

# Information security

An independent report from Special Report Publishing exclusively distributed in The Daily Telegraph

3rd April 2008



**Identity crisis:**  
Bullet-proof your data

02



**Spam killer:**  
defeat the cyber criminals

04

In association with:  
**infosecurity**<sup>®</sup>  
EUROPE

22-24 April 2008  
London, United Kingdom  
www.infosec.co.uk

## COVER STORY

# Establishing a culture of security

The challenges to business security are constantly changing as technology, and criminals, become ever more sophisticated

From April 22 to 24, London's Olympia plays host to the 2008 edition of Infosecurity, an event at which the good and the great, the small and the hopeful of the \$20bn IT security industry show off their wares, do deals and generally network.

The majority of the companies exhibiting will be in the area of edge security, which is technology designed to sit on the perimeter of a corporate network and keep the bad guys, or bad stuff like viruses, spam and spyware, out.

### Data Leakage Prevention

Over the last couple of years, however, some of the major players in this market, such as Symantec and McAfee, have been acquiring companies that offer data leakage prevention (DLP) technology, which puts a new twist on edge security: it also sits on the perimeter of a network but its objective is to keep the good stuff in, such as sensitive information or intellectual property.

A smaller number of companies, but making up a nonetheless vigorous minority, will be in core security, which is technology that sits inside the perimeter and controls who, among authorised users, can access what databases and software programmes, known as applications.

### IRAM

This is identity and access management (IRAM) technology and is destined to become just as critical as edge security, as companies face a growing wave of legislation and regulations with which they must comply to stay in business.

This supplement covers all these areas, as well as discussing some of the other hot topics in current IT security development. For instance, with laptop computers tipped to overtake fixed desktop PCs in total sales in the next few years, the issue of how to protect the data on them is rising on the corporate agenda.

### VoIP and social networks

And with voice over Internet Protocol (VoIP) telephony being adopted by an increasing number of companies to replace traditional voice circuits, we also discuss the increased need for security when voice traffic becomes just one more stream of bits and bytes on a hackable data network.

**"Doing business safely has to be actively pursued if people are to trust that their personal data and identities are in good hands"**

The last couple of years have seen the rise in the UK of social networking, a trend imported from the US and adopted wholeheartedly by the so-called Generation X and Y age groups. Hugely popular websites such as Facebook, MySpace and YouTube have drawn a lot of media attention and launched the careers of several budding musicians, but they also represent a challenge for businesses.

Firstly, there is the sheer capacity for time wasting by employees they represent, but secondly there is the security threat, as hackers and writers of malware can infect them, using them as a route on to a company network.

### Controlling web access

Companies now face a decision whether to block access to social networking sites, in the name both of employee productivity and information security. However, Nigel Hawthorn, international marketing VP at security vendor Blue Coat, was phlegmatic on the subject.

"A recent independent survey of more than 250 security managers and network managers commissioned by Blue Coat found that 74 per cent of security managers and 71 per cent of network managers believe that... applications like Facebook should be banned from the workplace," he began. "But I think social networking sites like Facebook and MySpace are another example of a new technology, like the Internet in its early days, which is still in the early phase of the 'Technology paranoia curve.'"

We're already finding that more liberally minded organisations can see that for some departments – like marketing or even HR – it can be a useful tool that they need to

use in the work place," he went on. "And like the Internet, once firms have found a way to control access, using a combination of acceptable usage policies and technologies to reinforce the policies, I believe it will find its place alongside email and the Internet in our daily working lives."

David Kelleher, a communications and research analyst at another infosec developer, GFI, identified three possible lines of action for companies in this situation. "First, a company can simply ban not only access to social networking sites (in the extreme case – no internet at all). Secondly, it can allow employees unrestricted access, confident that they will only use it during their lunch break and they will not download material on to the network. The third way is to monitor and limit staff access to these type of sites, including general internet browsing and downloading," he explained.

Looking at each option, Kelleher argued that outright banning, while increasing security, also sends a negative signal to employees, imposes limitations on those who need to access the internet and ignores the employee's "right" to spend his free time at work as he or she chooses.

The second option, unrestricted access, is obviously dangerous and no system administrator would want employees to be visiting and downloading material from sites that are known to contain viruses etc. Also the uncontrolled downloading of material or widgets from Facebook could be a security threat.

"The third option is probably the best and means striking a balance," Kelleher concluded. "Companies can install software that monitors what sites are being visited and allows administrators to block those that are not permitted, such as porn or gambling sites. At the same time, administrators can also block access to certain sites, such as Facebook, for most periods of the day except during lunch or after hours." Companies can also prevent or block downloads from these sites by implementing policies for particular file-types.

"There are arguments in favour of each option and for many companies the solution may not be as easy as choosing one or the



other," Kelleher went on. "There is no doubt, however, that social networking, is starting to cause problems for IT administrators and a solution is needed that offers a balance: providing access without compromising the security of your corporate network."

### Compliance

Finally, we discuss the ever-increasing mountain of legislation and regulations companies must comply with, how this drives them to deploy information security products and how they can help companies meet their compliance requirements.

From the Data Protection Act, the Companies Act and the Computer Misuse Act in the UK, through innumerable EU directives to Sarbanes Oxley in the States, businesses face the challenge of complying with multiple rules and regulations, so something that can help them demonstrate they are endeavouring to do so is much needed.

### Nice timing

David Leighton, director of professional services at Siemens Enterprise Communications, said this year's Infosecurity

show takes place at a particularly opportune moment for the industry in the UK. "The security market has never been more exciting. The public sector as a whole, as well as parts of the commercial sector, is in the middle of what could be described as a 'perfect storm.'"

He enumerated the components of that storm: "The National IA (Information Assurance) strategy launched in July last year at the IA07 conference; the major security incidents that have peppered the last 12 months and the subsequent Cabinet Office Data Handling review which is being finalised at the time of writing, plus the release of new risk management practices by GCHQ/CEG, have meant that the whole security and risk management arena is under ever increasing scrutiny."

Adding into that heady mixture the wider trends towards the adoption of VoIP, wireless, mobility, plus the move towards shared services [i.e. the partial outsourcing of non-core business functions], "the value of consultancy services to support these business changes and transformations is

increasingly evident both to clients and citizens alike."

### A culture of security

Beyond that, Leighton identified a need not just for infosec products to be installed, but for an actual culture of security to be inculcated in organisations. "What is clear from the events of the last year, the MoD laptop losses being an example, is that technical solutions alone aren't enough. There must be awareness at all levels and throughout an organisation – a 'culture' of security must be established."

He elaborated further on what he meant by a culture of security. "Part of this is the staff awareness and induction training that we always talk about, but further than that there must be intrinsic security discussions within projects and developments, the outputs of penetration tests should be 'understood' rather than blindly fixed as a kind of 'snag list'; the root causes of security failures should be established and acted upon. Doing business safely has to be actively pursued if people are to trust that their personal data and identities are in good hands."

**"SECURITY PRODUCT OF THE YEAR" "WINNER"**

Finalist, CNET Networks UK Business Technology Awards

**"2007 GLOBAL PRODUCT EXCELLENCE" "BEST BUY" "INNOVATOR"**

Finalist, Info Security Products Guide

SC Magazine 2007

SC Magazine 2007

**"HOT COMPANY" "BEST ENCRYPTION SOLUTION"**

Info Security Products Guide

SC Magazine Global Awards

**PRETTY GOOD IS NOW GREAT.**

www.pgp.com

DEFENDING THE DATA



## Contributing editor

Rik Turner,  
Senior tech analyst, Datamonitor

## Contributor:

Jason Stammer,  
Computer Business Review editor

## special report publishing

Publisher  
Tom Eales

Editor  
Andrew Baker

Design & Production  
John Kirby

Print & Distribution  
Telegraph Media Group Limited

www.specialreportpublishing.com

For more information about future reports distributed exclusively with the Daily Telegraph please contact Special Report Publishing on 020 7629 7080

Copyright Special Report Publishing © 2008

## Security quick facts

In January this year, MessageLabs identified an average of 1,068 new websites per day that had become carriers of malware, spyware or adware. For the same month, the proportion of emails containing malicious links rose to 29.5%. Phishing attacks had grown to reach 89.2% of all malware threats by January, such that one in every 147 emails comprised some form of phishing attack.

Despite all the talk of Russian or Asian gangs, in reality the US remained the largest single source of spam, being responsible for 36.6% of all spam sent in the month of January.

# How to avoid an identity crisis

Simple passwords are no longer sufficient to protect vital company data. A more sophisticated approach is essential

While one set of information security products tends to see the world in black and white terms, seeking to protect everything that's inside a company network from anything that's outside it, another group takes a more granular view of what goes within the walls of the castle.

These are identity and access management (IAM) products, which recognise that while an individual may indeed be a bona fide user on a company's network, that does not mean they have open access to every database, programme or system it contains. For instance, only certain members of staff will be authorised to see the HR database, another group will be allowed to see the payroll system, and so on.

In addition to these different types and levels of role-based access within the staff, there is an increasing requirement, in the new outsourced, globalised economy, for non-employees to have some level of access to a company's systems. Contractors and service providers, for instance, may need to access areas of a company's ERP system to update stock levels after a delivery or to input the time of the most recent maintenance check on a critical piece of machinery.

