Enterprise Strategy Group™ by TechTarget

SHOWCASE

Email Encryption Enables Innovative and Secure Digital Business Processes

Date: November 2022 **Author:** Jack Poller, Senior Analyst

ABSTRACT: Organizations are dependent on and constantly introducing new digital business processes that leverage the ubiquity of email. However, information in messages is easily stolen or compromised when it is not encrypted. To provide security and enable digital processes that rely on sensitive data, leading firms are deploying an email encryption platform to secure sensitive information across many apps.

Overview

Email has long been the most common means of electronic communication both within and between organizations, as well as with customers, and the importance of email is steadily increasing. With broad usage, email often contains sensitive or confidential information that is all too rarely protected. Many organizations are realizing that they need to encrypt sensitive information in email, as interception of this information can be compromising and damaging. Further, organizations are facing new and evolving regulatory and compliance standards that can best be met by encryption.

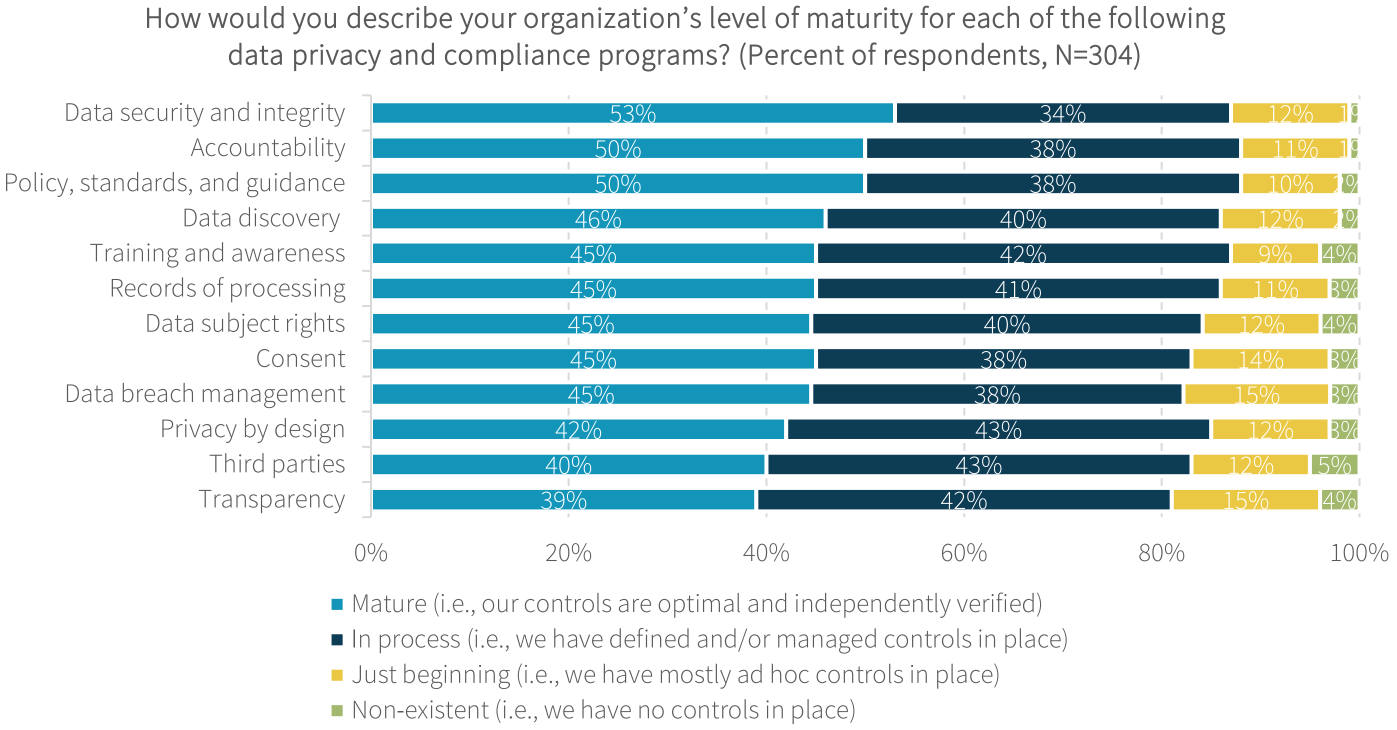
Many organizations also see that email encryption can deliver important customer benefits. The public has become more concerned about theft of their private data, and many people now choose to do business with companies based on those companies' ability to deliver better protection for their personal or sensitive information. For such customers, email encryption can be evidence of an organization's commitment to data protection.

