ALTERNATIVE
SOLUTIONS

## Data Security in Trust Companies

For many years we have advised our clients on the need for data security to protect the assets of the company. There are risks to data inside the office and the danger of data loss only increases if employees are permitted to take data outside the office on devices such as memory sticks, smart phones, tablets and laptops. There is also a risk to data when a member of staff leaves the organisation as they could potentially take sensitive information with them. Loss of data can lead to severe commercial problems if that sensitive data ends up in the wrong hands and it could also result in significant fines.

There is a new focus to data security as regulators insist on securing data not just to protect the individual or company but the whole jurisdiction. Here we consider just some of the areas where an organisation should consider its security arrangements.

- **If you don't need to see it, you should not be able to see it**

  This sounds simple to achieve, but preventing unauthorised people seeing information can be difficult.

  In a traditional paper office environment files can be locked away in cabinets (although they are often held in open filing racks). The vast majority of documents are created electronically, however, so even if the final printed paper document is secured what happens to the electronic copy?

  In most organisations, documents are stored in folders on file servers. Preventing access to a particular folder is relatively easy but that means all the documents in that folder are restricted. It is possible to apply security to individual files but, in practical terms, it isn't a feasible option and so a user that has access to a folder will normally have access to all files and sub-folders.

  The solution is to implement systems that allow security to be applied to individual documents, preferably with default settings so the possibility for human error is at least reduced if not completely removed. Individuals will then only see the documents that they are permitted to see and all activity can be monitored through an audit trail.

- **Who has done what?**

  A question we are often asked when a member of staff leaves is "what did they access prior to leaving". Standard systems don't record this information. In general terms if a user can see a file then they can read and print the information without any history being recorded.

  With a reasonable system in place, a complete history of all actions will be recorded in an audit trail. Actions recorded will include who has viewed, opened, printed and even emailed a document. With a complete audit trail it is then a simple task to report on exactly what information a member of staff has seen and also what they have done.

- **Taking data out of the office**

  USB drives are a convenient way to transport data when out of the office. Their small physical size and massive capacity makes it easy for staff to carry large amounts of information to meetings and deliver presentations without the need to carry a laptop computer. Their small size also makes them very easy to lose!

ALTERNATIVE
SOLUTIONS

All data that is removed from the office should be protected by strong encryption and passwords. Ideally there should also be ways to manage the device remotely, resetting passwords if forgotten and remotely "killing" devices if they are lost.

- **Mobile devices**

Travelling executives and home workers expect to be able to perform the same tasks away from the office as when they are at their desk. There is also a growing trend for Bring Your Own Devices (BYOD) where staff use their own mobile equipment to carry out work tasks.

By their nature mobile devices are a high risk and some technology provides higher levels of security than others. Devices need to be secured and remote access to systems controlled to minimise the risk of compromising data. If a device is lost or stolen it is important to know that the information held on it is secure and preferably that it can be destroyed.

- **The dangers of email**

Email is the default method for quick and efficient communication with colleagues and clients. There are a number of inherent dangers with email that need to be considered. Email is normally sent unencrypted, meaning there is always the possibility that it can be intercepted and read. There is also a very real danger that emails are sent to the wrong person. It is very easy to start typing someone's name and the 'auto fill' feature completes the address. Without thinking about it we have sent confidential information to the wrong person.

As soon as information leaves our environment it can be copied and distributed, we lose control and cannot prevent a recipient sending the email on to another party.

Systems are available to encrypt and remotely manage email allowing us to maintain complete control. Emails cannot be intercepted, emails sent in error can be properly stopped so the recipient cannot read them and forwarded emails can also be controlled.

## Conclusion

Not every security risk has been covered in this short briefing, these are just some of the important issues that are pertinent to local trust companies. 100% security is not possible, but it is important for regulated companies to understand the risks of data loss and have suitable policies and systems in place to reduce that risk to an acceptable level. This is required not just for the protection of the individual company but also for regulation and for the protection of the jurisdiction.

## About the author

Tim Roussel has worked in the information management industry for over 20 years. He has experience of working with public bodies and commercial organisations across the UK and EMEA. He has been working for Alternative Solutions Limited for the past two and a half years, advising and assisting a variety of organisations on improving business processes with a specific interest in managing information. Tim can be contacted on 01481 701234, 07781 140353 or by email tim@asl.gg.