THE MAGAZINE OF THE BCS SECURITY FORUM

iSNOW

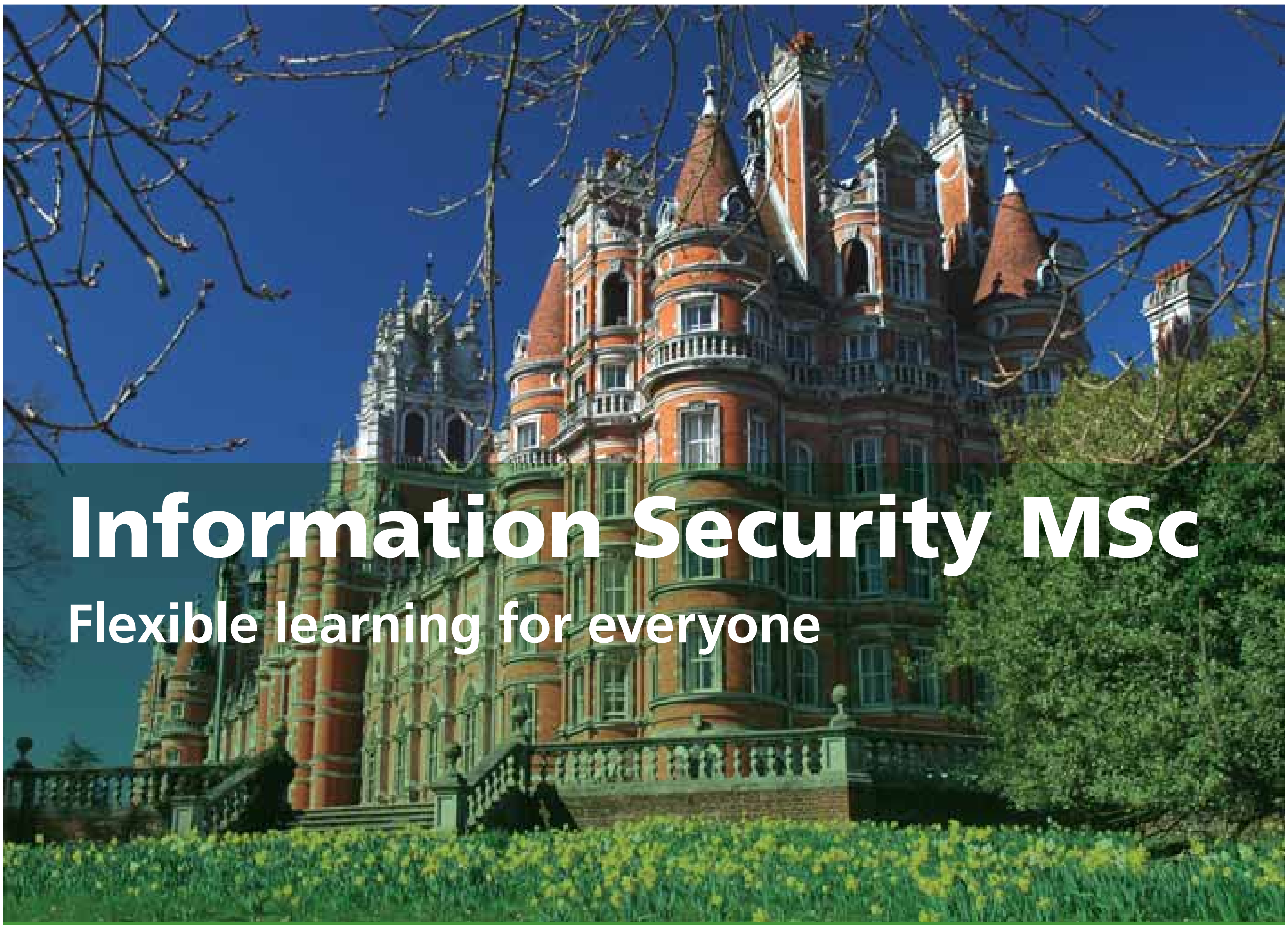
AUTUMN 2009

www.bcs.org/security

INSIDER THREATS

Deal with prying employees and **keep** your data safe

bcs
The Chartered Institute for IT



Information Security MSc

Flexible learning for everyone

We have extended the way in which Royal Holloway's internationally recognised MSc is offered.

- **CPD/CPE Modules:** Most MSc modules are now available as stand-alone courses of one week's duration (Block Mode). These modules may be taken with or without an examination.

As a result the MSc now has the following traditional delivery modes:

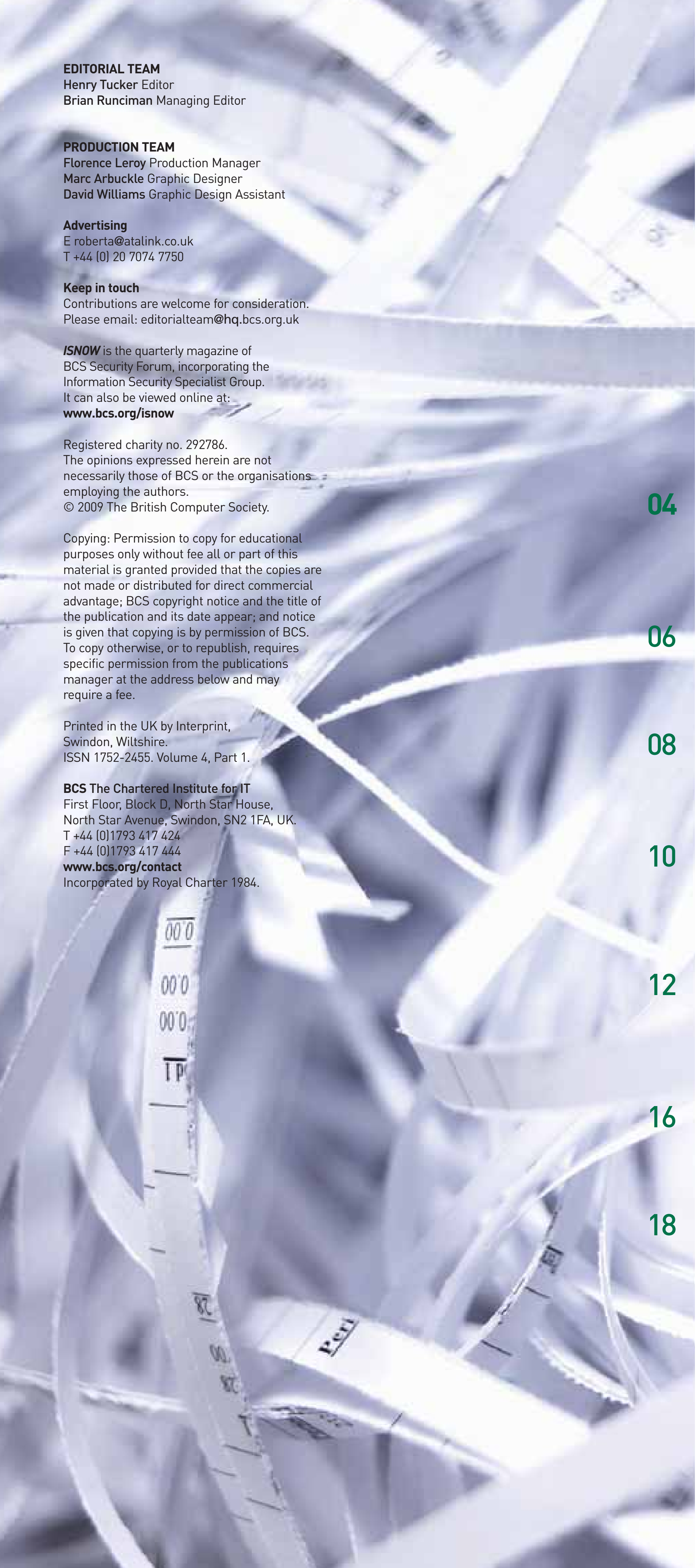
Full-time, one year, on campus; **Part-time**, two years, on campus; **Block Mode**, two years, on or off campus; **Distance Learning**, up to four years via the Virtual Learning Environment.