Thus, it is not unusual today for executive leadership to fully support efforts to protect email communications containing private or sensitive information with effective encryption. In fact, most enterprises today have a mature and progressing set of data privacy and compliance policies that can be the foundation of a comprehensive email encryption strategy (see Figure 1).[1]

[1] Source: Enterprise Strategy Group Survey Results, *The State of Data Privacy, Compliance, and Data Security*, October 2021.

This Enterprise Strategy Group Showcase was commissioned by Echoworx and is distributed under license from TechTarget, Inc.

Figure 1. Level of Maturity of Data Privacy and Compliance Programs



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Email Encryption Solutions Must Meet Specific and Demanding Requirements

Many organizations empower IT, developer, and security teams to fix their problem of allowing unprotected sensitive information to be sent by email. These teams know that email encryption solutions are commonly available and that many solutions won't be effective because they are too unwieldy for users, take too long to deploy and implement, or require constant attention and management.

If the mandate is to encrypt all email containing sensitive information, all potential lapses must be eliminated. Complexity created by the encryption solution will lead employees to find workarounds and customers to go elsewhere. What organizations need is an email encryption solution that makes email encryption a central component of business process design, seamless for the users, and more than an add-on used just before sending.

An effective email encryption solution must be agile and flexible enough to support multiple use cases so that one platform can support all use cases for the organization. The encryption platform must deliver the needed level of protection for each specific use case by using the optimal cryptographic and data protection standards for that specific business process. Leveraging a single platform provides efficiency and simplifies management of the email encryption effort. It also ensures consistent implementation of policies and a consistent user experience throughout the organization.

An ideal encryption platform will deliver important business benefits, including:

- Visible commitment to privacy and security: When email encryption is employed, both customers and employees can see that data protection is a corporate commitment. Visible email encryption improves sender and recipient confidence that their data is protected.

- Seamless encryption of email communications: Providing IT, developer, and SecOps teams with a platform that can be integrated into the app development and upgrade processes makes data protection an intrinsic part of these processes. Incorporating encryption as a part of the processes provides better, more reliable security than bolting on encryption at the end of the development process.

- Secured sensitive email communications in all forms: An email encryption platform that accommodates multiple use cases ensures that organizations can secure their email communication for internal and external communications and for senders and recipients that may not understand why they need encryption or how to use email encryption.

- Rapid implementation of protection: The need to encrypt email is paramount, as organizations are routinely sending sensitive and critical data in clear text. Fast and easy deployment of email encryption limits the potential damage should unencrypted data become exposed. And, as technical teams that deploy the encryption platform build knowledge and expertise, each subsequent project involving the platform goes faster. The result: accelerating the organization's efforts to secure data in more email messages in more business processes.

- Support for evolving compliance requirements and governance demands: Deploying an email encryption platform that quickly adapts to changing compliance requirements by updating existing encryption processes simplifies maintaining compliance.

Key Features Necessary for an Effective Email Encryption Solution

An organization that uses an email encryption platform that is flexible enough for multiple use cases is less likely to hesitate before deploying innovative new business processes that rely on email. But the chosen solution should include several other key features and functionality.

