Corporate data breaches and losses of data in both the public and private arenas show no signs of abating, so how can organisations control the rising tide of emails and consumerised devices without drowning? Terry Greer-King, UK MD, Check Point, has some of the answers.

According to popular legend, King Canute set his throne by the sea shore and commanded the tide to halt in order to demonstrate his powerlessness against the forces of nature. And faced with the ever-rising tide of data breaches, many senior IT staff will know the feeling.

In August 2012, the Information Commissioner’s Office (ICO) revealed that breaches had increased by a factor of 10 in the UK, in just five years. In local government, the increase was 1,609 per cent, and within the NHS 938 per cent. Of course, much of this increase has been because public sector organisations must now legally report breaches, but even so, the upward trend is worrying.

The majority of these reported breaches have resulted from lost or stolen laptops, storage devices or smartphones – a situation made worse by the bring your own device (BYOD) boom of the last three years. Employees are using their own laptops and smartphones to process work emails, store work-related files and more, meaning a hugely increased breach risk.

Accidents will happen

Then there’s an equally significant risk for accidental data loss: corporate email. Due to the sheer volume of emails sent by organisations from all devices on a daily basis, accidental data losses are almost inevitable. Common mistakes include inserting the wrong email address, attaching the wrong file and sending emails that contain sensitive and restricted data to the wrong recipient.

Between lost devices and email mistakes,
any member of an organisation has the potential to cause a data breach in just a matter of seconds. Staff often fail to realise what they have done until it’s too late, by which time the damage is done. So how can organisations prevent these losses from happening and protect against those simple human errors of misplacing a device or mis-keying an email address?

I believe a two-stage solution is needed: one that both educates users about their actions in real-time, and also enforces security without the user being able to tamper with it or turn security off.

Let’s look first at how email data breaches can be curbed; then at how data in documents can be protected to add a further layer of security, irrespective of the medium or device on which the document is being sent or processed.

Boiling the ocean

Traditional data loss prevention (DLP) solutions have tried to address the email issue, but with limited success. They usually take a long time to set up, as weeks or even months of intensive ‘training’ is needed to help the solution in classifying data and files that are unique to each organisation. What’s more, emails that the system identifies as a potential data-breach risk are usually flagged to the IT department, which then has to check with the email sender before either allowing or blocking the email.

Both of these factors mean a significant drain on IT staff resources. When combined with the volume of outgoing emails in any organisation, the traditional approach to DLP quickly becomes unworkable when trying to identify the one or two rogue emails. It’s the equivalent of trying to boil the ocean to find enemy submarines.

A different approach is needed – one that doesn’t rely on the extensive ‘training’ demanded by a purely artificial intelligence-based solution, and one that doesn’t require constant intervention by IT staff.

Prevention is the cure

Involving individual employees in the corporate security process is the only viable approach to avoid data loss incidents. It is also the only way to turn a DLP solution into a truly preventative tool – as opposed to a reactive tool.

First, in order to increase the user awareness, an effective DLP solution will alert the user before they can send an email that may cause a loss incident.

Let’s take the scenario of an employee who has composed an email, addressed it and clicked on the ‘send’ button. The DLP solution should analyse the body of the email, complete with its attachments and the intended recipient’s address, against a set of predefined characteristics to identify potentially sensitive data. This could include, for example, certain key words in the email body text such as ‘financial’, ‘report’, ‘specifications’, ‘confidential’ and so on. Also, file types such as spreadsheets or presentations with financial data, confidential records or strategic material may need to be carefully scrutinised.

If the DLP solution detects a potential breach based on this analysis, it will override the ‘send’ instruction and present the user with a pop-up alert to inform them of the potential data loss and ask how they wish to proceed.

The user will have to decide whether they: a) want to send the email and its attachments as it stands; or b) realise that they have made a mistake, correct the body text or remove the suspicious attachments. There should also be the option for the user to leave a brief explanation as to why they overrode the DLP solution’s alert.

Users choose

The DLP solution keeps records of all of the user’s actions, of the fact that they were alerted, as well as the justification they provided, giving an audit trail for subsequent analysis. This establishes a clear chain of events when reviewing a data-loss incident, which is useful for internal review and external compliance purposes.

It also creates a decision point for the user, encouraging them to review what they plan to send and to whom. This increases users’ responsibility and helps to correct any potential security issues before an incident happens. Furthermore, engaging the users in the DLP process will reduce the burden of day-to-day security management from IT staff.

For your eyes only

This approach goes a long way towards addressing email data breaches. But an email with attached documents or files containing sensitive data could still be accidentally sent to the wrong party. And of course, there’s the issue of securing data in the actual documents once they leave the corporate network.

While applying encryption to an entire device is one approach to protecting data, it’s not always practical or even possible – especially on a user’s personal laptop or smartphone. Also, even sensitive documents quickly become scattered across email inboxes (often replicated on smartphones, too), on laptops, in webmail or other cloud apps, and on removable storage. This multiplies the chances of an unsecured document going astray.

Traditional document security has meant password protection: but that offers almost no defence to freely available online tools that are designed to crack file passwords.

What’s needed instead is a method of securing the file using strong encryption, together with a method for granting access to those files based on user permissions. This would enable documents in a variety of formats (Excel spreadsheets, Word, PowerPoint and Acrobat files, and others) to be created and secured, with different rights assigned to different users or groups of users. A basic default would be to ensure documents can only be read by authorised employees.

Users can then access or view documents when they have the relevant permissions, which are set by the author or organisation. For example, only HR or finance personnel may be able to access and edit certain documents, with their credentials being assured by the use of the correct client on their device, together with username and password.

Documents could also be shared outside the organisation, with certain restrictions on usage, and viewed either in the cloud (after the user has accessed the cloud service using the relevant credentials) or with the use of a secure client on the user’s PC or device.

This two-stage approach to managing data and preventing losses closes off the most common data breach vectors. With data watchdogs becoming increasingly vigilant and forceful in applying sanctions to those organisations that have suffered breaches, it may be time for all businesses – especially those holding customer data – to consider the value of a DLP solution within their organisation. After all, prevention is always better – and far cheaper – than a cure.

www.checkpoint.com