BIZCOMMUNITY

Managing risk: Why email archiving is critical

By Yossi Hasson

4 Nov 2014

In a fast moving and rapidly evolving business environment, which is undergoing a transformative shift to digital communications - it is increasingly important for businesses to protect themselves against legal, financial, and reputational risks.

Many of these risks will come in the form of existing and new legislation, as regulators and lawmakers strive to keep pace with innovations and developments linked to the use of digital platforms and new data storage capabilities.

One powerful and particularly important example of legislation impacting business practices can be found in the way companies are being required to store and archive emails. Email archiving is the process of capturing, preserving, and making easily searchable all email traffic to and from an organisation. Email archiving solutions capture email content either directly from the email server itself (labelled journaling) or during message transit. The email archive can then be stored on magnetic tape, disk arrays, or more commonly these days, in the cloud.

Legal data records

Few could argue that email has become an essential business tool, yet many companies still fail to recognise that like other information they possess and generate, it requires proper storage and management. Unsurprisingly, digital records are now regarded as functional and legal data records, which means that proficient storage and retention methods must be put in place to secure and accommodate electronic communications.

One of the primary reasons for the increasing calls for digital information to be securely stored and retained is for evidentiary purposes. Sections 14 and 15 of the Electronic Communications and Transactions Act, for example, touch on the originality, admissibility and evidential weight of data messages, respectively.

Currently, the standard practice in South Africa is to retain email for three years. There are some exceptions to this rule, such as under the Companies Act, whereby electronic documents may have to be retained for up to seven years. Under the VAT Act, for example, electronically generated tax invoices need to be stored for five years or more. (The Value-Added Tax Act, No 89 of 1991 (VAT Act) requires that an invoice be presented as a 'document'. With regards to the provisions of the ECT Act, a 'document' includes a data message and sending an invoice in electronic form will be acceptable for purposes of the VAT Act, subject to certain requirements - such as storage - being met.

Corporate governance

It is also important for businesses to be aware of the fact that the King Report on Corporate Governance for South Africa states that directors are responsible for risk management and - specifically with regards to IT - that they have a responsibility to ensure that an effective internal control system is in place.

This underscores the point that electronic document management should be a top priority not just for CIOs and IT departments, but also for executive leaders. Failing to prioritise document management - which naturally includes email and proper email archiving - can put directors at risk of heavy penalties and even, in some cases, imprisonment.

Stuck in history

For most companies, relying on existing, and in many respects, outdated methods of managing their email, is risky business. Current and impending legislation, which is likely to get even tougher on electronic document management, calls for companies to explore various email archiving solutions. When deciding on the right solution, businesses need to make sure that it complies with the requirements of the Electronic Communications and Transactions Act and associated laws/legal frameworks.*

In short, it is critical to remain compliant and up to date with regards to the retention and storage of all electronic communication - not only from a legal and financial perspective, but also from a purely reputational viewpoint. With effective email archiving, for example, businesses can respond quickly and decisively in the event of complaints against them. Moreover, efficient digital record keeping enables a business to run all the more smoothly, responding to both internal and external requests with ease.

The below checklist provides guidance on this:

- Emails must be captured and stored in their final form and must be capable of being displayed or presented in this form
- Emails must not be altered in any way
- The form in which the emails are stored must allow for them to be viewed to accurately showcase the information generated, sent or received in final form
- The email archival service must be able to verify and track the lifespan of stored emails as well as any actions taken which may affect the stored emails or their storage environment
- Information about the email origin must be ascertainable, retained and associated with the emails themselves either in a manner that is consistent with their final form or in a manner that does not undermine the email integrity
- Emails must be retained in such a manner that the information is accessible
- The email archival infrastructure must be subject to regular and verifiable checks in order to ensure integrity and proper functioning
- Emails must be capable of being extracted from their storage environment in a nondestructive manner to preserve the information extracted as evidence as well as the stored versions' and copies' integrity
- Emails that are extracted from their storage environment for use as evidence should be capable of being verified as having been stored in a compliant archival infrastructure

ABOUT YOSSI HASSON

Yossi Hasson is the CEO of SYNAQ, leading provider cloud messaging and communication services for South African business.
- Managing risk: Why email archiving is critical - 4 Nov 2014

View my profile and articles...