One essential feature is strong encryption protection for messages both on the server and in the user's inbox. Another is encryption that is applied to both inbound and outbound messages, with push and pull encryption options. The encryption solution must also work with common standards such as Transport Layer Security (TLS), PGP, S/MIME, or PDF. And the platform should support numerous options for authentication, including user-created authentication and platform-provided authentication.

An effective email encryption platform provides seamless encryption and is simple to use. Users need to be able to send and receive encrypted email without installing new software or downloading additional tools. The type of device being used should not matter, and multiple methods of encryption delivery should be available so that users can choose the one that best suits their current needs. Ease of use demands that those methods of delivery be accessible from the message itself.

An important capability for email encryption platforms is close integration with key on-premises email platforms such as Microsoft Exchange, plus cloud-based email platforms such as Google Workspace and Microsoft 365. In addition, the platform must support a consistent set of policies across various use cases for better security. Another feature to look for is a secure self-service cloud-based portal where users can register, retrieve, and respond to encrypted emails, eliminating the need for admins to create user accounts.

To effectively meet compliance, security, and governance requirements, the email encryption platform must have a policy engine that defines how messages will be encrypted based on key message attributes such as keywords, message content, and sender or recipient location. Another feature to aid compliance and governance is full message logging and tracking, aiding auditing and forensic investigations.

The Echoworx Email Encryption Platform

The Echoworx Email Encryption Platform delivers a secure, easy-to-use, and flexible solution for securing an organization's email communications internally and externally, whether outgoing or incoming, and across different business processes. Echoworx designed the platform to meet the demands of executive management, risk and compliance officers, developers, SecOps teams, IT teams, line-of-business management, and customers. Echoworx delivers a comprehensive set of critical features and capabilities that can streamline email-based business processes that incorporate confidential information.

The flexibility of the Echoworx platform supports a plethora of use cases that require encrypting email messages. For example, the platform supports eight separate delivery methods: web portal, S/MIME, PGP, PDF, PDF attachment, Office file attachment, ZIP attachment, and TLS with fallback. The flexibility in delivery choices provides more control over how messages are sent and received, ensuring that Echoworx can secure most email communication workflows.

In addition, Echoworx offers seven authentication options, which can be easily configured based on policies or the preferences of the sender or recipient, including OAuth-vetted social connectors, self-registration, shared-secret passphrases, single sign-on (SSO), system-generated verification codes, passwordless authentication that leverages a user device's existing biometric technology, and multifactor authentication.

The Echoworx Email Encryption Platform also offers comprehensive message tracking, providing detailed information about delivery, an email's opening by the recipient, message recalls, and notifications about any errors or exceptions. Such extensive tracking provides full visibility, helps in maintaining compliance, and gives more control to senders.

Echoworx enables the seamless migration of PGP and S/MIME encryption to the cloud by integrating all PGP or S/MIME activity, including auto key generation, digital signing, and signature verification in one fully managed platform. This enables organizations to leverage the scalability, reliability, and economics of cloud-delivered solutions while eliminating on-premises costs, reducing workarounds, and consolidating message encryption on a single platform.

Other compelling benefits of the Echoworx Email Encryption Platform include support for 27 languages, multiple branding options for email messages and secure portals, and access via any device, anywhere.

The Bigger Truth

Organizations will continue to rely on email for most communications, including messages that contain sensitive information, for the foreseeable future. More organizations are realizing that all such sensitive information needs to be encrypted to meet data security, legal, compliance, and governance requirements, as well as the expectations of customers. And the number of digital business processes that leverage email to communicate sensitive information is increasing. In this complex environment, organizations need a single platform that flexibly supports email message encryption for multiple use cases.

The Echoworx Email Encryption Platform provides an agile and secure solution for protecting information while eliminating complexity for users and providing numerous options for message delivery, authentication, and branding. Organizations looking for a solution that delivers email encryption for a multitude of use cases, rapid and simple deployment, and an easy-to-use customer experience that demonstrates the organizations' efforts to protect sensitive information may want to learn more about how Echoworx can help.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Enterprise Strategy Group by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188