The introduction of CPD modules has enabled us to introduce even more flexibility into our methods of delivery.

- **Latest innovation** – 'Mix and Match' degree programmes. It is now possible to obtain the MSc by accumulating modules by any delivery method listed above (maximum period seven years).
- **Postgraduate Diploma** – each module is also available in condensed mode and taught as a one, two or three-day training course offered by QCC Training Ltd. Students may follow a structured programme of these courses and then undertake an MSc level project to obtain the Postgraduate Diploma in Information Security.

Royal Holloway
University of London

Information Security Group
www.isg.rhul.ac.uk
p.stoner@rhul.ac.uk
z.ciechanowicz@rhul.ac.uk
T: 01784 443101



EDITORIAL TEAM
Henry Tucker Editor
Brian Runciman Managing Editor

PRODUCTION TEAM
Florence Leroy Production Manager
Marc Arbuckle Graphic Designer
David Williams Graphic Design Assistant

Advertising
E roberta@atalink.co.uk
T +44 (0) 20 7074 7750

Keep in touch
Contributions are welcome for consideration.
Please email: editorialteam@hq.bcs.org.uk

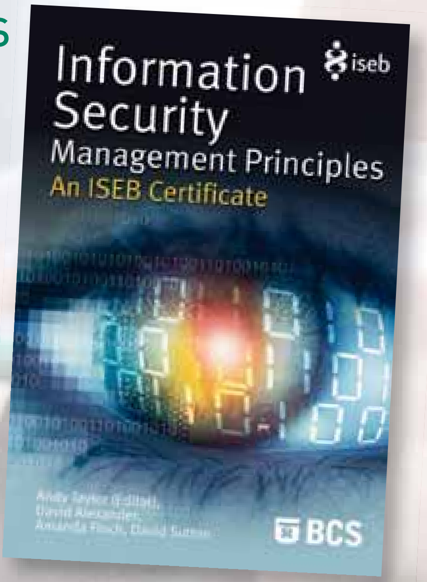
ISNOW is the quarterly magazine of BCS Security Forum, incorporating the Information Security Specialist Group. It can also be viewed online at: **www.bcs.org/isnow**

Registered charity no. 292786.
The opinions expressed herein are not necessarily those of BCS or the organisations employing the authors.

Printed in the UK by Interprint,
Swindon, Wiltshire.
ISSN 1752-2455. Volume 4, Part 1.

BCS The Chartered Institute for IT
First Floor, Block D, North Star House,
North Star Avenue, Swindon, SN2 1FA, UK.
T +44 (0)1793 417 424
F +44 (0)1793 417 444
www.bcs.org/contact
Incorporated by Royal Charter 1984.

INSIDER THREAT


Information Security Management Principles
An ISEB Certificate
iseb
Andy Taylor (Editor), David Alexander, Amanda Finch, David Sutton
BCS

INSIDER **THREAT**

Gareth Niblett says there are ways to combat the threat of untrustworthy employees.

The insider threat is not new. But when companies seek to make cost savings by divesting themselves of their biggest assets, especially during a recession when uncertainty amongst the workforce is likely to be heightened and financial pressures felt more acutely, the likelihood and impact of the threat may increase.

Normal controls, such as separation of duty, audit and training, may well get left behind as the remaining employees each try to do more, due to necessity and self-preservation. Whereas a company making significant changes should review their risk assessments, which may show increased controls are required.

Taking away data

Research appears to bear out the view that staff will take information when they leave a business, and may also exploit that information in any future role. Indeed, senior management and IT staff seem more likely to take information in their possession, which may be more valuable and accessible due to their roles.

Logic bombs

Recent scandals in Formula 1 have demonstrated the value of competitor intelligence, however obtained, and secret arrangements being exposed. Also, in the last few years there have been a number of cases of logic bombs, left just in case the person lost their job, and passwords being changed on departure.

Robust contracts

When dealing with an insider threat, the whole gamut of people, process and technology controls should be considered, preferably in that order, to help mitigate the risk; including robust contracts, staff screening, training, awareness, information marking, handling, access based on business need, role and least privilege, separation of duties, logging/audit, data loss prevention and so on.

Gareth Niblett is chairman of the Information Security Specialist Group (ISSG). www.bcs-issg.org.uk

FURTHER INFORMATION

Information Risk Management and Assurance Specialist Group:
www.bcs.org/groups/irma

BCS Security Portal:
www.bcs.org/security

ISNOW online:
www.bcs.org/forum/isnow

INSIDE THE INSIDER THREAT

Do you really know who is working for you? Do you trust them? Are they really working for you or someone else asks **Stuart Compton** Security Consultant at SELEX Communications.

The insider attack - it can come from disgruntled employees seeking revenge, those who have financial motives, criminals or foreign intelligence services infiltrating your organisation with the sole intention of stealing your data, or worse. The consequences can be financial or loss of reputation, but in extreme cases can mean the loss of the business itself.

