

Secure in the knowledge

As 'tellings-off' go, the explosive chiding about data protection recently meted out by Richard Thomas, the information commissioner, is right up there with the most impassioned. Fortinet's UK director Paul Judd outlines the challenges for data security

Quoting an eye-watering litany of real-world public sector shortcomings, information commissioner Richard Thomas drew a picture of reckless and feckless personal information usage that had reached unacceptably frequent levels. He called upon local authority and government department bosses to stop passing the buck to 'the IT boys' and take responsibility for delivering improvements, and he warned that – sooner or later – these hitherto employed inadequate approaches would start to cost lives. Concerned? He was absolutely livid...

The 'hairdryer' treatment clearly thawed

the legislative process, because weeks later Mr. Thomas and his colleagues at the Information Commissioner's Office were granted sweeping new powers to enforce the Data Protection Act. These allow the commissioner to enter government departments, health authorities, and local councils without warning to check databases. Anyone holding information on databases will also be required, upon a warrant being served, to hand it over to the commissioner. The power to fine is also being strengthened, with the level potentially able to reach millions of pounds in the worst cases.

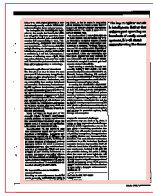
Fortinet understands that while criticising

the government sector might be a straightforward thing to do, locating solutions to the challenges they face is altogether more difficult.

Plenty of stick, but not enough carrots?

With increasing pressure to deliver significant data security improvements, the additional effects of the economic downturn mean that government spending on solutions is more heavily scrutinised than ever before. The answer is tighter security; tighter on the threats but also tighter on the pennies...

The key to tighter security is intelligence.



Rather than extravagant spending on hundreds of costly security systems, it is all about understanding the threat and your enemy.

The first application of intelligence ought to be by the people that handle the data. Assuming that they have your best interests at heart in the first place, ensuring they exercise full responsibility is vital. This means training, compliance and disciplinary procedures... but of course, that isn't enough. Limiting the damage that a single individual can ensue, whether accidentally or maliciously, is critical. This requires a mixture of enforcing access rights, clear separation of duties, and a cast-iron audit trail. These last few points mark a clear shift from policy and procedure to technology.

Protect the application and the network

The first place to start is where the user meets your IT infrastructure; the application. The most sensitive of applications is – as Mr. Thomas would contest – the database, and any vulnerability here needs to be isolated and remedied. For instance, Fortinet's new FortiDB appliance does just that; providing powerful automated processes that discover and assess risks across 30 databases at a time, supporting database administrators in their critical security responsibilities. FortiDB is also continually updated with the latest policies, threats and regulatory requirements via Fortinet's FortiGuard services, which are provided 24/7 by a global team of specialist security professionals.

These services also form part of the strength behind Fortinet's consolidated security platform, FortiGate. FortiGate enables organisations of all sizes to obtain the highest levels of security and application level control over networked traffic.

Consolidation via the FortiGate platform reduces the capital and operational expenses of purchasing, managing and maintaining a multitude of different solutions and provides a scalable, flexible path for future adoption of additional security functions without the need to purchase additional hardware. This enables reduced total cost of ownership (TCO) and preservation of your security investment. In addition, the ability to 'virtualise' all security functions onboard a scaleable hardware appliance allows organisations of all sizes to extend the benefits of IT virtualisation deep into their security infrastructures.

The impact of Moore's Law and more avenues of attack

One thing we can safely assume about information generally, is that there isn't going to be any less of it. We know that IT is becoming

faster, as the increases in processing speed foreseen by Moore in turn demand larger and higher capacity networking infrastructure. The result is more data to have to contend with.

We also know that IT networks are becoming more complex, and excess data and users are introducing additional avenues of attack. New social networking applications and tools such as Facebook, MySpace, blogging sites and IM, are adding a new dimension of risk for today's communication-dependent organisations. 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.

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.

In turning to a consolidated approach to security, organisations 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.

Prepare for tomorrow's challenges

Whichever way you look at it, when it comes to data protection the challenges faced by public organisations are on the rise. There is increasing speculation that US-style laws will soon be introduced to the UK, making it compulsory for organisations to publicly disclose any instances of data breaches. This would further undermine confidence in public institutions (and businesses) in the event they would be forced to suffer the humiliation of publicising their own weaknesses. Looking to the past and the probable future, the pattern seems clear that more and more legislation will come if solutions don't come first. Fortinet already supports a significant proportion of the UK government sector finding secure, comprehensive and cost effective solutions to meet today's demands and tomorrow's challenges. ●

Paul Judd, director, Fortinet (UK)
T: 0203 207 9029
www.fortinet.com

“The key to tighter security is intelligence. Rather than extravagant spending on hundreds of costly security systems, it is all about understanding the threat”