There is yet another level of access that a growing number of companies are starting to grant, which is guest access. A customer or business partner, for instance, may be on a company's premises for the best part of a day, during which they will want to check their emails or do some internet banking, but should not be able to get onto any of the company's systems. In other words, they should get internet access and no more.

**IdM**  
Identity management (IdM) systems address these requirements by associating a user name and password with an entry in a special back-end database called a

"Encryption remains the only bullet-proof way to ensure that data – if stolen – is of absolutely no use to cybercriminals"

directory, where a company's entire staff can be listed with each individual's areas of authorised access. Ideally all their access rights should be centralised into a single directory, enabling so-called single sign-on functionality, rather than each system requiring its own user name, password and so on.

For contractors and guests in this scenario, the company's IT department can grant short-term access rights and issue a user name and password, even specifying the amount of time for which they are valid.

There are, however, issues with relying exclusively on user names and static passwords, i.e. ones that are changed, perhaps once a month. "A major problem is that people are forgetful, so when asked to pick a memorable combination of letters and numbers, most will opt for something simple like the name of a relative, pet, football team and the date of a birthday," said John Stewart, director of sales and marketing at Signify, a Cambridgeshire company that develops so-called two-factor authentication (2FA) technology.

"This drives IT managers crazy; but it's not easy to change human nature. And even if users do use more complex passwords, they can easily be stolen through simple 'shoulder surfing' or using readily available

software for password cracking, keyboard logging, or by installing a Trojan horse password piracy programme."

### 2FA and OTPs

Signify and other companies therefore propose 2FA, which Stewart described. "A strong authentication system demands two or more distinct proofs of identity before granting access. Known as two-factor authentication, the most common factors used are something you know such as a secret PIN or password plus something you have. This can be a unique, physical device such as a token, smart card or even a mobile phone or PDA."

The physical device is used to generate what is called a one-time passcode or OTP, he went on, so that "the user presents a different passcode every time they login. Therefore, even if a user's session is snooped, the stolen passcode cannot be reused. Most OTPs require no special reader or input device, so the user is able to log in from any convenient PC or other Internet connected device."

### Encryption

Still a further level of security can be added by implementing encryption technology. For instance, a company could mandate that all HR documents must be encrypted, or could choose to selectively encrypt particularly sensitive emails. Thus in addition to being allowed onto the company's network and even being allowed access to a given database, someone can still have to provide further authentication credentials in order for encrypted data to be decrypted so that they can see it.

"If last year's high profile data breaches have taught us anything, it's that mass data loss is and will be a problem for organisations



everywhere, unless precautions are taken now. Today's cybercriminal has well and truly evolved beyond passwords and padlocks – and a vast amount of confidential data remains vulnerable, even within organisations that are seemingly fully protected," said Jamie Cowper, director of marketing for the EMEA region at encryption vendor PGP.

"Encryption remains the only bullet-proof way to ensure that data – if stolen – is of

absolutely no use to cybercriminals.

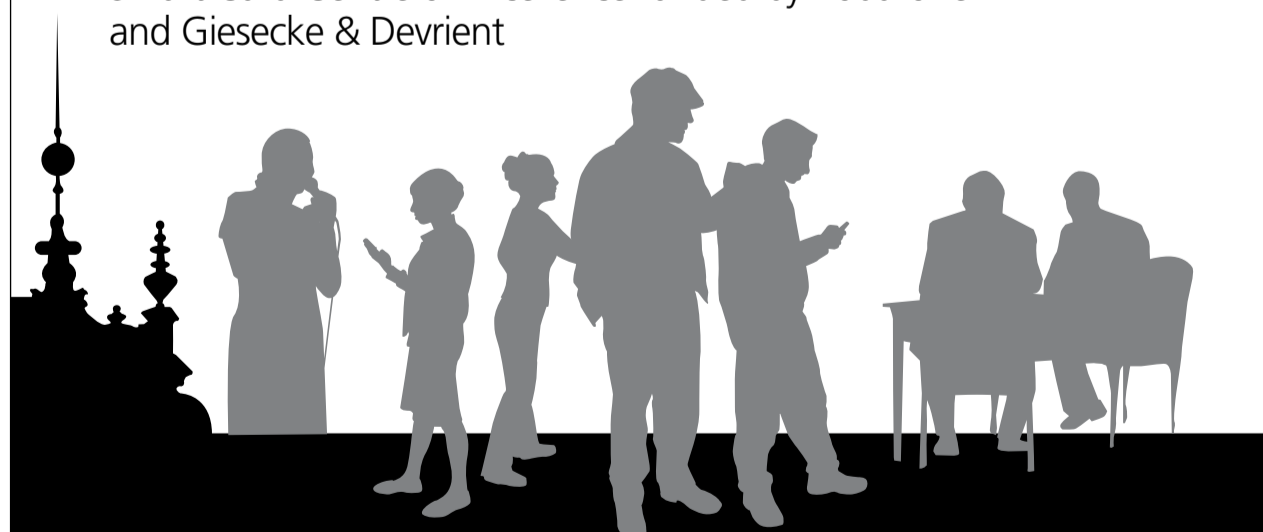
However, in their bid to address the external threat, organisations must be careful not to ignore the very real threat from within. Organisations that unwittingly grant employees (and third parties and contractors) blanket access to all data on a shared server would be wise to use encryption to enforce an effective 'separation of duties' policy, thus ensuring that only those members of staff with the correct level of authentication can access confidential information."



## Information Security Group

One of the largest academic Security Groups in the world, the Information Security Group at Royal Holloway has been at the forefront of research and consultancy in the field of information and network security over the last 20 years. We offer:

- World-leading Masters Programme in Information Security
- Taught by experts from industry and academia
- Flexible delivery (full-time, part-time, on/off campus, block-mode, CPD mode)
- Available worldwide by distance (online) learning
- Unique association with (ISC)<sup>2</sup>
- Smart Card Centre of Excellence funded by Vodafone and Giesecke & Devrient



Information Security Group  
Royal Holloway  
University of London  
Egham, Surrey TW20 0EX  
isg-secretary@rhul.ac.uk  
www.isg.rhul.ac.uk  
T: +44 (0)1784 443093  
F: +44 (0)1784 430766

*"To me, the MSc programme is the window to the wealth of information security knowledge in the world. It is an invaluable programme that has escalated my career in information security"*  
Meng Chow Kang,  
Microsoft Chief Security & Privacy Advisor, Asia Pacific Region

## Infosecurity Europe 2008

A survey by Infosecurity Europe of 1,311 companies has found that the single greatest security weakness for 79% of organisations is due to people not knowing about, ignoring or circumventing security processes and technical countermeasures. Lack of awareness has been the main cause of some of the most impactful security incidents in the UK in the last 12 months whether as a result of HMRC sending inadequately protected discs containing millions of peoples sensitive data in the post, the MOD leaving a lap top in a car with hundreds of thousands of confidential data records on it, or TJX transmitting millions of credit card transactions over an open wireless network.

Customers, taxpayers and citizens expect governments, companies and organisations to keep their information safe. When that trust is betrayed by people either deliberately or by mistake it can have a serious impact. We are yet to see how the laws relating to data security are going to be amended in light of HMRC, however it is expected that there will be significant strengthening to the Data Protection Act and Companies Act. The impact of this could result in a legal requirement for public disclosure of information losses and also criminal prosecution for Company Directors, senior civil servants and politicians responsible for security breaches.

The research also found that a sixth of organisations feel that the greatest threat to information comes from out of date or insufficient security technology and countermeasures. Infosecurity Europe is the event where those responsible for securing their organisations information can find all the latest technology, services and advice from over 300 of the top information security companies across

the globe exhibiting. The cutting-edge education programme at Infosecurity Europe is the highlight of the information

"The greatest threat to information comes from out of date or insufficient security technology and countermeasures"

security industry's international calendar reflecting the issues that organisations need to resolve. Over three days visitors have the opportunity to listen to 130 experts including Adam Laurie, Alan Paller, Bruce Schneier, Prof Fred Piper, and Prof. Howard Schmidt. Two key pieces of industry research will also be released at the show this year with the launch of the 2008 Information Security Breaches Survey on behalf of the UK Government and the (ISC)<sup>2</sup> Global Information Security Workforce Study 2008.

The Interactive Theatre sessions are a new feature for 2008 where visitors can see information security presented as never before. The Interactive Theatre is a great place for visitors to pit their wits against the people that are driving information security. Electronic voting facilities will bring visitors into the discussion to experience the pressures of security breaches as they hit an organisation. Scenarios vary from courtroom examinations of culpability and process in a cyberattack, to quizzes, malware tracking and data security examinations, 'ask the expert' clinics and



the legendary Lions Den. Fortify Software will present their new movie documentary, "The New Face of Cybercrime". Visitors can be the first to watch this groundbreaking feature. Filmed by Academy Award-nominated filmmaker Frederic Golding, it highlights the impact cybercrime has on consumers and businesses, and is tipped to win awards at independent film festivals this year. The film will be followed by an interactive panel debate led by Prof. Howard Schmidt, former Cyber Security Adviser to the White House.

The Cyber Attack Special, sponsored by Symantec, will simulate a situation which could ultimately destroy a company. Will it turn the CEO's hair grey or will the CISO be able save the day? Ed Gibson, Chief Security Adviser for Microsoft UK will chair a team of experts who will review the latest threats and mitigation strategies. The audience in this session will interact electronically with the panel to share their experiences anonymously of where their real threats are coming from and provide a unique forum to benchmark security strategy.