As a security consultant and penetration tester, I have completed hundreds of security assessments for clients. I still find that many organisations focus on the network perimeter, which does little to provide security against the threat of insider attacks.

The insider threat is something that has always existed and will always need to be defended against. The Information Security Breach Survey (ISBS) 2008 shows that in the UK, 62 per cent of the worst incidents reported had an internal cause. In April 2008, an insider at the Sumitomo Mitsui Banking Corporation in London, gained access to the bank's computer network. An attempt was made to pull off what would have been the biggest bank theft in the UK.

Insiders are well placed to potentially carry out an enormous amount of damage to your organisation. The threats are not only from current employees, but also ex-employees who have a working knowledge of the organisation. Current employees have legitimate physical and network access to information. If building and network access (including remote access) is not revoked immediately upon an employee's termination or resignation, then ex-employees represent a potential insider threat.

Therefore, controls need be in place to reduce the insider threat. The foundation stone for ensuring that adequate controls are present is the development and maintenance of security policies. The security policy sets out the role that security has in the organisation, the goals and responsibilities. Additional policies, standards, guidelines, baselines and procedures will support this. Employees must understand the consequences of ignoring these security policies. This is very important as every employee plays a key role in the security of your organisation – it is not just a function of IT.

Acceptable use

One very important policy is the acceptable usage policy (AUP). This is a set of clear rules which cover the most important points about what users are and are not permitted to do with your information systems. It is good practice to ask new employees to sign this before they are given access to information systems.

Through an ongoing security awareness training program, employees can be educated on the threats to the organisation and what security practices they need to incorporate into their roles. Security awareness training can show your employees how information can be unnecessarily passed on through phone conversations, emails and who they should contact if they suspect something suspicious.

Who you are hiring?

Background checks should be carried out before employees start. The terms and conditions of the employment contract should state the responsibilities that your organisation and your employee have for information security. What about when employees resign or their employment has been terminated? All physical and network access (including remote access) should always be revoked upon termination. Company equipment and access passes should be returned and key codes changed to secure access areas.

Ex-employees may have a very good

working knowledge of your procedures. With this knowledge, could they or an associate be successful in calling your help desk to gain information or access to systems? Often a sense of urgency will be used to bypass correct security procedures. This style of attack is known as social engineering, which is the act of manipulating people into performing actions or divulging information. However, if you have security awareness training, a well structured procedure for handling calls and an audit trail, this can mitigate an attack or at least limit the damage.

Back in the 1990s I worked in the city of London and in the evening the chairman would walk around the office checking that staff had cleared their desks. If not, the whole contents went into a black bin bag and the next day, well you had to see the chairman to reclaim your possessions. Extreme as this may seem, a clear desk policy can help to ensure that information is not unnecessarily passed to unauthorised individuals. Look around your office now, are there business confidential or technical diagrams on flip charts, or white boards on the office walls? These should never be accessible to unauthorised individuals.

In April 2008, an insider at the Sumitomo Mitsui Banking Corporation in London, gained access to the bank's computer network. An attempt was made to pull off what would have been the biggest bank theft in the UK.

They say 'one man's rubbish is someone else's treasure' this can never be more true when it comes to your organisations rubbish. Who exactly is diving into your rubbish and where is it stored? Rubbish can contain all sorts of interesting information such as old telephone lists and organisational structure charts. 'Dumpster divers' will sift through rubbish to find items that may be of interest to them and use it to build a profile of your organisation. Providing cross-cut shredders to employees is an excellent step to reducing this information leakage.

In the office environment, some simple physical controls are often overlooked, for example, storing removable media and confidential documents in a locked cabinet at the end of each day. Door entry controls, security guards, CCTV and motion detectors are among physical controls that can be used to act as a deterrent or response to suspicious activities.

If any one individual in your organisation has the ability to compromise your security controls then perhaps you should consider implementing separation of duties. This will reduce the likelihood of an internal attack as for the attack to be successful, employee collusion is required. All users in your organisation should have a unique identifier to access information systems and if any unauthorised activities occur, logging, monitoring and auditing will help any detection and investigation.

For further information please visit:
www.bcs.org/security

INSIDER THREAT

MYTH **OR** REALITY

There have been a number of articles over recent months about the insider threat to security. So what is the insider threat, and has it increased asks Neil O'Connor from Activity.

Media interest has concentrated on the risks created with decreased job security and growing redundancies. The main threats highlighted have been the theft or the deliberate destruction of information in cases of redundancy.

So have these threats increased in the current economic climate? Although they are more aware of the potential problems, we do not have any evidence from our clients they have had data stolen. Having said that, it takes considerable effort to detect the misuse of information of which an employee has access to perform their job.

Real threats

In our opinion there is no real evidence of an increase in the insider threat as defined above - this could be due to the theft of information going undetected. However, in context to the overall threats to information security, people in the organisation remain the biggest issue. So what are the real threats concerning our clients today?

- theft of information - as discussed above, the theft of information is a concern;
- loss of information - it is all too easy to accidentally email the wrong document to a client, or lose a memory stick with valuable data on it;
- unavailability of information - a substantial risk is the denial of access

to systems or information such that business operations are disrupted;
- loss of reputation - the loss of portable IT assets such as laptops, CDs, memory sticks etc containing company information, or even worse client information, can lead to high profile naming and shaming.

Countering the threats

Some simple security measures can help counter threats posed by employees. Every business has its own particular needs and priorities – there is no one size fits all solution. In putting together the list of countermeasures below, I have assumed that basic security measures such as firewalls, anti-virus, user accounts with unique IDs and passwords are in place.

Security risk management

In order to justify and prioritise the implementation of security controls, it is essential to have a security risk management process. This should:

- identify the key information assets in the business, and the impact of their compromise;
- rank risks to the organisation;
- be regularly updated from audits, reviews and security incidents;
- escalate into corporate risk assessment processes.

Information security management

In order to implement security risk management, you need an information security management system (ISMS) such as the International Standard for Information Security Management ISO 27001. The ISMS should:

- set security objectives;
- identify security responsibilities;
- implement a plan to meet those objectives;
- measure those objectives;
- measure the effectiveness of security controls;
- gather information on security incidents;
- audit security;
- review the above measures to update the security risk assessment and identify any further security controls required.

