Tackling company data leakage

Companies are at constant risk of leaking highly-sensitive company information, which could result in them being slapped with a £500,000 fine. Here, **Boyd Butler** explains how to maximise your controls.

Since the invention of the floppy disk, data leakage has been the stuff of nightmares for IT security personnel. As Daniel Berke reported recently in *The Negotiator* (April 16), there's now tough new legislation that allows the Information Commissioner Christopher Graham to issue fines of up to £500,000 fine for breaches of the Data Protection Act, so it's worth looking at these issues in more detail to understand exactly how to protect yourself against such fines.

Boyd Butler is an independent marketing consultant

Type

Securing customer data should be the number one priority for any business. Without customers a business would fail. Securing customer data keeps customers happy, so keep them updated about the steps you take to secure their data.

It is equally vital to the success of a business to protect the interests of its employees. Most companies have detailed personal information about employees, such as social security numbers, addresses, telephone numbers, and employment records, which should be treated with the same case as client data is.

Finally, there is company information to consider, which includes financial, sales and marketing information, which in the wrong hands could prove disastrous.

Leakage

Data can leak from many places. USB sticks, laptops, printers, documents in shared network drivers and of course, email, are the key high risk areas that should be kept secure at all times.

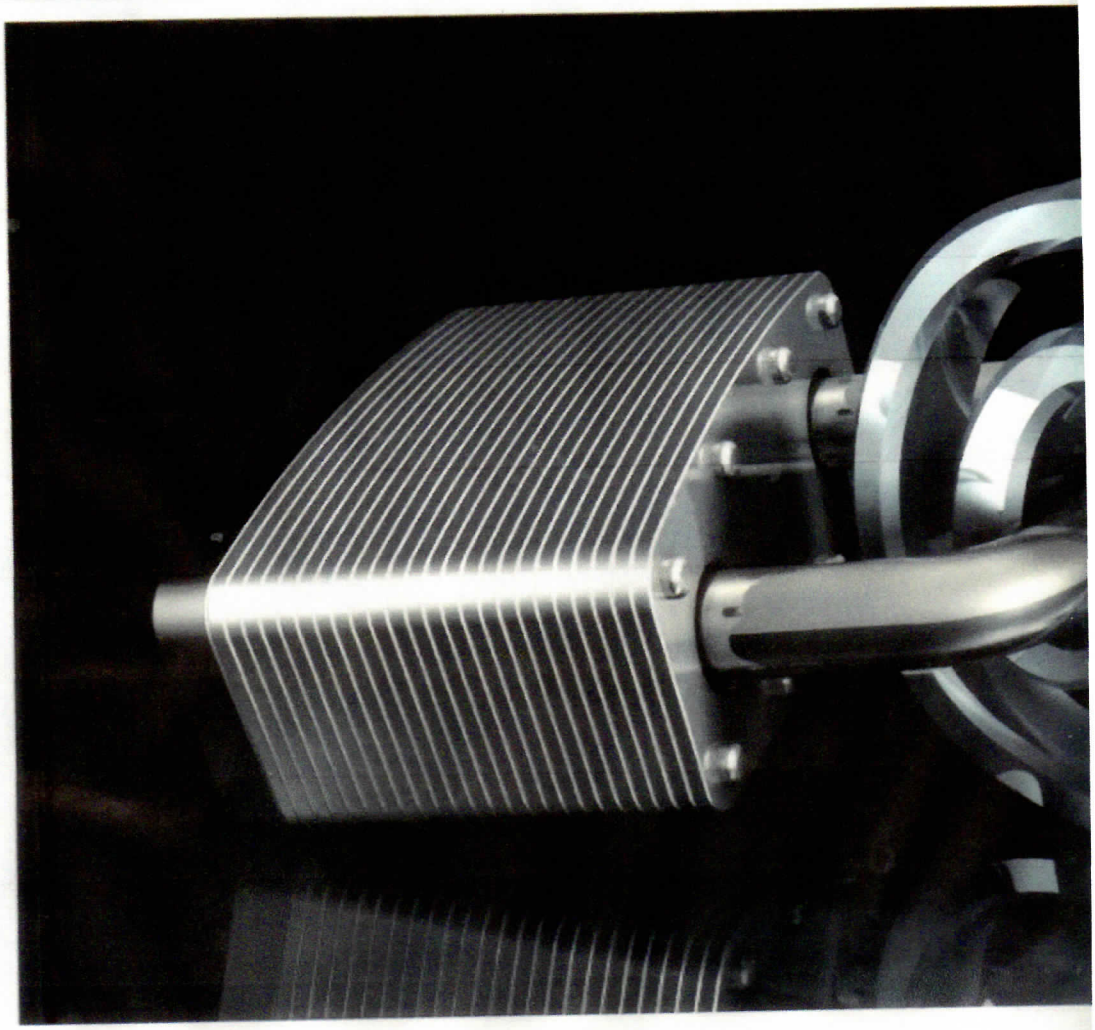
It's very likely that highly-sensitive company information is leaving your office insecurely on a daily basis through email. It's the biggest business tool and the one that gets most overlooked as a risk factor.

People assume wrongly that email is secure. But email can easily be intercepted and as we all know, it can be sent easily to the wrong person by mistake. Nevertheless, there are simple and inexpensive ways of encrypting email, which will allow you to send messages securely and confidentially.