Visitors will also have their chance to 'Ask the Experts' in a sessions dedicated to PCI Compliance and Enterprise Application Security and Securing the Application Aware Network, sponsored by Akamai Technologies.

For FREE entry and further information about Infosecurity Europe 2008, visit the website at [www.infosec.co.uk](http://www.infosec.co.uk). Pre-register before 18th April to avoid the onsite booking fee of £20.

# Stop that leak

Businesses are rightly concerned with what they can gain. But in the area of data protection they should be more worried about what they can lose

Information security infrastructure is often likened to the fortifications of a medieval castle, where a moat and thick walls would keep out the enemy, while a drawbridge (which in this analogy would be the firewall) could be lowered to let friends in.

The comparison is a fair one, in that a host of product types, including anti-virus, anti-spam, anti-spyware, intrusion detection and prevention systems, content filtering software and the aforementioned firewalls, are all designed to keep undesirable software or actual individuals off a corporate network.

However, in the last few years a new class of product has grown up, which again sits at the boundary between the private company network and the public internet but looks at outbound traffic, with a view to stopping valuable information being spirited out. It's as if the castle had guards on the inside, stopping people from leaving with the baron's gold and silver or his lady's jewels.

#### Mergers and acquisitions in DLP

This technology is called Data Leakage Prevention, or DLP, and like most new classes of product, it was initially pioneered by a group of small start-up companies, who developed the technology and evangelised about its capabilities. At a certain point, however, larger infosec vendors saw the desirability of having DLP in their portfolio, and a round of acquisitions got underway.

Over the space of a year, half a dozen of these start-ups were acquired by larger entities, including the two biggest players in anti-virus (Symantec and McAfee) and the best-known name in encryption (RSA, now part of storage heavyweight EMC). While several of the deals were quite small, around the \$10m-\$20m mark, Symantec's acquisition of Vontu, widely seen as the market leader

in DLP, in November last year had a price tag of \$400m, an indication of how seriously the anti-virus heavyweight wanted to get into the emerging market segment.

#### Gateway and client

Most of the start-ups in the DLP market developed one of two types of technology, namely "client" products, which are software designed to sit on individual end-user machines and watch for potential data loss through copying it to USB sticks or outbound emails containing sensitive files; and gateway products, which sit on the perimeter of a corporate network and inspect all outbound traffic for potential breaches.

In reality, of course, both types are required, for while the gateway may be a powerful way to lock down the data on a corporate network, there is always the risk of a company laptop working from an employee's house or an internet café, so the need for the client software continues independently. Indeed, most of the companies that offered one or other of the parts had already cut partnerships with someone in the other camp for a complete offering.

"We bought PortAuthority at the beginning of 2007 because they had a network-based technology," recalled Devin Redmond, senior director of product management at Web filtering company Websense. At the same time that it developed its own endpoint technology, in January the company also announced an Open Endpoint Initiative whereby other vendor's clients can work with its product, enabling companies to leverage their investment in other DLP endpoint products in conjunction with the Websense gateway.

#### The threat within

Of course, malicious data loss is only part of the problem. "Most people don't get up in the

morning planning to make a hash of their job," said David Stanley, VP for Europe, Middle East and Africa (EMEA) at Proofpoint, a developer of email security and DLP technology. "And in the case of data loss, for the most part it's not malicious or pre-planned - it's simply a case of human error."

Andrew Clarke, senior VP for international business at infosec developer Lumension, identified a certain misunderstanding with regard to DLP. "A number of companies... are falling prey to a series of misconceptions. Due to the high profile reports of data missing through lost laptops and discs, the belief that the outside threat is greater than the inside threat has risen. These days most enterprises have full protection from outside assaults, which are typically achieved through malicious programs designed to install invisible backdoors into the enterprise," he went on. "What leaves them truly vulnerable is the threat from inside."

"Most organisations have no methods in place to prevent trusted employees from loading data onto external devices and walking away," Clarke explained. "And yet, this route of data leakage can prove the most dangerous to a company. Not only does the trusted insider have access to the data, but they usually know the value of the data and what to do with it. If organisations are serious about prioritising security based on the severity of risk, they must put insider threat protection at the top of their list."

#### Authorised user, unauthorised behaviour

The threat within typically comes from someone who is a legitimate user on a corporate network, and so can come in through the normal channels of authentication by the identity management (IdM) system, but once on the network starts to do things they

shouldn't, such as access databases that are outside of their remit, copy data to USB drives or email it to outside destinations, for instance.

Geoff Sweeney, CTO of Australian infosec developer Tier-3, also acknowledged the seriousness of the threat within, but argued that no combination of identity management and DLP technology would be sufficient to address the challenge. Instead, his company offers technology it calls behavioural intelligence, which in essence is self-learning anomaly detection that flags the unusual and irregular in employee behaviour, without relying on a pre-existing rule against which to compare it.

"A lot of companies with inspection technology claim behavioural analysis capabilities, but many of them are limited to looking at the data, network and transport layers," said Sweeney. "This is insufficient for true anomaly detection, there being a need to understand the application itself, which we and comparatively few other vendors have."

#### B.A.D.

Tier-3's Behavioural Anomaly Detection (B.A.D.) technology works by implementing a central repository to hold the logs on all access requests, through which the anomaly detection software can then highlight inappropriate behaviour and unusual patterns that need to be investigated.

"This obviates the need for companies to retain droves of specialised and thus expensive people to analyse all logs, enabling them instead to have a few well-trained specialists looking into what the software has already flagged as suspicious," Sweeney said. The repository can also serve as a source of records that, if properly stored, can have evidential weight in the event of court proceedings against an individual being necessary.

# VoIP security



One of the most profound changes in telecommunications is currently underway, namely the widespread adoption of a technology called voice over Internet Protocol, or VoIP.

A protocol is a set of rules for how the bits and bytes in a stream of data are arranged so as to signify a particular meaning. The Internet Protocol (IP) is, as its name suggests, the one used for the public internet, but is also now universally used on data networks in the corporate environment.

VoIP means that voice traffic is transformed into bits of data flowing over an IP network, and this obviates the need for a separate, dedicated voice network in offices alongside a data one. The potential advantages are many: if a company already has a private network joining up offices around the country for data communications, it can run voice traffic over it too, and avoid paying a telephone company for internal calls.

#### Security issues

However, for all the positive sides to VoIP, there is also a disadvantage. For when voice becomes just another data stream on an IP network, it is as hackable as any other traffic on that wire. For instance, if your office is on VoIP and you engage in phone banking while at work, your call, with all the account details, could be recorded with far less intervention than is required on a conventional phone network.

#### No single VoIP standard

The Royal Holloway University, a branch of the University of London located in Egham, in Surrey, has a dedicated Information Security Group and in 1992 became the first institution of higher education in the UK to create a Master of Science course in the subject.

Kenny Paterson, a professor of information security at the Royal Holloway, commented that the issue of security for VoIP installations "is a complex one because there are multiple competing standards, with each equipment vendor using their own proprietary protocols."

There is a clear groundswell of support among equipment vendors for a putative standard called the Session Initiation Protocol, or SIP, and a number of companies now offer SIP-compliant IP phones and PBXs. The technology also gained an important backer in recent years when Microsoft threw its weight behind SIP. However, even with SIP "the standard is a very long one, with multiple options within it, and each vendor implements only parts," argued Paterson.

Despite the increasing media attention devoted to VoIP security, however, Paterson said he was "not losing any sleep over it at the moment." Indeed, he went on, "what causes me concern is the fact that CDs with the details of child benefits recipients are travelling through the post in an unencrypted form."

## INFORMATION SECURITY

it's all about trust.

insider threat      identity management  
security training      intrusion protection  
company reports      remote access

Are you sure that your information security is in safe hands?

Threats to your business can come at anytime and from anyone; your customers, your suppliers or your employees.

Find out how to protect your company's business information at Infosecurity Europe, Europe's No.1 information security event.