Training and awareness

Training and awareness is a key security countermeasure. This should cover:

- The acceptable use of IT resources (internet, email etc) tying in with corporate HR policies, and advice on the handling of IT assets, and secure practices such as the use of passwords. In addition, it should provide information on who is responsible for security and who to contact with queries.
- Specific training on handling procedures should be given to people with access to personal information.
- What is not acceptable when using IT systems, what auditing is in place to detect misuse and the consequences of misuse. Again, this should be aligned with corporate HR policies.

To prevent loss of systems or the denial of access to information, the overall integrity of information systems needs to be maintained.

Privilege and audit

One of the key steps to counter information theft is to limit access to it with an access control system. To do this, you need to identify what different types of information you hold, and who needs to access that information. This does not solve the theft problem, but it does limit your exposure to it.

The next step is to audit who actually accesses the information. If users believe that there is a likelihood of improper use of information being detected and acted upon, then they are less likely to take the risk of being caught.

To prevent loss of systems or the denial of access to information, the overall integrity of information systems needs to be maintained. A key concern is the presence of development systems on operational networks. This introduces potential vulnerabilities due to developers needing unrestricted access to servers, peripherals, operating systems and so on that are best managed by separating development and operational systems. Malware can infect organisations in spite of anti-virus deployment. The lesson to be learnt here is to ensure that systems are as resilient as possible to a virus outbreak. There are two key controls: patching and network architecture. Internal servers should be kept up to date with security patches. Segregated network architecture will help to restrict any malware outbreak to a segment of the network.

End-point protection

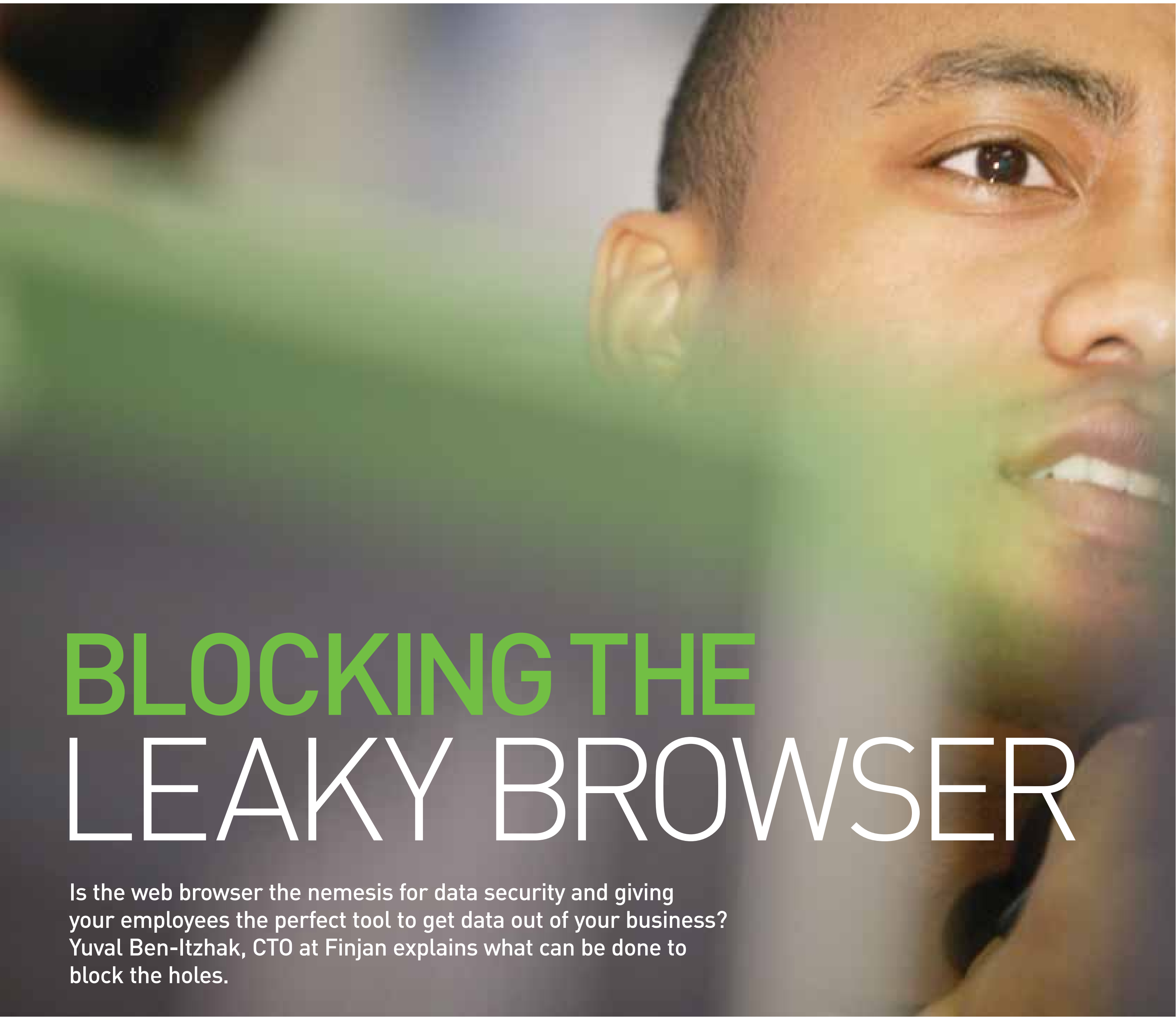
A security control now implemented in many organisations is end-point protection encompassing the encryption of portable IT equipment and writeable media, control of the connection of peripherals to devices, and control over the ability to write to media.

End-point protection can be used to counter several of the threats posed by people, notably:

- the loss of information, and more importantly the risk of loss of reputation;
- control over peripherals and media reduces the risk of the introduction of malware, and limits the potential for the theft of information.

While we have not seen evidence of an increase in the insider threat, the people that use our IT systems continue to pose one of the biggest risks to information security. The threats posed by people can be mitigated by a range of measures that need to be tailored to the particular needs of the organisation using a security risk management process.

For further information please visit:
www.bcs.org/security



BLOCKING THE LEAKY BROWSER

Is the web browser the nemesis for data security and giving your employees the perfect tool to get data out of your business? Yuval Ben-Itzhak, CTO at Finjan explains what can be done to block the holes.

The incidents of data intentionally or unintentionally leaving corporate networks are rising. The CSI Computer Crime and Security Survey in 2008 showed that 44 per cent of the polled companies registered data leakage to be the second biggest problem of their corporate IT security. In a survey conducted among German companies, less than 25 per cent were found to use HTTP traffic monitoring systems for protection from confidential data leakage.

