

What are the main security challenges facing enterprises today?

Anthony O'Mara, VP of sales and operations for Europe, Middle East and Africa at security software developer Trend Micro: Mobility is key to successful and effective working because people no longer need to go to an office to get their work done, but mobile internet devices are more vulnerable because they aren't protected by as many layers of the enterprise network security system. The chance of picking up malware increases outside of the company's network.

Paul Simmonds, chief information security officer at ICI and co-founder of the Jericho Forum, a group of CISOs from large enterprises: The change of working demanded by the business, with the emphasis of working outside your (secure) perimeter. This is everything from everyone having Web access, to banking via the Internet, mobile working, leveraging consumerisation, the closer (electronic) working with business partners, joint ventures, customers and so on.

Mark Sumner, chief security analyst at managed security service provider, MessageLabs: The convergence of virus and spam techniques was developed to overcome highly effective filtering systems that blocked delivery of most of the unsolicited email being sent to businesses. For the perpetrators, compromising systems by secretly planting Trojans, spyware and other intrusive software on individual PCs has become a relatively simple task. In fact, 'the bad guys' are now harnessing other communication platforms for their malicious benefit, such as attacks over instant messaging.

Natalya Kaspersky, CEO, security software developer Kaspersky Labs: We've seen the decline of the 'global epidemic', malware created to set off 'bells & whistles', cause downtime and data loss. Threats today are increasingly designed with financial gain in mind, crimeware designed to remain unnoticed, silently harvesting information and paving the way for more serious targeted attacks.

How can they address these challenges?

O'Mara: Firstly, install and update your security solution, including firewall, antivirus programmes and so on. Scan for spyware and other malware, install Windows updates, turn off file sharing, make regular backups of important data; disconnect your computer from the network or turn it off when not in use, don't open email attachments from unknown origin and don't run programmes of unknown origin.

Simmonds: Accept that the perimeter is dying (or dead) as a security boundary; it has increasingly less relevance as we continue to either punch holes in it, or just bypass it, so most enlightened enterprises today are actively planning for its demise in a few years time. Secondly, join the Jericho Forum, the owners of thought leadership in this area.

Sumner: Businesses need to adopt multi-layered defences against threats. Traditional enterprise desktop security software is no longer enough to protect them from the ever-evolving threat landscape. They need to keep threats away from desktop and stop risks "in the cloud" at the Internet level, which a managed service approach provides.

Kaspersky: 'Follow-me security' is important too. Solutions must be smart enough to defend staff wherever they work: at home, on the road or in the office. They must also be smart enough to protect any type of computer they may use, including mobile devices. It also means applying variable security settings depending on the employee's location and susceptibility to attack: e.g. if out of the office, update from the Internet instead of the LAN, apply stricter browser settings if not connected to the LAN, and so forth.

How different are the challenges facing small and medium-sized businesses (SMBs)?

Kaspersky: The nature of the threat is largely the same. However, SMBs seldom have the same resources and expertise to deal with the issues. For this reason, SMBs (a) more often make use of a security suite, rather than sourcing solutions from separate vendors and (b) rely on the expertise of third-parties to help them implement effective security.

O'Mara: SMBs usually have little or no IT support. 'All-in-one' solutions like our 'Worry-Free Security' automate nearly all the management processes involved, so they don't have to devote time and expertise to protect against all type of threats, and the loss of confidential information.

Simmonds: SMBs rarely have information security staff with time to think about these problems. Generally they will ride on the coat-tails of the larger enterprises as they demand changes to existing solutions or new products.

Sumner: Increasing sophistication and volume of threats, limited IT resources, and lack of security expertise. According to recent research compiled by MessageLabs, almost half of all small businesses are not providing adequate training regarding online threats, therefore employees are likely to be oblivious to the dangers to hand and need protecting by other means.

Stop the hackers

The range of viruses that can invade computer systems is constantly evolving – but so are the systems that can protect your systems

CASE STUDY: GFI

I was searching for solution to the potential dangers from the upsurge in popularity of the many various types of portable storage available on the market today. Active Directory has some functionality but is too inflexible and time consuming. GFI EndPointSecurity is a clear, simple and effective solution to the security issue.

The 30 day trial period was an excellent opportunity to fully trial the product on the various hardware configurations and personal requirements that our company has. I had no hesitation in purchasing the license and a two year support subscription.

Michael Hurworth
IT & Facilities Manager
Fair Trades

Computer viruses are what might be termed a mature industry, in that the first such program to make it out "into the wild," i.e. beyond the single computer on which it was created, dates from 1982. It went by the name of Elk Cloner and, interestingly, was written for Apple machines rather than PCs. Since then, of course, technology has evolved almost beyond recognition. Not only are the computers on people's desks today as powerful as ones that filled an entire, specially cooled room back then, but the speeds at which networks operate, the volumes of data that can be delivered and the amount that can be stored on a single desk or laptop machine have increased dramatically.