Register FREE\* to attend now at:  
[www.infosec.co.uk](http://www.infosec.co.uk)

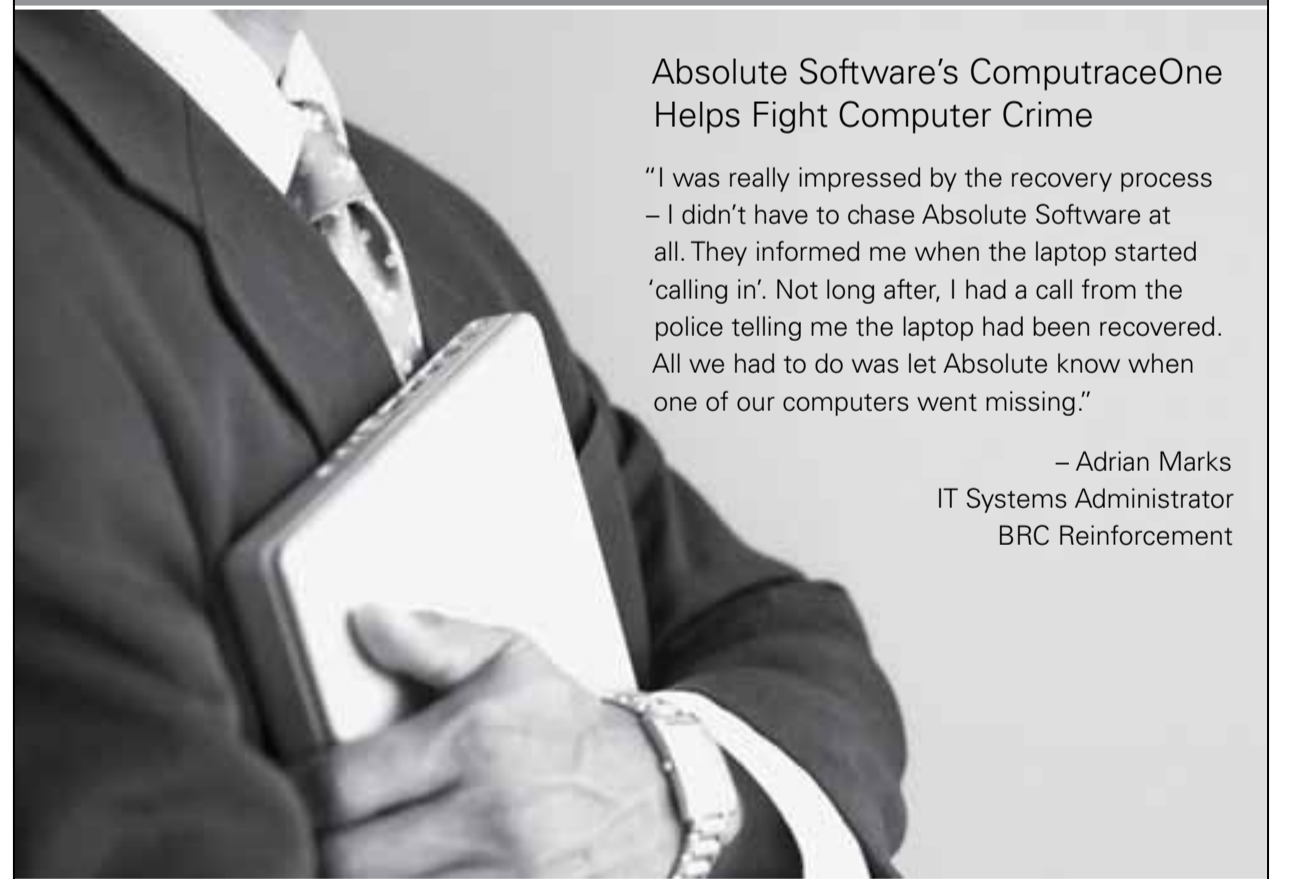
**infosecurity**  
EUROPE

22nd - 24th April 2008  
Grand Hall, Olympia, London, UK.

Reed Exhibitions

\*Visitors not registered by 5pm on Friday 18th April will be charged a £20 entrance fee.

## Prevent Data Breaches from Lost or Stolen Computers with ComputraceOne



### Absolute Software's ComputraceOne Helps Fight Computer Crime

"I was really impressed by the recovery process - I didn't have to chase Absolute Software at all. They informed me when the laptop started 'calling in'. Not long after, I had a call from the police telling me the laptop had been recovered. All we had to do was let Absolute know when one of our computers went missing."

- Adrian Marks  
IT Systems Administrator  
BRC Reinforcement

Today's computing assets contain more sensitive and valuable information than ever before - making each computer a potential liability without proper protection. Organisations risk legal and public relations nightmares when even one notebook goes missing.

Computrace®One™ notebook security and tracking software helps ensure regulatory compliance by protecting data, tracking hardware and users, providing auditing capabilities and acting as a historical record of computer assets and their use.

Download the free whitepaper: "Compliance. Protection. Recovery. A Layered Approach to Laptop Security" and learn how to:

- Track & recover lost or stolen computers
- Delete data remotely to protect confidential information
- Detect unauthorised software & hardware
- Accurately inventory computers regardless of their location

Download the essential laptop security whitepaper at:  
[www.absolute.com/DT308](http://www.absolute.com/DT308)

Visit Absolute®Software at InfoSec Stand H217 & enter to win a Lenovo ThinkPad preloaded with ComputraceOne software!

[www.absolute.com/emea](http://www.absolute.com/emea) | 01635 30424

**AbsoluteSoftware**

# Time to can the spam

E-criminals, be they spammers or phishers, are becoming ever more sophisticated. So is the technology that can foil them

On the face of it, spam emails are an irksome waste of time, which the unwilling recipient must expend effort to delete from his or her inbox. Technology for blocking spam is offered as a service by a number of companies, including UK-based MessageLabs and Postini in the US (now part of Google), and they all agree that spam currently represents anywhere between 80 and 95 per cent of all email traffic.

But beyond the irritation factor lurks a security threat. Spam can come contaminated with malware, and if the title is sufficiently intriguing as to cause the recipient to open it, it may unleash some form of infection for the user's machine.

It may install some software on the machine that covertly inspects what the user is writing (a keyboard logger) or in the browser to know what websites are visited and passwords used to access information (man-in-the-browser technology), or simply a programme that lies dormant until, on a given day, it starts to send hundreds of emails or requests to access a site in a distributed denial of service (DDoS) attack.

## The rise of the botnet

When hundreds of such machines are contaminated by the same piece of malware, such that they can be made to operate together when an attack is mounted, they are referred to as "zombies" or "bots", a collection of which is called a botnet, with the criminals who rent them out for spam runs known as herders.

This has become the delivery mechanism of choice for large volumes of spam, and indeed the Storm botnet, which has an estimated 2 million compromised computers under its control, was a major force in driving spam during the first three months of 2008. MessageLabs' statistics suggest Storm was responsible for 20 per cent of all spam during this period.

For the first time, the Storm botnet has been used to send spam touting VXPL, a drug

"Today's cybercriminals are motivated by financial gain, and their main vector of attack has become the Web"

promising male sex organ enlargement, and nicotine patches, likely to be tapping into a seasonal increase in smokers trying to quit.

## Web-based threats take over

Malware is increasingly written for financial gain rather than kudos, and the type that is designed to harvest sensitive information such as log-in details for internet banking or credit card details carries out what is called phishing. It need not even rely on infected emails per se to find its way onto a user's machine, and indeed, the preferred vector for entry is increasingly the Web itself rather than viruses contained in an email.

For instance, an apparently innocent email can be sent with a Web address (called a URL) and suggesting the reader go there for more information on a given topic. Clicking on the URL takes them to a page where, in addition to the information they expect, they are also surreptitiously infected with the phishing software.

"Today's cybercriminals are motivated by financial gain, and their main vector of attack has become the Web," said Yuval Ben-Itzhak, chief technology officer of information security vendor Finjan. "They understand too well that signature- and database-reliant solutions [such as anti-virus software, URL filtering and reputation based security] are not designed to protect against obfuscated malicious codes served on compromised legitimate sites, Web 2.0-based sites, and other dynamic attack vectors that use the Web. These sophisticated Web-based



attacks are specifically designed to hit the 'blind spots' of traditional security systems that rely on signatures or databases."

## Evolution

"2008 got off to an aggressive start, with spammers proving to be more business-minded and time sensitive than ever in their strategies, and seeking to exploit the most common and current weaknesses - everything from New Year weight loss hopes to fears about the credit crunch," said Paul Wood, a senior analyst at MessageLabs. "Unfortunately every month of the year provides the spammers with a newly vulnerable group to target."

"For years now, this has been a cat-and-mouse game between spammers and anti-spam developers," said David Kelleher, a communications and research analyst at email security developer GFI. "More recently, we have seen image

spam, PDF spam and MP3 spam hitting the headlines and this shows just how creative spammers have become."

David Harley, research author at anti-virus developer ESET, identified still further areas of development in security threat technology. "Phishing and botnet activity is actually showing a perceptible downward trend in its 'classic' forms," he began. "However, as people become more aware of the risks, criminals are looking for new areas to exploit."

"One trend we've noticed in anti-malware research is to put out Mac versions of malware such as backdoors, bots and rogue 'security' software, which is either useless or frankly malicious. This is probably an attempt to exploit Mac users with the naive belief that Mac OS X is intrinsically so safe that security breaches are impossible."

## What to do

GFI's Kelleher outlined three ways companies can effectively stop spam:

"Employees should be told to delete any spam that looks suspicious and to ignore emails asking for personal details. It is surprising how many people still fall for spammers' tricks (and that's why spammers are still around)," he began.

"Also, employees should not be allowed to install unauthorised software and they should be denied access peer-to-peer sites to avoid machines becoming infected by worms, trojans, or other malware and thus become part of a botnet. The third method is to install a best of breed product that is capable of identifying as many forms of spam as possible yet without deleting email that is important. The test for any anti-spam solution is to identify spam and allow genuine email to pass through the filters."

## Shopping for anti-spam

For companies that choose the third path, Kelleher had three more recommendations of what to look for in an anti-spam product:

**First, choose a product that battles spam at server level rather than at client level. A server-based product offers the following advantages:**

1. Installation on the server eliminates the need for workstation based anti-spam software.
2. It is far cheaper to license.
3. Spam is stopped at the entry point of the company's network and not each end-users' mailbox
4. A server-based product provides more information that can be used to deal with spam faster and more effectively.

