DATA WORTH PROTECTING

As we enter an era of zero-trust, organizations are more mindful of securing their data and privacy. Given the severity of major breaches across the world, there is a need among organizations to assert stricter control over their data.

Many of the major security lapses occur over email and, in the first half of 2019 alone, there were over 4.1 billion records that had been compromised as a result of breaches. Around 70% of these breaches constituted emails alone.

These attacks also come at a serious cost to an organization, where average losses can be up to $4 million per breach and is expected to cost businesses over $5 trillion in total by 2024.

Despite incurring great losses, why do organizations fail to use email encryption strategies to defend themselves against harmful breaches?

Having reflected on over 2 decades of privacy and data security attitudes, Echoworx has highlighted the clear and present need for collaborative email data encryption. As early as 2004, it was noted in a study for Echoworx that 68% had concerns about email privacy. This resulted in a seachange in attitudes towards email encryption where, in 2004, 46% of organizations had an email data encryption strategy. In 2016, that figure increased to 63%.

It's now 2020 and we wanted to know just how mindful IT leaders are of the importance of a collaborative email data protection strategy.

In collaboration with Pulse, we put this question to 100 IT executives from North America and Europe. Read on to find out more of what your peers understand about the importance of email data encryption.

BREAKDOWN ON RESPONDENTS

ZERO TRUST MINDSET TODAY

13% of organizations polled were either unsure or did not have secure data encryption as part of their strategy.

What do you currently define as valuable information for your encryption strategy?

Though respondents consider Company and Third Party data valuable information, they also believe Security and IT have the most valuable information in the company. However, other departments such as Product, Marketing, Finance, HR and R&D are also vulnerable to breaches through their use of documents, files and spreadsheets via email.

Security, IT and engineering were seen as the departments with the most valuable data within the organization.

Meanwhile, the product team, HR, Marketing, R&D and Finance were lower ranked when it came to important data.

> "When asked who gets advanced access for email encryption within the company, respondents largely said this access was reserved for the **"leadership"**, **"senior executives"** and that it was **"based on hierarchy"**.

How was this decided?

ALL IN THIS TOGETHER?

93%

of IT leaders described their email encryption strategy as being either "very collaborative" or "somewhat collaborative".

However, despite describing their email encryption strategy as collaborative, in reality, organizations had left much of the buying and decision making power to the CIO and CTO.

Percentage of respondents who chose the role most important in encryption purchasing decisions.

As to how these buying decisions get made, 59% said there was a dedicated team that looked into email data protection requirements

9%

whereas another 9% said it was made by the top executives.

31%

Only 31% of IT leaders said that this was a decision across several departments.

Moreover, over half (54%) of IT leaders say that these decisions are made by a single team, rather than across multiple teams.

A QUESTION OF TIMING

Purchasing a tool is a major decision for many organization with contracts often exceeding millions of dollars. However, when vetting for the perfect tool that fits their business, 40% take between 1-2 months to come to this decision. Another 34% take 3-4 months to settle on an email encryption tool.

What are the key factors that determine whether a tool meets the needs of a business?

Cost-effectiveness was mentioned over twice as much as other factors when purchasing a new tool. Interestingly, 40% of respondents said they take less than 6 months to purchase a new tool but 36% mentioned cost as a key factor to the business needs. It seems surprising that up to four months of deliberation on a new encryption tool would eventually be decided on costs.

Conclusion

When protecting a company's assets, most in the industry are in agreement that more needs to be done to improve email security. Yet, according to the data within this study, a change in mindset is required to drive a collaborative approach to address the gaps often found in email data encryption strategies.

Security and risk management leaders responsible for email security should:

- Ensure that email security purchasing decisions are balanced between the requirements of the business and the requirements of the security team.
- Collaborate with business leaders to define and prioritize the business needs for email data encryption and score solutions based on critical capabilities.
- Protect valuable email data person-to-person, business-to-consumer or system-to-person with access to encryption

To find out more about protecting email data with encryption, collaborate with Echoworx to help build a trusted path to secure communication.