventing such attacks and email leaks has never been more critical, as any violations are liable to attract intense scrutiny through high-level enforcement of the GDPR.

Non-compliance can cost money, reputation and customers

While the prospect of huge fines is making headlines and prompting board-level conversations about data protection, there are other adverse implications of falling afoul of the GDPR.

In the digital age, where reputations can live or die on social media and a competitor is only one click away, organizations cannot afford to risk the long-term fallout of lost business because customers are concerned that adequate procedures aren't being followed to secure their personal data.

The GDPR allows for legal action from customers. People must be informed if their data is stolen in a cyberattack, and they can sue. Awareness of these rights is growing, and such action is inevitable if customers believe their data has been mishandled or compromised by an organization.

The impact of privacy breaches on business valuations is another consideration. For example, Verizon sought a $925 million discount on its Yahoo merger in the wake of massive cyberattacks on the Internet company, and it eventually got $350 million knocked off the purchase price of the deal.

Mitigating risk and ensuring email resiliency with Mimecast

The GDPR requires a pragmatic, top-down strategy, and email resiliency is fundamental to this multi-pronged approach. Advanced threat protection can defend organizations against phishing, weaponized attachments and whaling attacks targeting individuals with access to valuable data.

Real-time data leak prevention and secure communication policies applied to outbound traffic protect against the leakage of intellectual property and other sensitive data. Secure messaging is vital, with end-to-end encryption regarded as good business practice in any GDPR-led investigation.

With the scope for SARs expected to expand exponentially, email archiving that enables access within seconds is critical to any data storage strategy. As unstructured data and file sizes continue to increase, organizations also want to ensure they can secure large files containing critical information and share them without risk.

Why the Mimecast solution works

Mimecast services are built with privacy and data protection in mind, ensuring a robust email security strategy that eases GDPR compliance.

Mimecast Targeted Threat Protection (TTP) defends organizations from spear phishing, ransomware and impersonation attacks, while Mimecast Content Control and Data Leak Prevention safeguards employee communication through real-time security controls and policies.

Mimecast Cloud Archive improves data governance and ensures SARs can be processed quickly to meet GDPR mandates. A single-console administration for security, archiving and continuity services enable IT administrators to protect email and corporate information efficiently, saving time and money. These capabilities allow organizations to address the challenges as well as take advantage of the opportunities the GDPR offers.

Conclusion

Email security is essential in preparing for the GDPR deadline, and putting security at the center of operations enforcement is underlined by the principle of data protection by design. Mimecast adheres to this principle and is ideally situated to ensure organizations have a robust security solution in place for business-critical emails.

There is no silver bullet to counter cybercriminals, but if your organization wants to ensure best practices and implement a solution that helps mitigate GDPR risk for email, then Mimecast is your first option.

About Mimecast

Mimecast Limited (NASDAQ:MIME) makes business email and data safer for more than 26,400 customers and millions of employees worldwide. Founded in 2003, the company's next-generation cloud-based security, archiving and continuity services protect email, and deliver comprehensive email risk management in a single, fully-integrated subscription service.

© 2017 Mimecast.com All rights reserved.