



Feature IT Security



Paul Judd



More s less ha

By Paul Judd, Regional Director, Fortinet

Fortinet is the pioneer and world's leading provider of Unified Threat communications and deliver the best security, performance and total

National and regional governments worldwide have found their network attacks. Traditional deep-packet inspection firewall and VPN technology government network, clearly lack the intelligence and capability to detect attacks emerging within the rapidly changing threat landscape.

Fortinet's FortiGate appliances provide complete security that fully in network and application-level protection capable of stopping today's n

With uniquely designed features, Fortinet delivers network security v command and control needed by all levels of government.

Years from now, everyone will still remember the horror of the HMRC data breach. Even if you weren't directly affected, your confidence in the UK's largest government department will probably be in tatters anyway.

The view that data confidentiality was largely of moral importance finally became antiquated. We witnessed 2007 as the year no one was left in any doubt as to the enormous monetary value of personal information, and that bad people can cause terrible damage if they obtain it.

The wheels of cultural change need a huge impetus to start turning, so an event of overwhelming magnitude was

always going to be required to create it. In the cold light of day, it's becoming increasingly clear that the HMRC breach has the capacity to change organisational approaches for the better. It may yet prove to have achieved more for the ongoing protection of critical data in public hands than any statute passed to date.

It is worth exploring the underlying reasons why the HMRC breach occurred and what its lasting effects will be. Moving forward, what lessons can be learned and how can future breaches be avoided through better practice and more resilient technical solutions?

Probable Cause

The HMRC data breach highlighted the scale of problems that can result when basic failures arise through basic eventualities being overlooked. There was no attack here; apparently ignorance rather than malice was the cause. In all the machinations of unsanctioned downloading, unencrypted CDs and confused chains of command, the value of the information at hand was simply not considered.

A significant fact in the case was that The National Audit Office requested only a subset of the information claimants to be made available, but to save time HMRC sent

the entire database. Time simply wasn't available. Data needed to flow quickly, and good practices that might consume time or cost money were never going to get in its way.

Personal Effects

The shockwaves have been profound. Every government institution in the land is now redoubling its efforts to prepare against the HMRC scenario, as well as the myriad of other stiffer threats to data security. The Information Commissioner's Office has apparently since been inundated by confessions and disclosures from public (and private) sector bodies reacting to the outcry of the



IT Security Feature

Speed, Haste

Management (UTM) security systems that enable secure business cost of ownership available.

orks under increased threat from today's more sophisticated cybergies, as deployed over the last several years in almost every tect and prevent application level, blended and content-based

egrates true 'best-of-breed' technologies to deliver comprehensive ost sophisticated attacks.

ith the necessary speed, mobility, performance, and integrated

HMRC case, and as many requests for advice and support.

Lessons will be learned, of course. If it can happen to a large government department, then it could happen to any of the thousands of smaller government bodies that hold customers' personal information. Like businesses, public sector organisations rely on their customers, and seek to take the right steps to safeguard trust and loyalty.

Perhaps it is inevitable that stronger UK laws will be brought in that require public and private sector organisations to disclose any data breaches, under pain of hefty fines and potential imprisonment of top executives. Similar legislation in the US is credited for

making data systems and processes among the most watertight in the world.

Evading Risks

The various technical solutions offered by 'experts' into preventing the HMRC breach before it arose are distracting away from the critical point at hand. If the HMRC breach never occurred because an administrator had used strong disk encryption, would that mean there was no problem to solve at the heart of government data protection policies? The point is larger than this. When HMRC's cultural ignorance of information's value collided with the relentless pressure of its day-to-day business processes,

the result was hastiness – a very human trait.

Take it as certainty that a group of individuals will occasionally do things that undermine data integrity, purposefully or otherwise. Security solutions are required to make sure that the consequences are minor when human beings make human mistakes.

Moreover, a successful security strategy must never threaten to be in conflict with the high-speed performance requirements of day-to-day business activity. However, it's hard to conceive that the pressures to reduce the time and financial cost associated with data processes will quieten in the face of new initiatives and protocols around security. Performance will be key, as will flexibility. More speed is relentlessly required, yet less haste...

A coherent security strategy is clearly favourable to kneejerk spending on piecemeal security infrastructures. These complex security infrastructures are the electronic equivalent of repetitive form-filling bureaucracy. Because there is a different solution available for every potential security breach on the market, the simplistic approach is to invest in each part of it and glue them all together. This is a mistake. Information that flows through a complicated security system will put immense pressure on network performance, leading organisations to either invest huge sums upgrading their underlying systems or else suffer the consequences of delay and failure.

On top of rising viruses, worms, bots and Trojan attacks, government organisations are contending with social engineering deception and traffic masquerading as legitimate applications on the network. Those choosing to layer their networks with standalone

firewalls, intrusion prevention devices, anti-virus and anti-spyware solutions in a desperate attempt to plug holes in the armoury are beginning to recognise it's a failed strategy. Piecemeal, reactive security solutions are giving way to strategically deployed, integrated multi-threat security systems. Instead of having to install, manage and maintain disparate devices, organisations can consolidate their security capabilities into a commonly managed appliance.

The best security solution isn't the largest, most expensive or widely distributed. After all, information is most secure when it is protected via an intelligent approach. Unifying security elements such as IPS, Anti-Virus, Firewall, Content Filtering and Anti-Spam dramatically reduces infrastructure complexity and deployment cost.

Using these functionalities in whatever combination is most appropriate - while also tracking users' file exchanges, IM/P2P traffic, emails and Internet sessions through a single, virtualised hardware platform – a government institution's data is protected against theft, damage, corruption and denial of service.

Amid the pressure-cooker of a large government department and the capacity constraints of an IT system, security protocols – vitally important as they are – still cannot be allowed to burden the speed and performance of business processes. Everything works perfectly when time isn't a concern, but that isn't a world any of us live in...

Paul Judd
Regional Director
Fortinet (UK) Limited
Quatro House, Frimley Road
Camberley, Surrey GU16 7ER
United Kingdom
Office:
+44 (0) 8707 353 666
Email: pjudd@fortinet.com
Web: www.fortinet.com