An older survey conducted in the US, investigated how data is being leaked through communication tools. Survey results showed that HTTP was the leading avenue for data leakage. Furthermore, it was found that customer data represented the vast majority of data leaked to unauthorised parties, followed by confidential information and Protected Health Information (PHI).

Data Loss Prevention or Data Leakage Prevention (DLP) is now a major issue, affecting the bottom line of enterprises. According to recent research by the Open Security Foundation, the total number of data loss incidents in 2008 has risen by 2,600 per cent compared to the total number of data loss accidents in 2004.

Not only companies, but also governmental agencies are at risk. One of the latest incidents occurred in May 2009 consisting of accidental data leakage. Some parties received electronic data consisting of the latest unemployment and average earnings figures from the Office for National Statistics (ONS) before their official publication date. The ONS was forced to officially release these figures ahead of time, resulting in the Sterling bouncing higher. (The released data showed a smaller than expected rise in claimant count unemployment even as the overall unemployment rate rose to 7.1 per cent). This incident is the latest addition to string of data breaches the British government has suffered over the past two years. They include leakage of secret intelligence files, the details of every prisoner in England and Wales, and information about thousands of potential army recruits.

Data leakage has grown into a global problem, as the following incidents show.

- In February 2009 in Hong Kong, more than 60 restricted government documents were leaked on the internet through file-sharing software FOXY, forcing the Privacy Commissioner for Personal Data Roderick B. Woo to take immediate action.
- At the start of 2009, Dartmouth

Organisations around the world have become aware of the need to protect their outbound data in transit. This growing demand has resulted in a booming market for DLP solutions; expected to reach $2 billion by 2012.

College researchers (US) searched file-sharing networks for key terms associated with the top 10 publicly traded health care firms in the country. Over a two-week period, they discovered numerous sensitive documents, including a spreadsheet from an AIDS clinic with client details; hospital databases containing detailed information on more than 20,000 patients; a 1,718 page document from a medical testing laboratory containing patient data; and more than 350MB of sensitive patient data from a group of anaesthesiologists.

- In April 2009, a data leakage incident occurred in a Prague hotel (Czech Republic). The flight details and passport numbers of around 200 EU leaders, including those of a Finnish state delegation, were leaked by accident. The data was related to a recent EU-US summit held in Prague and attended by U.S. President Barack Obama.
- In April 2009, an employee of Mitsubishi UFJ Securities, who was Deputy Chief of its computer department, sold personal data on more than 49,000 of its customers to three dealers who specialise in personal data lists, which in turn sold them to more than 80 real estate agents and other firms.
- In March 2009, a spreadsheet containing customer data of Kabel Deutschland (a German provider of internet, cable TV and telephony) was leaked to questionable call centres.

Data leakage prevention (DLP) is gaining more and more attention as governments and organisations also realise the danger to their compliance status and to their commercial health. Web 2.0, especially peer-to-peer (P2P) networks, provides conduits through which information can leak. Especially intellectual property and patient information disclosed on P2P networks are at risk. IBM's Many Eyes, which is essentially a mashup application for visualising data, contains a lot of data that probably shouldn't be there, such as sales forecasts, corporate income statements, and data from government agencies, including the CIA.

Although most data loss is unintentional, we see a growing number of intentional data loss incidents. During mergers, layoffs and reorganisations, corporate data are vulnerable. An employee could leak data for their personal benefit. Such data includes customer lists, intellectual property (IP) and other business data that could be useful for the (former) employee. Organisations around the world have become aware of their need to protect their outbound data in transit. This growing demand has resulted in a booming market for DLP solutions; expected to reach $2 billion by 2012.

Protecting loss of data in transit is complicated, even more so when malware is involved as in the case of Trojans phoning home. The optimal way to prevent data leaking out of the network is the use of a gateway-based web security solution. Such solutions consist of dedicated hardware/software platforms. They analyse network traffic to search for unauthorised information transmissions, including IM, FTP, HTTP, and HTTPS. When selecting a DLP solution, an enterprise needs to focus on the following elements:

- All outbound communication should be analysed in real time and identified by their true content payload, not just by their file extensions. True content type detection capabilities prevent selected file types from leaking out or being downloaded by users.
- Administrators should be able to set policies based on dictionaries/lists containing words or formats (such as customer or employee information with names, addresses, social security numbers and other identity-related information) that should be protected. The solution should also enable lexical analysis and dictionaries/lists for words or formats relating to company-specific sensitive information (e.g., intellectual property (IP), financial information).
- A policy-based management is needed to setup and enforce granular rules per specific user or per user group (e.g. sales, marketing, R&D, finance, legal).
- The ability to set up compliancy lists for PCI, HIPAA, GLBA, SOX, CISP, FISMA, governmental regulations, etc. is needed, especially for publicly traded companies, financial institutions, and healthcare providers.

Numerous enterprises are now looking for DLP as an integral part of their web security solution rather than dedicated DLP solutions which are available as a stand-alone solution. This enables administrators to turn specific features on and off, deploy security features in stages and even disable superfluous functions. This type of integrated DLP solution prevents intentional (as a result of malicious activity) and unintentional data leakage with low cost of ownership.

For further information please visit:
www.bcs.org/security

STOPPING THE SNOOPERS

If you are worried that your staff may steal your company's data, **Mark Fullbrook** has five steps to protect your organisation from desperate employees.

According to figures released in June 2009 by the Office for National Statistics the number of redundancies for the three months to April 2009 was 302,000, up 36,000 over the quarter and up 191,000 over the year. This is the highest figure since comparable records began in 1995. However anxious these times may be for employees, nervously looking round to see where the axe will fall next, employers should not be complacent and expect loyalty in return for a regular pay packet. In fact the opposite could well be true – as the saying goes 'desperate times call for desperate measures'.

In a recent survey into 'The recession and its effects on work ethics' carried out by Cyber-Ark amongst 250 office workers in London's busy Canary Wharf, a staggering 60 per cent admitted they would take valuable data with them, if they could get away with it, were they faced with redundancy or the sack. Remarkably, 40 per cent confessed to having already snooped around the networks and downloaded sensitive company secrets from under their bosses nose in anticipation that they could lose their job. Top of the list of desirable information to steal is customer and contact databases, with plans and proposals, product information, and access/password codes all popular choices and as having a perceived value, either monetary to an unscrupulous third party or as a negotiating tool in securing a new position.