**Second, choose a product that uses multiple technologies**

A solution that only identifies spam using keywords is bound to fail because spammers have adapted their techniques to bypass traditional methods of detection. Today they are using image spam, audio files, common office documents etc to gain access to mailboxes. Thus, companies need an all-round solution that offers second generation Bayesian filtering - a mathematical method that allows the software to 'teach' itself what is spam - as well as whitelists, intelligent mail header analysis, checking senders against custom blacklists and public blacklists such as ORDB or SpamHaus and others.

**Third, choose a product that returns few false positives**

The worst nightmare for an administrator is to use a product that also deletes important and critical business emails. The test for any anti-spam product is to reduce spam as much as possible but with the lowest return of false positives.

## Knock out spam at Exchange level!

Visit us at  
Infosecurity  
Europe,  
Stand G200!

## GFI MailEssentials

Anti-spam for Exchange, anti-phishing and email management

WAS  
£ 405  
NOW  
£ 257.50  
for 25 users

With over 60 awards to its name, 80,000 satisfied customers and unbeatable price-performance, GFI MailEssentials for Exchange/SMTP/Lotus is a best-of-breed anti-spam package that is easy to set up, captures over 98% of spam and also removes the need to install and update anti-spam software on each desktop. Eliminate spam from your mail server with the following key features:

- **Server-based anti-spam and anti-phishing** - Detects and blocks spam and phishing emails
- **Bayesian filtering** - Detects over 98% of spam based on statistical message analysis
- **Automatic whitelist management** - Keeps whitelists up-to-date without extra admin
- **Attachment spam check** - Detects image, PDF, Excel, ZIP and mp3 spam
- **Email header analysis and keyword checking** - Blocks spam based on message field info and keywords
- **#1 anti-spam solution** - Over 60 awards and 80,000 customers
- And much more!

Voted MSExchange.org Readers' Choice Award Winner in the Anti-Spam Category four times, GFI MailEssentials is the number one server anti-spam solution at unbeatable pricing!



**GFI** NETWORK SECURITY  
CONTENT SECURITY  
MESSAGING

Download your free trial from [www.gfi.com/tdt/](http://www.gfi.com/tdt/)

tel: +44 (0) 870 770 5370 | fax: +44 (0) 870 770 5377 | email: [sales@gfi.co.uk](mailto:sales@gfi.co.uk) | url: [www.gfi.com/tdt/](http://www.gfi.com/tdt/)

## How to protect your laptop

Laptops have overtaken desktops in business use. But they are much more vulnerable than office-based equipment. How can you best protect your hardware and data?

Laptop computers outsold desktop machines in Western Europe in the fourth quarter of 2006 and the trend is set to be the same worldwide by 2010, according to analyst firm IDC.

The reasons for this shift are obvious. The portability of a laptop machine means you can take your work with you, from the office to home or the nearest Starbucks. Meanwhile, laptop prices have dropped to such an extent that buying a fixed desktop machine these days is motivated almost exclusively by the fact that you get a lot more processing power (i.e. the microprocessor and memory) and storage (the hard drive) for the money.

But with the greater convenience of laptops comes increased risk. Stealing a desktop computer implies breaching a building's physical security and timing it in such a way that you can make your escape, lugging the computer as you go, without detection. Stealing a laptop, by contrast, can be as simple as being in the right coffee shop or railway carriage at the right time.

## Biometric security

Not surprisingly, therefore, the IT industry has been addressing the security risk of laptop theft for some time. Manufacturers such as HP and Lenovo (the Chinese company that bought IBM's laptop division) have offered biometric security in the form of fingerprint readers on their machines for the business community since the early part of this decade, such that anyone else getting their hands on them won't be able to open them and access the data.

Jim Fulton, VP of fingerprint authentication vendor DigitalPersona, said such technology can help companies overcome the shortcomings of approaches such as passwords, PIN numbers and smart cards. "Biometric authentication, specifically

"Passwords aren't enough. To achieve absolute information security, organisations have to deploy comprehensive encryption policies across the enterprise"

fingerprint authentication, can solve the authentication problems which current methods of ID verification are proving incapable. Aside from providing unrivalled ease of use and an impressive return on investment (due to increased productivity and reduced demands for IT support - it is estimated that 25-50 per cent of help desk calls are for password resets), fingerprint biometrics provides organisations with the tools to comply with the increasing levels of corporate governance."

## Encryption

Of course, not every corporate laptop today is acquired with such technology, and for those that aren't, Jamie Cowper, director of marketing for EMEA at PGP, a developer of encryption technology, recommended a policy of encrypting all data on a corporate network as default.

"Passwords aren't enough," he argued. "To achieve absolute information security, organisations have to deploy comprehensive encryption policies across the enterprise. By automatically encrypting data whenever a laptop is plugged into the corporate network, companies can ensure that if and when hardware does go missing, the data on board stays protected and safe."

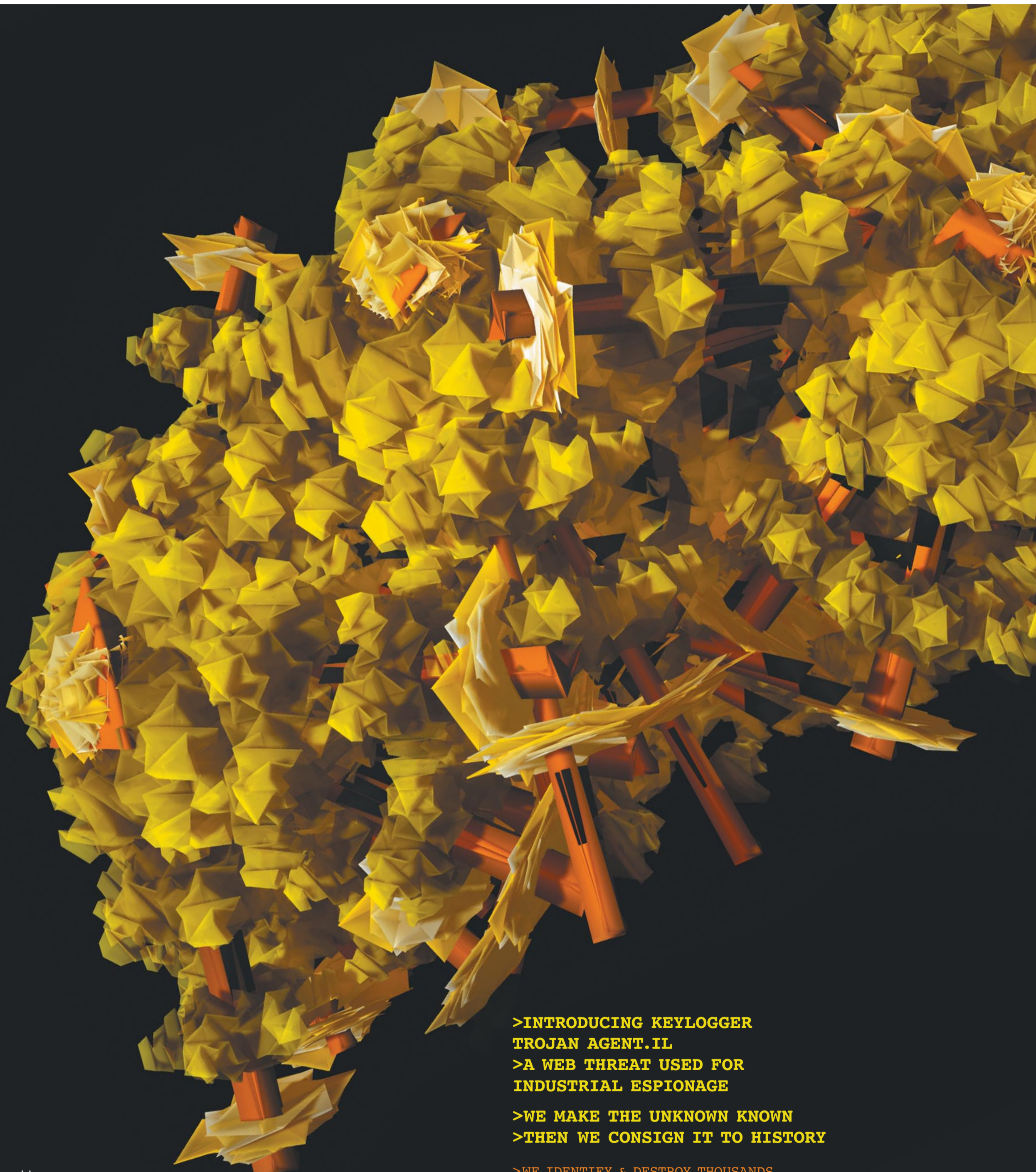
## Tracking stolen machines

Beyond biometrics to lock down a machine and encryption to protect the data on it, there is also technology to track stolen laptops, despite attempts to reformat them. Canadian developer Absolute Software has a product called Computrace, which involves installing software into the machine's Basic Input/Output System (BIOS), which runs at the start-up sequence to configure the device, then boot up the operating system.

The BIOS is actually set in the machine's hardware, by being coded into the chips on a motherboard, so the Computrace Agent, as it is called, is rendered immune from any system re-installs, hard drive re-formats or replacements that thieves may try to make the machine re-usable. Though the software has a further element that does reside on the hard drive, if that piece of hardware is replaced, the Agent in BIOS rebuilds the necessary files on the new hard drive.