Powerful computers now sit on broadband networks, and while that means infinitely more potential for their legitimate use as business tools, it also opens up a whole new world of possibilities for hackers. Entire malicious programmes, called Trojans, can now be installed unobtrusively on a PC and, at a given signal, wake up and start causing havoc.

There is another important change too. The profile of hackers has gone from the geeky kid in his bedroom, who thinks it would be cool to break into the Pentagon's computers and thumb his nose at authority, to the full-blown cyber-criminal, seeking not fame but fortune, concealing his identity so as to strike again in future. The recent three-week onslaught on government, financial and media websites in Estonia, rendering them inactive and creating tens of millions of euros of damage and disruption to the country's economy, is a perfect example of how far we've come from Elk Cloner.

An emerging name in traditional anti-virus software is that of Kaspersky Labs, a Russian software developer that has gained a name for technical excellence while maintaining competitive prices. However, aware that the classic virus delivered via email is only one way malware writers are attacking nowadays, Kaspersky has expanded its offering to take in a broad gamut of security functions.

Its business portfolio is now called Kaspersky Open Space Security, it offers four levels of product, all of which include anti-virus, anti-spyware, anti-spam and firewall with intrusion detection/prevention (IDS/IPS) capabilities.

"Entire malicious programmes can be installed unobtrusively on a PC and, at a given signal, wake up and start causing havoc."

"The smallest is Kaspersky Work Space Security, which is for workstations," said David Emm, senior technology consultant for the developer in the UK. "Then come Business Space, which adds server security, Enterprise Space that adds mail server, and finally Total Space, which adds an Internet gateway for email traffic, protection for personal digital assistants (PDAs) like the iPAQ and the new mobile phone protection,

supporting the Symbian and Windows Mobile operating systems."

At the high end of the market, the speed with which attackers alter the profile of their assaults on corporate networks is such that it defies any time to codify them. To address that challenge, Australian software company Tier-3 was created in 1999 specifically to develop technology that would be able to analyse any data traversing a network without any rules, i.e. with no preconceived ideas as to what constituted malicious code. It launched its Huntsman product two years later.

"Huntsman is based on an entirely dynamic technology that uses heuristic algorithms," said Tier-3's CTO Geoff Sweeney. "We call it Behavioural Anomaly Detection." Heuristic scanning is a method which, instead of looking for specific "signatures," or predefined strings of code already identified as malicious, looks for certain instructions or commands within a programme that are not found in typical application programs.

As a result, it is able to detect potentially malicious functionality in new, previously unexamined traffic, such as the replication mechanism of a virus, the distribution routine of a worm or the payload of a Trojan. ►

COMMERCIAL FEATURE

Information Availability – the key to business survival

Information is the lifeblood of today's connected organisation, so make sure your continuity and availability plans really work, and fast.

Every aspect of what we do when we're at work depends on being connected to information and other people. Yet just as we are placing an unprecedented reliance on systems and the data they contain being available at all times, the threats that jeopardise them have never been greater (see A-Z of business interruption below).

It is sobering to consider that in the past couple of years UK plc has experienced such incidents as the July 7 bombings and the Buncefield explosions. Of course, these are the headline grabbing events, but as the statistics in the graph below demonstrate, it is the mundane that is much more likely to cause real headaches.

In today's connected enterprise, it is no longer enough for the IT department to take daily to weekly backups of files with tapes stored off-site somewhere. The complexity and pervasiveness of systems requires a much more sophisticated approach, in order to meet the degree of information that stakeholders now demand for key applications and processes.

Businesses everywhere need to keep people and data connected at all times. This need is what SunGard Availability Services refers to as Information Availability.

The key aspect of the concept is to ensure that information will always be available in as timely a fashion as it is needed, and it requires companies to think hard about each of their processes.

Assess the risk

Some parts of an organisation's operations are more mission-critical than others. Some services could go down for a day, and while it might be a nuisance, business could carry on. In others, such as a stock-trading office, every lost minute could cost millions.

Any business continuity programme therefore has to start with a proper business impact and risk review, looking at the importance of each and every process, and asking how long you could carry on without the system or network connection without serious consequences.

For each level of process, the business will set a recovery-time objective (RTO) – the time in which they would like to see the service returned to full operation – and Recovery Point Objective (RPO) – how recent the information restored needs to be – and then put in place plans that will help them achieve these goals.