In a separate Cyber-Ark global survey into 'Trust, Security and Passwords' of more than 400 senior IT professionals both in the US and UK, mainly from enterprise class companies, 35 per cent of IT workers admitted to accessing corporate information without authorisation. The types of information this audience would target was proprietary data and information that is critical to maintaining competitive advantage and corporate security. Ominously, 1 in 5 companies confessed to having experienced cases of insider sabotage or IT security fraud.

When staff take data and cause a security incident, it tends to be filed away as an example of an employee gone bad. In reality it constitutes a failure of the organisation to uphold its responsibility on behalf of the business to manage, control and monitor the power it provides to its employees and systems or indeed have any controls actually in place to actually manage and control staff from causing breaches. The failure stems from the 'perception of control' an organisation has over their most sensitive networks, systems and devices versus the stark reality that this control is most often not in place across the organisation. So, what can be done to protect sensitive data from an increasingly unsettled, and to some extent desperate, workforce?

Trust is not a security policy

To significantly cut the risk of these insider breaches, employers must have appropriate systems and processes in place to prevent prying personnel.

One approach to address this challenge is a privileged identity management holistic approach using solutions such as digital vaults, especially valuable for users with high levels of enterprise/network access as well as those handling sensitive information and/or business processes. Instead of trying to protect every facet of an enterprise network, digital vault technology creates safe havens, distinct areas for storing, protecting, and sharing the most critical business information, and provides a detailed audit trail for all activity associated in these safe havens. This encourages secure employee behaviour and significantly reduces the risk of human error.

For organisations serious about preventing internal breaches, be they accidental or malicious, here are five steps to protecting company data from desperate employees tempted to steal secrets:

Step 1: establish a safe harbour

By establishing a safe harbour, or vault, for highly sensitive data (such as administrator account passwords, HR files, or intellectual property including corporate databases), security is built directly into the business process independent of the existing network infrastructure. This will protect the data from the security threats of not only nosy employees snooping around for information they should not be privy to, but also from hackers.

A digital vault is set up as a dedicated, hardened server that provides a single data access channel with only one way in and one way out. It is protected with multiple layers of integrated security including a firewall, VPN, authentication, access control, and full encryption. By separating the server interfaces from the storage engine, many of the security risks associated with widespread connectivity are removed.

To cut the risk of these insider breaches employers must have appropriate systems and processes in place to prevent prying eyes.

Step 2: automate privileged identities and activities

Ensure that privileged administrative and application accounts, and their underlying passwords are actively managed, secured, changed regularly, highly guarded from unauthorised use, and closely monitored, including full activity capture and recording. Once these privileged identities are being managed, make sure to proactively monitor and report actual adherence to the defined policies, and adopt the well-accepted security axiom of 'Trust, but verify'. This is a critical component in safeguarding organisations and helps to simplify audit and compliance requirements, as companies are able to answer questions associated with who has access and what is being accessed.

Step 3: identify all your privileged accounts

The best way to start managing privileged accounts is to create a checklist of operating systems, databases, appliances, routers, servers, directories, and applications throughout the enterprise. Each target system typically has between one and five privileged accounts. Add them up and determine which area poses the greatest risk. With this data in hand, organisations can easily create a plan to secure, manage, automatically change, and log all privileged passwords.

Step 4: secure embedded application accounts

Up to 80 per cent of system breaches are caused by internal users, including privileged administrators and power users, who accidentally or deliberately damage IT systems or release confidential data assets. Many times, the accounts leveraged by these users are the application identities embedded in scripts, configuration files, or an application. The identities are used to log into a target database or system and the fact that these credentials, are traditionally hard-coded, in clear-text and usually never changed is often overlooked within a traditional security review. Even if located, the account identities are difficult to monitor and log because they appear to a monitoring system as if the application (not the person using the account) is logging in.

These privileged, application identities are being increasingly scrutinised by internal and external auditors, especially during PCI- and SOX-driven audits, and are becoming one of the key reasons that many organisations fail compliance audits. Therefore, organisations must have effective control of all privileged identities, including application identities, to ensure compliance with audit and regulatory requirements.

Step 5: avoid bad habits

To better protect against snoopers, organisations must establish best practices for securely exchanging privileged information. For instance, employees must avoid bad habits (such as sending sensitive or highly confidential information via courier). IT managers must also ensure they educate employees about the need to create and set secure passwords for their computers instead of using sequential password combinations or their first names.

The risk of internal data misuse from snoopers can be significantly mitigated by implementing effective policies and technologies. In doing so, organisations can better manage, control, and monitor the power they provide to their employees and systems and avoid the negative economic and reputational impacts caused by an insider data breach. It would be unthinkable to leave money on a desk, an obvious temptation to anyone passing, instead it is always safely locked away. The time has come for companies to give sensitive information and key systems the same consideration, and as always, 'trust, but verify'.

For further information please visit:
www.cyber-ark.com

THE SHIFTING SANDS OF **PRIVACY**

Organisations need to balance their security needs but also monitor employees' activities whilst at the same time respecting their rights to privacy says **Adam Bosnian,** Cyber-Ark Software.

Privacy is considered a human right in Europe and to this extent organisations have focused on protecting the privacy of their customers' data. However, there's a blurring of lines between monitoring employee's activities to make sure that the organisation is secure, with the employees perception of a 'right to privacy.'

To ensure the security of personal data, organisations have grasped the need to manage the people within the organisation by restricting the data they have access to, specifically, providing access only to the information needed to complete their specific business related activities. While this controlled access is in line with the fundamental security tenet of 'Least Privilege', in order to ensure the integrity of its information, an organisation also needs to be able to identify if someone has done anything that they shouldn't have done with this information, or the underlying systems. For this reason companies need to know: who is logging in to the system, what they're doing and if they had the rights and approval to do so. This is managed in order to deliver another fundamental security tenet 'trust, but verify', so that the organisation can justify the activity based on the final piece of the puzzle, the captured and recorded activity log.

As raised above, the actual identity of the users requiring access to key information is a vital element of robust, secure process. To that end, it is important to note that with many 'privileged' accounts within an organisation, there is no named, specific user. Instead, with these powerful, built-in accounts found in all applications, systems, operating systems, databases et al, the risk of a generic system administrator account - designed to be used by many people without specifically recording the actual identity of any of them, is evident. In this case, a secure company must have a way of knowing who is behind a generic identity and collect subsequent activities in the same way.

