



**Paul Judd, Regional Director for
UK and Ireland, Fortinet (www.fortinet.com)**

Everyone will remember 2007 as the year when masses of valuable information was lost; causing uproar amongst the public, government and private sectors. As data is now generally considered the most valuable asset that a business can hold and therefore, potentially lose; precautionary measures must be evaluated and strengthened on a continual basis to eliminate unnecessary risk.

Data loss and identity theft are crimes that we all fear and thanks to the Internet, criminals aren't forced to rummage through office waste to garner the critical information needed to perpetrate it. Cyber criminals are constantly on the lookout for valuable corporate data and if efficient IT security isn't in place, the damage caused to a business, its reputation and its customers can be unprecedented. Recent high-scale public data breaches have made us all more aware of this imposing threat, but how easy is it to put vigilance into practice?

The infamous HMRC data breach demonstrated the extent of disruption that can be caused when the very basics are overlooked. No vicious attack or crafty criminals were involved in this case; the guilty culprits were simply ignorance and carelessness. The fact is, that human beings can make human mistakes - but if an effective IT security solution is in place, the consequences of these mistakes can be minor and often removed from the equation completely.

As quickly and easily as human beings can make mistakes, they can assume responsibility for them. All accountability for the success or decline of a business' IT strategy is placed with the IT department and it is within its remit to take simple steps to ensure risks are kept to a minimum. Criminals aren't loitering around government buildings, waiting for valuable discs or USBs to be misplaced; instead they are utilising a far easier method of exploiting corporate networks -cybercrime.

Ensuring that all highly sensitive data is encrypted is a sure fire way of avoiding any major mishaps like those we have witnessed of late, however introducing other simple measures such as user profiling, segregating your network and password protection can

ensure data is accessed only by those who should, and can be just as effective.

All in all, the key to tighter security - and this extends into the types of IT solution you must select to protect your staff, customers and data - is intelligence. Rather than extravagant spending on hundreds of costly security systems, it is all about understanding the threat and your enemy. Implementing a carefully thought out security strategy that unifies and integrates security elements such as Anti-Virus, Firewall, Content Filtering, IPS and Anti-Spam is the easiest and most effective way of protecting your information as it is secured from every avenue of cyber attack.

Corporate networks are getting more complex and excess data and users are introducing additional avenues of attack for enterprises to contend with. New social networking sites and communication tools such as Facebook, MySpace, blogging sites and IM, are adding a new dimension of risk for today's business. Sophisticated and wrapped with an air of mystery, these new applications provide quick, popular and easy methods for user interaction and provide new forums for criminals to exploit in order to gain easy access to desired information.

In turning to a consolidated approach to security, businesses can eliminate the risk of their data falling into the wrong hands. Strategic investments in multi-threat systems mean that businesses avoid the management strain of implementing, updating and maintaining numerous security devices and, by having all security components on one powerful platform (in whatever combination is needed), a business can be protected against, and manage its protection against, theft, damage and corruption.

With increasing speculation that US-style laws will soon be introduced to the UK, making it compulsory for companies to publicly disclose any instances of data breaches, businesses may well be forced to suffer the humiliation of publicising its own weaknesses. Whilst this shouldn't be the only driver, it is clear that businesses need to take action and prepare for the unexpected, before it's too late.