If a laptop is stolen and re-formatting of the hard drive takes place, the Agent nonetheless persists and initiates communication with a Monitoring Center, via an internet or phone connection, the next time the machine is plugged in. At that point it can enable theft recovery and remote deletion of any sensitive data.

"Organisations in both the public and private sector should adopt a layered approach to security," said William Pound, VP of international operations for Absolute. "The security measures should range from the obvious, such as not leaving laptops in view in a car, through to the tactical such as installing anti-virus and firewalls, to the strategic such as creating a contingency plan and implementing asset tracking and recovery software to track and recover lost or stolen computers. This software also allows for the deletion of any sensitive data remotely."



**>INTRODUCING KEYLOGGER  
TROJAN AGENT.IL  
>A WEB THREAT USED FOR  
INDUSTRIAL ESPIONAGE  
  
>WE MAKE THE UNKNOWN KNOWN  
>THEN WE CONSIGN IT TO HISTORY**

>WE IDENTIFY & DESTROY THOUSANDS  
OF WEB THREATS EVERY DAY  
>WE PROTECT SOME OF THE WORLD'S MOST  
SECURITY SENSITIVE ORGANISATIONS  
>OUR 24/7 MANAGED SERVICE HAS NO  
SOFTWARE OR HARDWARE TO MAINTAIN  
>VISIT [MESSAGELABS.COM/THREATS](https://messagelabs.com/threats) FOR  
A FREE TRIAL

 **MessageLabs** | Be certain

IMAGE GENERATED USING SOURCE CODE FROM TROJAN AGENT.IL

# Safe as houses

With ever-increasing threats to corporate security and increasing challenges in complying with industry-specific and regulatory legislation, security is a hard nut to crack. Jason Stamper asks a wide range of industry experts about the latest challenges

**Q** How can companies best make the business case for investment in security?

**Paul Williams**, chair of the ISACA [Information Systems Audit and Control Association] Strategic Advisory Group: "It is difficult to apply the same rules on investment business cases to security as might be applied to more traditional discretionary investments. Instead, the business cases need to be based upon a full assessment of risk, covering not just financial loss but also reputational and competitor risk."

**Yuval Ben-Itzhak**, CTO, Finjan: "Using audit/assessment devices, businesses can view existing malware already installed in their networks sending confidential data out to criminals. Once businesses see such assessment reports that were created based on their own network traffic, investment in security is made simple."

**Geoff Sweeney**, Tier-3 CTO: "Any failure to maintain the integrity and security of information assets can seriously impact stakeholder value. Whether it's to comply with regulatory obligations or protect company information assets from misuse or loss, IT security is a legitimate part of managing business risks. Failure to control such risks can impact a company and its stakeholders with legal, commercial and financial losses."

**Jamie Cowper**, director of marketing EMEA, PGP: "IT security teams need to help the business understand the risk associated with particular problems – security doesn't happen in a vacuum. For instance, a recent study into the cost of a data breach in the UK by the Ponemon Institute found the average cost per compromised record to be £47 – this provides a clear business case for companies to invest in enterprise data protection solutions to mitigate the risk of a breach."

"In today's world of constantly evolving and dynamic Web threats, the most effective protection is real-time scanning that will block threats at the Internet level before they reach the network"

**Tim Best**, Director of Enterprise Security Solutions, Logica: "Overall whilst we are seeing that more organisations are recognising that fraud and security issues are not 'grudge spend' but rather an investment, there needs to be a shift in perception that security solutions are not simply technology implementations but rather a catalyst for business change and revenue growth."

**Q** Do you believe that the focus on security has now shifted from the perimeter back to endpoint security (securing individual devices rather than concentrating on perimeter security such as firewalls?) If so, why?

**Pieter Van den Broecke**, Credant Technologies director of business development EMEA: "The question should not be whether the focus needs to be on the perimeter or on the end-point. The focus needs to be on what matters. In today's world data travels to various endpoints which cannot be controlled by the enterprise. For instance, an iPod owned by

a company employee can be connected to the enterprise network, and enterprise data can be transferred to this personal device for further use by the co-worker. It is important that from an enterprise data security perspective, the data on this 'personal' device is protected in a dynamic way."

**Calum MacLeod**, business development director, Cyber-Ark Software: "The shift back to the core has become increasingly evident over the past two or three years. And this is driven by a number of factors. Probably most critical is the realisation that every major 'attack' in the past few years has resulted from improper access to business-critical information."

**Rob Rachwald**, director of product marketing, Fortify Software: "No. Perimeter is still the focus of many companies and that is the problem, because hackers are going after the core."

**Q** Rather than relatively straightforward threat vectors such as viruses and spam, there is now the prospect of so-called "blended threats". How should companies protect themselves from this more complicated, or multi-pronged attack?

**Eldar Tuvey**, CEO, ScanSafe: "In today's world of constantly evolving and dynamic Web threats, the most effective protection is real-time scanning that will block threats at the Internet level before they reach the network."

**Donal Casey**, security consultant, Morse: "When protecting themselves from 'traditional' attacks such as viruses and spam, organisations have focused on the sources – namely email and web traffic and, to an extent, removable media. Blended threats add another dimension. The traditional methods remain appropriate but must be shored up with the use of technology such as IPS [intrusion

prevention systems] to monitor abnormal network behaviour; endpoint behaviour analysis to prevent clients and servers from acting inappropriately; and by ensuring that all critical systems within an organisation are protected by either network zoning to prevent threats from spreading, or by appropriate identity and access controls."

**Carole Theriault**, senior security consultant, Sophos: "Cyber-criminals meticulously craft these blended attacks to infect unsuspecting victims with the aim of stealing their confidential data or using their computer resource for the propagation of spam or infection. Today's network protection has moved beyond mere anti-virus. As the network perimeter dissolves, with users wanting more freedom to work on different devices from home or on the road, comprehensive security management has become key. This includes ensuring that all software is patched and kept up-to date, websites are checked prior to loading, firewall protection is installed and appropriately configured, and proactive threat protection is in place to stop certain programmes, be they malicious or unwanted, from even running. Being vigilant today better ensures that they are equipped to ward off current and future threats."

**Q** Security technology is useless unless employees follow the security policy. What can companies do to try and ensure employees comply with that policy?

**David Hobson**, MD of Global Secure Systems: "People are very often the weakest link. Education, education, education is the answer. The major issue is HR – most employees sign a policy when they join a business, and then never acknowledge any change of policy, if they are ever told of a change of policy."

**Jonathan Craymer**, chairman, GridSure: "A threat is a threat, wherever it

"Every major 'attack' in the past few years has resulted from improper access to business-critical information"

comes from. There's no point in locking the front door and bolting the windows to keep out thieves, if those within the company are allowed unnecessary free access to all areas. The answer is to have a clear hierarchical system/policy, allowing only key staff to access vulnerable areas; and to have ways of tracking who's been where and done what."

**Ann Bouquet**, MD, SafeBoot: "Despite the recent spate of security breaches, IT security is still not being taken seriously by employees; according to research we recently conducted of 1,000 IT managers across all sectors, 54 per cent of workers ignore company security policies. A company can do a number of things. Firstly, they can make staff aware of any security breaches in the media and inform them that security is very real and important. It is also important to inform the employees that if security guidelines and procedures are not followed it could be them exposed in the press along with the company. A very effective way of getting staff buy-in is to have the security message sent from the C-level management, getting them to lead by example."

**Q** It has long been held that the biggest threat to enterprise security comes from inside, not outside its walls. How should companies balance the need for

security inside the enterprise with the need for employees to have access to the data and systems they need to do their jobs, and how can the latest technology help?

**David Stanley**, Proofpoint MD, EMEA: "It's important to understand that inside threats such as data leakage usually relates back to education, policy and compliance. In some cases, the threat of exposure is low, and can be prevented and corrected, in others, the opportunity to 'leak' sensitive information isn't even possible. This is key to balancing access to data, as access rights can be divided up accord to the serious nature of the data in hand."

**Andrew Clarke**, SVP international, Lumension Security: "In order to protect against the insider threat - whether intentional or malicious - IT staff within the organisation need to take control away from the end user. This means adopting innovative technologies such as 'whitelisting' capabilities – that allows only the known good onto the network. Furthermore, policy development around what data employees can access and what they can't and strict enforcement of those policies is essential. As data moves beyond the perimeter, so too must the protection mechanism."

**Theriault**: "With more and more businesses now offering flexible working practices, and with visitors to the office increasingly expecting to be able to get on the Internet and check their email, the issue of how to ensure that all devices connecting to the network are up-to-date with their anti-virus protection and security patches, is top of mind. Sophos research has revealed that two thirds of corporate endpoints are not compliant with the company's security policies, but actually establishing which devices are falling foul of the rules can be tricky. To mitigate this risk, businesses should consider deploying network access control (NAC) solutions."

## Comply or die

When protecting your company's data, and that of your clients, you will do well to follow the rules

The Enron and WorldCom debacles, as well as a number of other major corporate accounting scandals that broke in 2001 and 2002, had a direct effect on legislation, leading to the passing by the US Congress of the Sarbanes-Oxley Act, or SOX.

