



# How far does the larger enterprise need dedicated solutions for Internet security?

While the House of Lords report discussed elsewhere in this edition focussed on Personal Internet security, there is a broad swathe of business activity which falls outside its scope.

Large IT companies are no less vulnerable to the vagaries of Internet-borne attack, but the nature of the target is sufficiently different to merit a separate analysis and an alternative approach.

As recent successful high-profile attacks on large company IT systems will confirm, companies and their data – customer data in particular - now need ever higher levels of protection if a PR and financial disaster is to be avoided.

The increasing criminalisation of hacking over the last 12 to 18 months or so, as witnessed by the rising involvement of organised gangs and potentially state sponsored espionage, is rapidly changing the face of IT security and the ability to manage that environment successfully.

Hackers are moving from 'sport' into that world of crime, where their expertise is being tapped through dedicated forums outside the control of Western enforcement agencies. Information on security flaws and exploits is either sold to the highest bidder or sold on a packaged and syndicated basis to all and sundry.

This criminal evolution of hacking is accelerating the rate at which malware and IT threats are developed and distributed. Serious thought is now going into malware at-

tacks and security flaw exploitation, with the result that simultaneous attacks involving multiple type of security breach are now becoming commonplace.

## Vendors expanding range of solutions

As a result of these changes, IT security vendors have started to expand their product range to help companies keep up with the latest security threats: UTM (Unified Threat Management) appliances are becoming ever more sophisticated and capable.

Traditionally, UTM appliances have been aimed at organisations with between 50 and 500 users, but the latest generation of UTM appliances are now being targeted at larger customers, catering for as many as 2,000 users and moving beyond their UTM origins.

Taking an alternative route, at least one high-end vendor is approaching the UTM market from the other side of coin by expanding its range of rack-based Unix and Linux appliances to create a UTM 'underlay' technology from which anti-malware software can be run on a virtualised basis.

This multi-operating system approach is clever as it anticipates the multi-vector nature of the predicted range of IT threats predicted during the next 12 to 24 months.

These threats, some of which are already making their presence felt, employ mechanisms such as Instant Messaging and Internet telephony as the 'host' for small pieces of malware (applets) which can then be loaded onto one of several executable code modules to achieve the criminal's aim of extracting a revenue stream from the targeted system.

## Taking the behavioural analysis approach

According to Peter Woollacott, CEO of behavioural analysis software specialist Tier-3, rather than remain captive to reactive response techniques, behavioural analysis can be used as the cornerstone upon which other IT security technologies can be layered and controlled. "This layering approach can, of course, be multi vendor-based, or it is possible to run a behavioural analysis system in parallel with a high-end UTM appliance to protect companies of more than 1,000 seats or more from both known and unknown threats."

## The increasing criminalisation of hacking over the last 12 to 18 months, as witnessed by the rising involvement of organised gangs and potentially state sponsored espionage, is rapidly changing the face of IT security

---

The importance of behavioural analysis systems is that they view threats from a totally different paradigm. Rather than identifying only threats, which can be predefined, and hence be vulnerable to anything unexpected, behavioural analysis technology enables unusual system, process or user activity to be identified instantly and its level of riskiness assessed.

As Woollacott observed, "Behavioural analysis would almost certainly have saved the reputation of a number of organisations in the last 12 months in situations where the companies concerned suffered high profile losses of customer information and lost both credibility and stockholder value as a result.

"Many of these instances of publicised system incursions are now the subject of lawsuits, as well as an investigation by a regulatory bodies on both sides of the Atlantic."

Initial indications suggest that the modus operandi of those involved in the hacking are quite sophisticated, but the resulting negative publicity is a clear warning to organisations of all sizes of the need to ensure that their security efforts are sufficient to protect them against a similar fate.

### Largest ever online bank heist

Security considerations impacted upon the reputation of one high profile European bank in January 2007, when an organised crime gang is reported to have committed a fraud costing the organisation \$1.1 million.

Peter Woollacott outlined the scenario. "In that scam, seen as probably the largest online attack on a bank, several hundred of its customers were sent a customised Trojan application that, once installed, triggered a key logging application whenever they accessed their bank account online. This data was then relayed across the Internet to a group of offshore servers, from where it was quickly used to withdraw money in relatively small amounts.

"Our observations on these - and other - thefts from previously highly protected enterprises is that cybercrime is now being driven by organised criminals who have the expertise to circumvent existing security efforts and gain easy access to an enterprise's most valuable assets."



# integrated threat management

IT security threats facing a modern organisation can now come from within, as well as without. Recent figures from the DBERR – the old DTI - show that more than half of the most serious threats affecting large organisations originated inside the organisation.

These criminals are increasingly using sophisticated techniques to circumvent existing security measures and extract assets of value from organisations and their partners without detection.

In almost all of these instances, had the victim organisation had a behavioural analysis system installed on its online banking systems, Wollacott believes, “the IT security staff would have been able to detect the scam at a much earlier stage and allow preventative measures to kick in and save the organisation – and its customers – significant sums of money.”

## Conventional IT security is no longer enough

These examples quoted, and the almost weekly revelation that another highly regarded enterprise has become the victim of cybercrime illustrate that conventional IT security technology on its own is no longer sufficient to protect an organisation's most precious assets, its customers and its reputation.

The need for improved security to protect an organisation's IT assets is becoming increasingly important. As the Tier 1 CEO noted, “IT security threats facing a modern organisation can now come from within, as well as without. Recent figures from the DBERR – the old DTI - show that more than half of the most serious threats affecting large organisations originated inside the organisation.”

That research found that two-thirds of large organisations suffered from staff misusing their systems, and that four out of ten were the victims of theft or fraud involving computers. Against this backdrop, the need for increased levels of vigilance against the growing range of multi-vectored attacks on IT system resources becomes ever more important. “IT managers must now be prepared to protect their organisation's IT assets from an increasingly disparate and wide-ranging number of threats, both known and unknown, using a combination of products and services from several vendors.”

## Protection against unknown threats

The best way of protecting against unknown threats is to augment an existing IT security solution from one or more of the major vendors with a behavioural analysis application. It is also preferable for these IT security applications to be managed using a single software dashboard for coordinated view and control. “As well as making the task of managing multiple IT security products from different vendors easier, the architecture helps prevent software conflicts or conflicting interpretations of risk from various free-standing security products.”

In practice, most IT security applications aimed at the enterprise end of the market have APIs (Application Programming Interfaces) to allow the various applications to communicate and even control each other.

## Holistic threat management

Accepting Peter Wollacott's argument, effective security management cannot be achieved by adding new specialist point solution technologies progressively into the solution mix. With an integrated approach, diverse point security solution outputs can be interpreted together with any unusual or unexpected activity and a comprehensive risk position of the enterprise made visible and manageable from a single point of control.

“This provides holistic threat management and removes the systemic risk associated with a mosaic of uncoordinated point-solutions. This trend is being driven, in part, by the recognition in many quarters that the use of multiple anti-virus and anti-malware engines can increase an organisation's IT security effectiveness towards the 100 per cent levels of protection that we all strive for.

“This can only be achieved, however, with the use of technology, which can detect and respond to all threats in the risk spectrum, and not just only those that are known.” §