An integral part of an effective corporate governance regime includes provisions for civil or criminal prosecution of individuals who conduct unethical or illegal acts in the name of the enterprise. It is therefore elementary that organisations must monitor and record employees conduct, compiling an audit trail which proves compliance with policies and takes preventative measures for data breaches.

As the value in collecting the data is for the purpose of identification, only knowing that someone is accessing, changing or removing valuable information isn't enough. Organisations need to be able to pinpoint the individual, the associated activity, and whether this activity is in line with policy.

Do employees have a right to privacy?

Historically organisations in the UK have fallen foul of the Data Protection Act (DPA) for failing to adequately protect customers' information – and this is replicated across the globe. However, even taking the security requirements and practices discussed previously, employees also have a right to the same protection for any identifiable data that is collected as part of audit trails and governance compliance.

Security and privacy are not, and should not be seen as, mutually exclusive or opposing concepts

The Wikipedia definition of information privacy, or data privacy, is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. Privacy concerns exist wherever personally identifiable information is collected and stored - in digital form or otherwise.

Globally there are a number of different legislations that affect the way data is stored and used. The US has deployed a variety of different laws and regulations at both the national and state level that seek to provide consumer protection in a number of sectors where privacy issues have emerged. Examples include HIPAA, which addresses the requirement for healthcare providers and payers to keep personal health information (PHI) secure and private, as well as other legislation requiring the credit card and financial services industry to also protect customers' non-public personal data and financial information such as the Payment Card Industry (PCI) standards and Gramm-Leach-Bliley Act (GLBA).

However, many uses of data fall outside the scope of this existing regulatory structure, and as such, are less strictly regulated. In Europe, The European Union Data Protection Directive (EU DPD) defines fundamental principles for privacy protection and includes mechanisms for cross-border transfers of personal data. Essentially, all principles are similar to the DPA in the UK that states anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate and up to date;
- not kept for longer than is necessary;
- processed in line with your rights;
- secure;
- not transferred to other countries without adequate protection.

Watch them and their right to privacy?

It's important that concerns over privacy do not deflect from the strong case for monitoring employees' behaviour. Carsten Casper, Research Director with Gartner and responsible for the security role in Gartner for IT Leaders in Germany, believes, 'Security and privacy are not, and should not be seen as, mutually exclusive or opposing concepts. Modern legal and technical tools allow a balanced consideration of both.'

Below are guidelines to avoid breaching privacy rights whilst gaining employee support:

1. Put policies in place explaining what is acceptable versus improper activity and/or behaviour – if you don't tell them how can they be expected to know? 'An ounce of prevention is worth a pound of cure.'

2. Educate employees about what's expected from them, and why it's important, to gain their appreciation and support for these important security measures and processes. Many employees may not even realise that their activities can cause a security breach.

3. Inform them that you can, and will monitor them and explain why

   a) It is important that employees understand this works in their interests too as, if there is unacceptable or illegal activity. Through monitoring it will be easy to identify the offender, thus eliminating the finger of suspicion and the ill-feeling it can cause for those not involved and doing the roles in-line with company policies. If they're not doing anything wrong they have nothing to fear.

   b) Employees should be aware that personal activities during company time and/or using company products will also be monitored and recorded so there are no surprises.

4. Capture relevant information
   c) When choosing a solution make sure that what it will capture is accurate, relevant and is kept secure from prying eyes.

5. Recognise that an employee has a right to know what information you have, and be able and willing to access and share it with them.

Carsten concludes: 'Enterprises and individuals should not be forced to achieve security at the expense of privacy, or vice versa.'

Introducing a full lifecycle solution to secure, manage, log and monitor all privileged activity benefits all, whether it be with privileged information, privileged users or privileged processes.

With this type of full security solution in place, as an employee you are comforted by the knowledge that your employer knows you're doing your job line with corporate governance and security policies. As an employer you are reassured by the evidence that proves your employees are doing, and seeing, only what they are supposed to.

As a customer you can trust the organisation to protect your personal information, as they are going to great lengths to ensure any access is secured and proper. Rather than allowing security and privacy to be at odds, following these steps will allow organisations to reduce the security risk whilst mitigating any privacy issues.

For further information please visit:
www.cyber-ark.com

BIOMETRIC SECURITY:
DATA PRIVACY DEVELOPMENTS

Charlotte Walker-Osborn, Partner, Technology Group, Eversheds LLP, considers whether a recent decision in France in relation to biometrics might impact on UK developments.

Biometric security, such as fingerprint identification, iris and retina scanning, face recognition and hand geometry, is becoming increasingly commonplace. A recent decision in France by the CNIL (the French equivalent of the UK Information Commissioner's Office) is likely to be of interest to UK organisations that use or produce such identity verification technology, or are planning to do so.

On 18 June, the CNIL authorised the use of 'palm vein technology' by the Graduate Management Admission Council (GMAC) in respect of its Graduate Management Admission Test (GMAT). The technology uses an infrared light to capture the pattern of palm veins and to generate an encrypted biometric template. It will be used by GMAC throughout the world to check the identity of individuals sitting the GMAT test. GMAC now intends to implement the technology and will file approval requests with the other EU data protection authorities.

The CNIL decided that the palm vein technology complies with the French equivalent of the Data Protection Act 1998 and French privacy law because it does not use trace technology, the image of the palm scan is not stored and the data cannot be read by other devices and, as such, it presents very little risk for civil liberties and fundamental rights.

However, it is worth noting that the CNIL did not give a green light for the technology to be used generally and its authorisation was granted specifically in the circumstances because of the special characteristics of the GMAT exam (sat in 110 countries by 200,000 candidates every year and a high score in one country is recognised in all and gives candidates access to courses - such as MBAs - in elite business schools throughout the world). The specific privacy protection and controls that GMAC will put in place were crucial in obtaining the CNIL's approval.

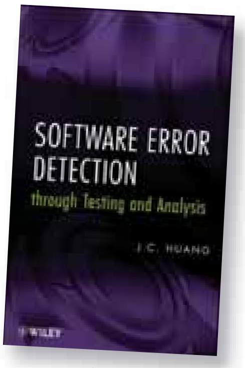
The CNIL's decision means that GMAT could now be approved throughout the EU by the relevant data protection authorities, including the ICO in the UK, as being a data-protection-compliant means of verifying identity and advancing security. In the past, the ICO has voiced its concerns with proposed use of biometric technology (for example, in relation to the national identity card and for use in schools for cashless catering).