To give it its more formal title, the Public Company Accounting Reform and Investor Protection Act of 2002 established new and enhanced standards for all US public company boards, management and public accounting firms, as well as for non-US companies with securities listed on US exchanges such as NYSE and Nasdaq.

It has 11 sections, including one covering criminal penalties, and it was the fact that company officers could go to prison for failing to comply that give it a high profile, as well as prompting the IT industry to bring forth a bevy of products designed to facilitate SOX compliance.

**SOX, DPA, Basel II and beyond...**

Because of its custodial implications, SOX is the most widely known and discussed piece of legislation when compliance issues are under discussion. There are, however, a host of others, including, in the UK, the Data Protection Act and Computer Misuse Act.

There are also sector-specific rules and regulations like the Revised International Capital Framework, or Basel II, in the banking world and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for the healthcare sector.

The credit and debit card sector is currently rolling something called the

Payment Card Industry Data Security Standard (PCI DSS) out across the globe, with companies that process, store or transmit payment card data having to prove their compliance at regular intervals or risk losing their ability to handle such transactions, as well as facing audits and/or fines.

**Involving stakeholders**

Compliance, like insurance, is normally something people do because they have to do rather than want to do, so David

"A quarter of companies that say they hold highly confidential electronic information lack procedures to comply with the Data Protection Act"

Stanley, VP for EMEA at Proofpoint, a vendor of email security and DLP technology, suggested an approach to implementing it that involves getting specific communities within the organisation on board.

"By involving key stakeholders such as HR, legal, product development and so on in creating and implementing a company's security policy, you create

understanding as to what is permissible and what's not from day one," he argued. "Then, taking into account that we're all bound to slip up at some stage, businesses can use the policy to educate users, rather than persecuting them for being, well, human."

**Management buy-in is critical**

Chris Potter, information security assurance partner at PricewaterhouseCoopers and the partner who leads the execution of the biennial IT security survey of British business for the Department for Business, Enterprise & Regulatory Reform (BERR), commented that "compliance with the Data Protection Act 1998 (DPA) continues to improve slowly."

Of course, the degree to which the top brass within a company buys into compliance is fundamental. "Senior management priority makes a big difference. 82 per cent of companies that give a very high priority to security have data protection procedures, versus 42 per cent of those where security is low or no priority. Worryingly, a quarter of companies that say they hold highly confidential electronic information lack procedures to comply with the Data Protection Act," Potter went on.

**Formal procedures**

He stresses the importance of structured processes for compliance. "A formal data protection process yields real benefits," Potter recommended. "Companies with documented procedures to ensure compliance with the DPA are half as likely to have data protection infringements, unauthorised access or confidentiality breaches by staff as those that do not."

COMMERCIAL FEATURE

## Unauthorized access and improper use

By Geoff Sweeney, CTO, Tier-3 [www.tier-3.com](http://www.tier-3.com)

A threat which is looming increasingly larger in the minds of CIOs is the risk of data loss through inappropriate behaviour or misuse by someone who is authorised to access the network and its information.

Let's consider a situation where a user has been granted access to the network, applications and databases in order to undertake their normal business activity; but whose behaviour becomes mischievous after authorisation. Perhaps they are downloading entire customer databases to their laptop or seeking to email sensitive data to an address outside the company, or copy it to a removable medium such as a USB stick. Either way they are abusing the access rights they have been granted and will need to be stopped urgently to protect against the loss of valuable company information assets.

According to Lars Davies, a compliance specialist from Kalypton, "If an authorised individual, has inappropriately accessed or copied company information then potentially an unauthorized access under the Computer Misuse Act has occurred; it could also be a breach of copyright law. If any personal data is involved, it could also constitute a breach of the Data Protection Act (DPA). This is not just a breach of trust. More immediate for the company is the loss of valuable information and the remediation costs. It may also stand accused of having failed to put in sufficient safeguards in place to prevent a breach and the directors could be implicated for failure in their fiduciary duties to protect company stakeholders from loss."

In response to this type of threat the information security industry has, in recent

years, developed a flurry of so-called data leakage prevention (DLP) systems which seek to address this emerging exposure for companies.

While the goal of DLP systems is undoubtedly well intended, the effectiveness of these technologies relies upon the satisfactory matching of user access authorisation levels with the classification of all corporate information assets according to their sensitivity and "value". The logic of such systems is clear but inflexibility and the administrative overheads of such systems is prohibitively high.

The thief may be a disgruntled employee, a contractor attempting to steal some of the company's intellectual property or even a trusted senior executive; there are no rules to predicting human behaviour. Inappropriate action of this type by anyone who has the authority to access sensitive company information can and still does occur. What is required is the means by which suspicious or unusual access or movement of sensitive data, irrespective of the initiator can be detected and assessed for legitimacy.

Behavioural Anomaly Detection uses intelligent real-time analysis technology to inspect and immediately alert on inappropriate user or system behaviour as soon as it deviate from the norm. Inappropriate data access can be spotted immediately without the need for complex access and asset prioritisation rules with their management overheads. The intelligent technology simply blocks unusual system or user activity and flags it to security and risk managers for their response.

Data breaches from unauthorized access and improper use are a growing problem,

"What is required is the means by which suspicious or unusual access or movement of sensitive data, irrespective of the initiator can be detected and assessed for legitimacy."

but they can be detected and prevented with appropriate security strategy and technology before they result in loss. Behavioural Anomaly Detection technology identifies when a legitimate user's behaviour non-compliant, blocks it and systematically stores a copy of all access logs in forensic repository for evidentiary purposes. Using smart technology Behavioural Anomaly Detection can automatically detect and protect valuable company information assets from misuse or theft as it occurs, rather than respond "after the horse (and its valuable information) has bolted".

Geoff Sweeney, Co-founder & Chief Technology Officer, Tier-3 Pty Ltd is speaking in the technical seminar programme at Infosecurity Europe on "WWIII has started: Shape shifting heuristic threats" 22nd – 24th April 2008 Olympia, London [www.infosec.co.uk](http://www.infosec.co.uk)



# Social networking - the threats

Allowing staff to play on the internet can cost companies a lot more than lost time

Even readers who are not part of Generations X or Y will be aware of the rise, in the last couple of years, of social networking websites, or will at least have heard of Facebook, MySpace or YouTube.

A social network is, to quote the online dictionary Wikipedia, "a social structure made of nodes (which are generally individuals or organisations) that are tied by one or more specific types of interdependency, such as values, visions, idea, financial exchange, friends, kinship, dislike, conflict, trade, web links, sexual relations, disease transmission (epidemiology), or airline routes."

Social networking sites, also known as social network services, use software to build online social networks for communities of people who share interests and activities, or who are interested in exploring the interests and activities of others. They provide a range of ways for individuals to interact on the site, including chat, messaging, email, video, voice chat, file sharing, blogging and discussion groups, and they have been the flavour of the month in the internet world for the last couple of years.

## Attracting eyeballs

The reason for this is simple: they attract large numbers of loyal users who frequent them to keep up with old friends or make new ones, in exchange for which they surrender all kinds of information about their likes and dislikes, which advertisers can use to target their eyeballs each time they visit the site.

The acclaim for such ventures as Facebook and MySpace has not been universal, however. Employers fret that, with so many of their workers requiring internet access to do their jobs, they need some means of curtailing how much time they can spend, during office hours, on social networking sites.

David Kelleher, a communications and research analyst at GFI, which develops a wide range of infosec products,

**"Organisations should proactively update their corporate policies to include social networking and other aspects of acceptable use related to the Internet and electronic communications"**

acknowledged the benefits of such sites, but also enumerated the problems they bring. "Social networking sites, while encouraging contact building and, as some have suggested, providing a fantastic opportunity for online marketing and recruiting, are the root of four problems:

- loss of productivity;
- impact on network resources as bandwidth is eaten up;
- the threat of social engineering and phishing resulting in data or identity theft; and
- the risk of malicious material finding its way into the corporate network."

According to a study undertaken by information security consultancy Global Secure Systems and the organizers of the Infosecurity exhibition, the use of such sites is costing UK business an estimated \$12.5bn per annum in terms of reduced output. Another study has shown that employees spend at least 30 minutes a day visiting these sites. In some cases, employees admitted spending up to three hours of their working day taking care of their online profile. The question that is being asked is: should employees be allowed to use social networking sites, or extending the options, personal email and personal affairs, such as online banking?

## Should businesses block social networking?

Since the early 1990s, the UK government's Department for Business, Enterprise & Regulatory Reform (BERR) has commissioned a survey, every two years, on the state of information security in UK businesses, and will publish the 2008 survey at Infosecurity. Chris Potter, the PricewaterhouseCoopers partner leading the survey for BERR, commented that "restricting which staff have access to the Internet used to be quite common, but has dropped significantly over the last two years as companies' dependence on web-based applications continues to grow."

This year's report will show that 9 per cent of UK companies do not give any staff access (roughly the same as in 2006), but among those that do, the proportion restricting access to some staff only has nearly halved (from 42 per cent to 24 per cent).

However, there have been other changes: two-thirds of companies that grant staff access to the internet have an acceptable usage policy, and two-thirds of those require staff to acknowledge that they have read the policy before they get that access. As for so-called "inappropriate sites," the survey will show that only 38 per cent of companies that grant staff access to the Internet block access to inappropriate sites, though 81 per cent of companies with more than 250 employees do so.