Encryption

Encryption is a process of converti plain text into an unintelligible form using a set of procedures and algorithms. A key is then used by t recipient to decipher the code.

The use of encryption/decryption is as old as the art of communication. The Ancient Egyptians used encryption to



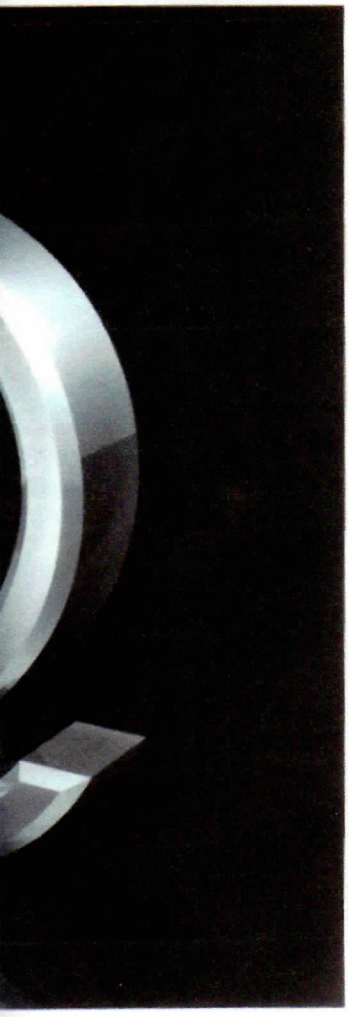
securely communicate with each other in wartime.

As Jim Everett, UK director of Global Security firm Echoworx notes, encryption is a highly flexible tool.

"Encryption services take many forms. But all are designed to keep data secure. For example, an independent agent might want a simple click of a button service, which means email never travels unencrypted. This is known as encrypted mail.

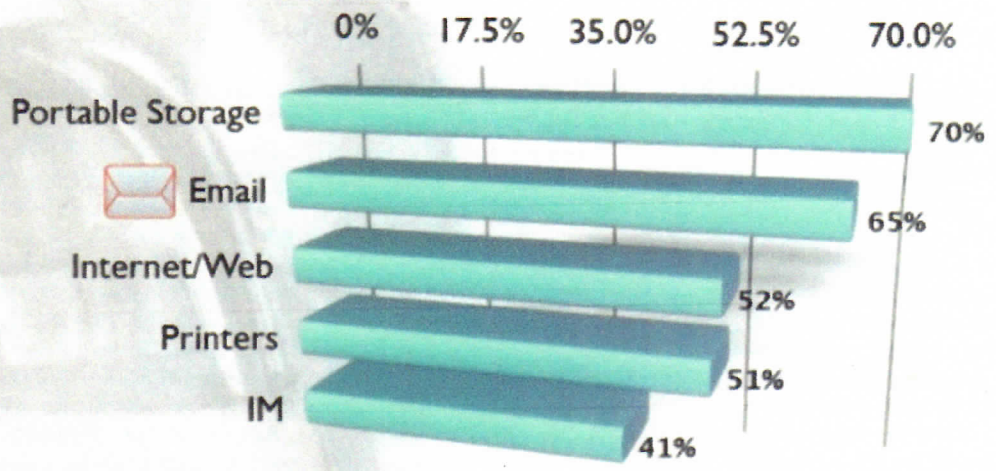
"A larger chain of agents or a franchise group may install a solution that will automatically encrypts emails, based on certain rules or policies set up at the administrator or company level. This is what's known as an encrypted mail gateway."

But solutions must be based on the specific needs of a business.



Why Encrypt Email?

The most common channels of data leakage



Source: DSPC technical study guide

Here, Stephanie Pritchett, solicitor and principal of the specialist data protection and privacy law firm Pritchetts, explains what agents need to do to ensure their data is secure.

1. **Review your data compliance** in light of the increased risks of a £500,000 penalty for breach of the Data Protection Act.

2. **Elevate data protection** up the corporate compliance agenda. It's a director-level thing, and half and million pounds looks even bigger when it's leaving your business.

3. **Undertake a health check** on your data protection policies and procedures; website and client facing privacy policies; data collection forms; internal data protection policies; monitoring; communications; data retention and data destruction policies; and outsourcing procedures. Ensure they comprehensively cover all data processing activities.

4. **Review the Information Commissioner Office notification.** Many people rely on ICO templates and renew their notification without making any relevant changes. Failure to notify new data processing activities within 28 days is a criminal offence.

5. **Implement a robust access request procedure** – failure to fully comply with requests for information from individuals is the top reason for complaints to the ICO.

6. **Review your marketing team's practices** to ensure they are compliant with the Act and the Privacy Regulations via appropriate use of customer databases, opt-ins, opt-outs and unsubscribe requests.

7. **Review all third party contracts** involving firms who are processing data for you in writing. They must contain the required data protection clauses.

8. **Formulate a policy** for data security and security breach.

9. **Review CCTV policies** to ensure that any necessary signage is compliant.

10. **Undertake staff data protection awareness training** and stay abreast of legal developments.

While data security may not be a sexy subject, no agent can afford the headache of sorting out a data leakage problem. It's time-consuming, expensive and potentially ruinous. Far better to put the right technology and policies in place and make it a key selling point when talking to clients.