The process of risk assessment and data profiling can also help to streamline an

organisation's business processes and data storage. SunGard assists its customers to profile and classify their data and provides storage solutions and consultancy to match their particular needs. Whatever technology a business uses, the same rule always applies – before you can determine what you'll need to store, you need to understand what you've got.

Electronic Vaulting

Even organisations that carry out regular tape backups, get the tapes to a safe off-site place, and also regularly test their recovery procedures to ensure the tapes can actually be read, are not immune to risk. Tapes can be damaged or lost en route, and in a recovery situation, the process of finding and getting back the tapes, and then loading them back on the system is onerous, long and error-prone.

Whilst having tape backup beats no backup at all, organisations reliant upon IT need to review whether it meets their needs today. SunGard's answer is to make good use of modern communications, and transmit backup data down the line to secure storage areas. This is called Electronic Vaulting, and it eliminates the many problems generally associated with tape backups. It puts to an end the inefficiencies and risks of tape backup.

Instead, daily backups are transmitted, either over the internet or via dedicated communications links, directly to disk in a resilient technology centre. The data is then automatically copied to a second geographically separate technology centre, giving true resilience.

Enhanced Recovery

System recoveries often fall foul of simple mistakes being made when re-loading the operating system. This can be very frustrating, and will delay the recovery process.

In order to ease the process, SunGard has introduced its Enhanced Recovery Service,

which is designed to help small and mid-sized companies avoid these problems. Its Standby*OS tool allows the affected server to be recovered remotely, and in tests comparing the Enhanced Recovery Service with standard recovery methodology, the process could be reduced by up to 10 hours – which gives back more than a working day!



SunGard also performs security analyses and penetration testing of network environments. Many organisations believe that they have a secure network since they have a firewall and antivirus software. However, most web applications now are connected to vital information systems such as databases and financial systems, making systems extremely vulnerable to security attack.

SunGard defines IT security as 'the right information to the right person at the right time'. It considers any computer system that does not fulfil these criteria a security risk. SunGard's security technicians monitor the same sources as real hackers to stay ahead of this threat.

When, not if, 'it' happens

SunGard has a network of 20 recovery centres around the UK, all of which are interconnected via the award-winning Ethernet-based SunGard National Network** and SunGard's high-bandwidth optical network ScaleNet delivering unparalleled resilience and connectivity for Information Availability; networking forms an essential part of disaster recovery,



vaulting and managed IT solutions. In May 2007, SunGard opened the latest addition to its portfolio of recovery centres in Elland, Yorkshire. (Representing an initial investment of £3.5m, the new centre provides 89,400 sq ft of Workplace Recovery and Tier-II data centre space. Within that space it offers over 360 Workplace Recovery positions, across six suites, and a conference room, four meeting rooms and two server rooms.

The centre – which features energy-efficient plant in support of business investment in low carbon technologies – is unrivalled in the locale in terms of its infrastructure and access to skilled support personnel. Further investment is earmarked to develop the site's capability and scalability including a dedicated suite, further data centre space and enhanced building infrastructure.)

Combined with a standardised voice and desktop infrastructure across all locations, SunGard has created a 'virtual' recovery campus which enables customers to 'rollback' to alternative recovery centres in the event of widespread invocation or in the instance that any one centre were to suffer

an attack of some kind. This ensures that organisations can continue to function, no matter how severe the disaster.

- Source: SunGard Availability Services Invocation Statistics
- ** Business Continuity Awards 2006 Most Innovative Product

About SunGard

Established in 1978, SunGard Availability Services is the pioneer and leading provider of Information Availability and disaster recovery solutions. SunGard customers include:

- Baillie Gifford.
- Great Ormond Street Hospital
- Irwin Mitchell
- James Galt Toys
- Northgate Information Solutions
- Sainsbury's.

An A-Z of business interruption*

Acts of God, air conditioning failure, arson, blackouts, blizzards, boiler explosion, bomb threats, bridge collapse, brownouts, chemical accidents, civil disobedience, communications failure, computer crime, corrosive materials, disgruntled employees, denial of service, earthquakes, embezzlement, explosions, extortion, falling objects, fires, floods, hardware crash, high winds, heat or cooling failure, hostage situations, human error, hurricanes, ice storms, interruption of public-infrastructure services, kidnapping, lightning strikes, malicious destruction, military operations, mismanagement, mud slides, personnel-non-availability, plane crashes, phishing, public demonstrations, quirky software, radiology accidents, railroad accidents, sabotage, sewage backups, snow storms, software failure, sprinkler breakdown, strikes, telephone problems, theft of data or computer time, thunderstorms, tornados, transportation problems, unexpected vandalism, viruses, water damage, worms, xenon gas leaks, yellow fever outbreak, zombie, attack of the (yes, that really is a hacker attack).