Now companies are asking themselves whether the social networking sites should be classified as inappropriate, said Potter. "Increasingly, companies are looking at whether they should be blocking access to social networking sites (such as MySpace, Facebook and Bebo)."

"Many of these sites can provide legitimate business benefits, such as sharing experience with other businesses," he went on. "However, many companies have found that the addictive nature of these sites can adversely impact staff productivity. In addition, businesses are

becoming increasingly concerned about what is being said about them on these sites, and some have experienced leakage of confidential information."

Mark Sunner, chief security analyst at MessageLabs, a UK-based provider of security services to corporate customers on email and Web traffic, counselled, "organisations should proactively update their corporate policies to include social networking and other aspects of acceptable use related to the Internet and electronic communications."

Where abuse of social networking sites is a real concern, he went on, "businesses should consider a combination of the right technology, user education and clear policy guidelines to mitigate the risks and manage the situation."

## Security

Then there are the security threats. "Social networking sites may feel like the virtual equivalent of gathering friends at a party or a local bar to swap stories, rant about politics, or talk about music," said Mike Shema, a Web application security researcher at Qualys, a company that provides information security as a managed service. "Yet such a metaphor obscures the risk these sites can pose to computer security, privacy, and personal safety."

He proceeded with a series of troubling questions. "Do you know who your friends are?", "Do you know whose else knows that?", or even, "Do you know what's happening to your web browser?," he mused.

PwC's Potter cited an example of how innocent, and apparently legitimate use of a social networking can have unforeseen consequences. "IT staff at an insurance company used an Internet chat room to help them solve technical issues. However, this resulted in them inadvertently disclosing the company's security set-up and configuration in a public forum."

## A target for malware

Shema at Qualys highlighted the

anonymity afforded by social networking sites, an aspect law enforcement agencies have already called attention to: they can enable a paedophile to masquerade as a fellow teenager to groom unsuspecting victims, for instance.

MessageLabs' Sunner pointed out that the sites are also heaven for writers of malware, given their popularity and the fact that many visitors won't be tech-savvy enough to protect themselves against potential threats.

"The rapid adoption rate of social networking sites such as Facebook has inevitably been exploited by cyber criminals intent on adding the content in these sites to their portfolio of tools. As we have seen in the past, mass adoption of new communication or web-based tools is often followed by a rise in the number of threats against it and the 'Facebook' effect will present new challenges to corporate and personal online security," Sunner argued.

"Many consumers may have only just made their first foray into this new and exciting internet 2.0 development—the last thing they will be expecting, and therefore not vigilant against, is that the same water which they treat as entertainment is already muddied with the kind of individual that makes a career out of identity theft spam and phishing."

## Web 2.0

Yuval Ben-Itzhak, chief technology officer of Israeli security vendor Finjan, said the move by malware writers to get into social networking sites was part of a broader process in which they are starting to adopt so-called "Web 2.0" technologies, which are new capabilities in the areas of multimedia and interactivity that Web designers have been using for the last couple of years.

"As email-borne attacks continue to diminish (except for spam) and the Web consolidates its claim as cybercriminals' favourite vector of attack, the Web channel will continue to evolve," he argued. "Finjan believes that the stage is

set for cybercriminals to leverage Web 2.0 technologies such as RSS feeds, social networks, blogs and mashups to reach new levels of technological sophistication. New types of upgraded attacks, such as Trojan 2.0, will use the web as a control channel for communicating with botnets, taking advantage of the very trust that users have been conditioned to place in their traditional security vendors (e.g. anti-virus, URL reputation, etc)."

## Mugged in the ether

David Harley, research author at US anti-virus developer ESET, said the real problem with social networking sites isn't one of technology at all, but rather of cultural expectations. "Problems with Myspace and YouTube attract a lot of attention," he began. "The underlying problems, though, have less to do with specific technology than with popular mindsets: the expectation of privacy in corners of the internet where none exists, and willingness to move from real-world malice to unexpected virtual equivalents. People just don't seem to expect to be mugged in Second Life, or phished in World of Warcraft."

William Pound, VP of international operations at Absolute Software, which develops technology for tracking stolen PCs and laptops, highlighted yet another problem with social networking: the temptation to be indiscreet. "Sites such as Facebook keep people connected and in touch, but it is all too easy to become complacent and forget about the implications of posting personal, often sensitive information, online," he commented. "Putting personal information online means that people understand everything from what school you went to, to where you work, to what you may or may not be up to on a Friday night and even your relationship status. Researching these social networking sites has even become part of the process that employers undertake when looking at prospective candidates and once up there, the information cannot be deleted."

## COMMERCIAL FEATURE

# New defence strategy to battle the current e-crime wave

By Yuval Ben-Itzhak, Chief Technology Officer, Finjan [www.finjan.com](http://www.finjan.com)

E-crime has evolved into a booming cybercrime business. Viruses, malware and online crime have moved from vandalistic hacking into a major shadow economy that closely mimics the real business world, including profit-driven organized cybercrime. Money is driving the growth of targeted attacks against financial institutions, enterprises and governmental agencies. The financial damages from security breaches will keep on running into millions of pounds.

Cybercriminals use the Web as a highly effective attack vector for a wide range of illegitimate and malicious activities, including identity theft through keylogging, financial fraud, espionage, and intelligence gathering. Their operations function as international organized crime networks which makes it hard to catch them, let alone to prosecute.

In 2008, we have seen the continued development of sophisticated Criminal-2-Criminal (C2C) business models. These mature business models operate on two levels. Crimeware developers are supplying "Crimeware Toolkits" to other criminal elements to be used for attacks. These "how to..." packages instruct its users step-by-step how to infect a system and then retrieve data for financial gain. But criminals can also go the old-fashioned way: purchasing data collected by Trojans, keyloggers and other types of Crimeware. These crime pros use robust and scalable Crimeware that gives them maximum flexibility in terms of command and control.

One of the main reasons why e-crime remains so profitable is the success rate of Trojan technologies, using Web 2.0 as the main attack vector. By using silent installations and drive-by downloads, PCs and networks have successfully been infected. These "Trojan

2.0" attacks combine various Web services to heighten their infection ratio. At the same time, they substantially reduced their chance of being detected. These Trojans use legitimate websites and domains for distributing instructions to botnets, which makes it look like regular Web traffic. To make things even more complicated, evasive techniques (such as the use of obfuscated codes) is deployed to bypass security applications. In short, any organization, company, enterprise or business with Internet access is a potential and prime target—regardless of its size or location.

A striking example is the wave of attacks that came from China in late 2007 and continue into 2008. Malicious content was distributed using obfuscated code and a network of websites to bypass traditional information security technologies. One of the websites that was (ab)used to distribute the Crimeware belonged to a Chinese government office. It illustrates that cybercriminals not only successfully attack governmental websites, but also turn them into "cyber crime tools". Due to its high success rate, we see more of these kinds of attacks using infected legitimate websites. A recent example is the Forth Road Bridge's website, where cybercriminals deployed the Neosploit Crimeware Toolkit, using obfuscated JavaScript, for their attack.

It is clear that traditional security solutions, such as anti-virus, URL filtering or reputation services, will become more and more limited in their ability to handle the latest and highly complicated cybercrime attacks. Traditional security technologies are not equipped to deal (let alone prevent) these threats. To meet the growing demand for more effective protection, the security industry must close the gap between these new attack techniques and the conventional defence strategies.



The optimal way to do this is concentrating on real-time code inspection technologies.

These technologies can effectively protect networks against such attacks, since they analyze each and every piece of content regardless of its source. They are therefore able to detect malicious codes without using signature updates or databases of classified URLs.

With the use of active real-time code inspection, entities can be sure that no malicious content will enter their corporate networks, even if the origin is highly respectable and trusted website.

Finjan will exhibit at Infosecurity Europe 2008 at booth F190. Yuval Ben-Itzhak will speak at the Technical Stream Seminar on "How to defend your organization in the new Web 2.0 Cybercrime world".

**finjan**  
Vital Security  
securing your web

**eset** we protect your digital worlds™

A new way to think smart

**ESET® Smart Security**

Intelligent protection for your PC

There are many software security solutions to choose from but only one can actually think.

Powered by ThreatSense® technology, ESET Smart Security anticipates potential dangers, doesn't slow systems down and excels in proactively protecting your computer. It's smart.

Antivirus + Antispyware + Antispam + Personal firewall

For Antivirus + Antispyware only, try **ESET NOD32 Antivirus v3.0**

Call 0845 838 0832 or download at [ESET.co.uk](http://ESET.co.uk).

**Come and see us at Infosec Stand F140**

ThreatSense  
NOD32

© 2007 ESET. All rights reserved.  
ThreatSense, Smart Security and Antispyware are registered trademarks of ESET.

# Ouch!



Security breaches are painful - Anything which destroys the data you rely on, breaches your confidentiality or affects your customers will hurt. Siemens can help you manage security to reduce the likelihood of something bad happening; we can test your systems and identify key vulnerabilities. On the other hand, if you decide to live dangerously, our incident management experts can help pick up the pieces.

Start right now! Visit Siemens at Infosecurity Europe, 22nd-24th April at Olympia, on stand G170, to discuss your security issues.

Communication for the open minded

Siemens Enterprise Communications  
[www.siemens.co.uk/security](http://www.siemens.co.uk/security)

**SIEMENS**