However, in the light of the CNIL's approval, and assuming GMAC would agree to similar guarantees and controls in the UK, it is difficult to see how the ICO could object to the use of PalmSecure technology in the context of GMAT. Unlike the National Identity Register, which was to be accessible to several public and private organisations, GMAC's database will be accessible only to itself and the data will be encrypted. A swipe card in the GMAT exam hall is not a viable alternative. For organisations in the UK interested in using this technology, the details behind this approval could usefully guide them as to how to build their offerings. It will also be interesting for us to keep an eye on the adoption of these biometric developments, going forward, as UK citizens.

Please note that the information provided above is for general information purposes only and should not be relied upon as a detailed legal source.

BOOK REVIEWS

Software Error Detection through Testing and Analysis
JC Huang
Wiley
ISBN 978-0-470-40444-7
£53.50



7/10

The author is a professor at the Department of Computer Science at the University of Houston. He claims that the book 'serves as a textbook for students and as a technical handbook for practitioners leading quality assurance efforts.' I am a practitioner in industry and for me this isn't the type of book that most practitioners would find useful.

This book is really aimed at students studying the subject at advanced undergraduate and graduate levels. It could also be used by practitioners implementing advanced testing techniques for application domains requiring advanced levels of rigour, e.g. safety critical systems and defence systems, but that only covers a very small proportion of practitioners.

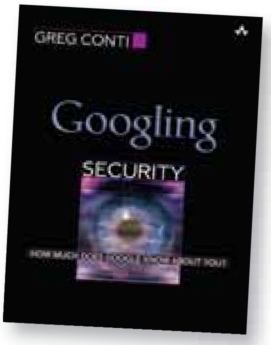
The book does introduce some rigour, concepts, principles and notation to the subject. This, however, is a double-edged sword in that you need to read and understand a 14-page introductory chapter on 'Concepts, Notation and Principles' and a 19-page appendix on 'Logico-Mathematical Background' that consists of mathematics covering propositional calculus, first-order predicate calculus, mathematical induction, matrices and set theory. If you can't cope with such mathematical concepts, then this definitely is not the book for you.

It has a good glossary and bibliography, exercises at the end of each main chapter and an appendix with 50 multiple choice questions for self assessment along with the answers. A disappointment for me is that there is no concluding chapter or discussion at the end of the book.

This is possibly a good book for students, researchers and academics, but a poor book for most practitioners in industry. I say possibly, as how many students can afford to buy a book for £53.50?

Kawal Banga CEng MBCS, CITP

Googling Security:
How Much Does Google Know About You?
Greg Conti
Addison-Wesley
ISBN 978-0-321-51866-8
£31.99



7/10

Google, with its diverse offering of application and services, is being perceived as a serious threat to the privacy of millions of online users. This is precisely the focus of Conti's book: using search, email and instant communications, and web services such as Google Docs/Maps/Earth, online users are leaking an incredible amount of personal information. The issue is addressed in systematic and good detail, using clear and accessible language.

Chapter 1 is a basic introduction to Google and the threat of information disclosure over its various web services. Chapter 2 provides an understanding of the technicalities underlying such disclosure over the ordinary computer and communication usage. Even if readers are familiar with the basics, the two chapters are recommended reading.

Conti presents a detailed breakdown of how personal and behavioural information is disclosed through ordinary activities such as web browsing, search, communications, mapping and web marketing. Each of the services offered by Google in this respect is closely examined from a technical and a legal standpoint. While the author largely concerns himself with Google, such disclosure applies to any web-based entity providing similar services.

Chapter 8 is a very interesting account of Googlebot, some of the insights here are truly novel and worth a read.

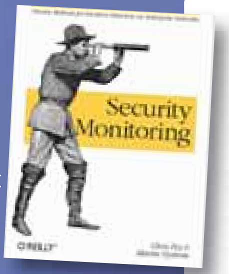
This book is a comprehensive resource on online privacy issues. Every chapter finishes with a short but meaningfully conclusive summary and the author makes an honest attempt to raise awareness of the increasing risks that online users are putting themselves in.

However, greater interactivity and customisation is the essence of web 2.0: there is a trade-off here to be made with security. Also, to single out Google for the focus of this thesis seems unfair.

Siraj A. Shaikh MBCS CITP

BOOK OF THE MONTH

Security Monitoring
Chris Fry, Martin Nystrom
O'Reilly
ISBN 978-0-5965-1816-5
£34.50



9.5/10

Although the authors were associated with Cisco the book doesn't focus solely on Cisco products, but actually presents software from multiple vendors and the methods are vendor independent.

The authors present this subject in a logical sequence, starting with monitoring. The problem with this is that it can actually be counter-productive if the wrong targets and events are monitored, which is essential to help achieve successful monitoring. Various methods are discussed to help identify what are the key targets. Having identified them, the authors then discuss what events should be collected, and the impact of collecting such events.

Now that the key targets have been identified, the authors discuss how such event feeds can be tuned so that real security events can be detected. This includes events from syslogs and logs from databases, Windows, network devices, and the use of NetFlow. Finally, with the events identified and turned into something useful the need to, and ways of, maintaining the whole environment is discussed.

The concluding chapter is aptly titled 'Keeping it real' and provides details of case studies and anecdotes. It also illustrates that security monitoring cannot be done in a piecemeal fashion. The authors state the book is not intended to be an introduction to network security and tools, or system and network administration, stating that some foundational understanding of these areas are required. However, I would argue this is an intermediate level book. Overall it is well written and presented in a clear and logical manner. The authors are knowledgeable, and the advice given is obviously based on sound experience in the field.

Mehmet Hurer B.Sc (Hons) MBCS CITP CEng AIISP

SECURITY: AN HR ISSUE

Security in business comes down to what employees do, which makes it an HR issue argues **John Mitchell,** Managing Director of LHS Business Control.

Organisations spend millions defending their cyber perimeters, but only a fraction of that in protecting themselves from insider threats. This is despite all the evidence pointing to insider threats as being a significant risk area.

We train our staff (and contractors), provide them with the necessary privileges to do their jobs and then we basically forget to monitor them. Where we do monitor it tends to be either spasmodic, or superficial, or both. I was once told by a CIO that 'we have trust someone' and when I asked why he was reduced to incoherent spluttering.

The audit motto by the way is 'trust, but verify'. I was once involved in a job which required us to check a network to detect undesirable images. I discussed it with the CIO and explained that first we would tell everyone of our intentions and then we would do the actual check. My logic being that the advance warning would see an immediate deletion of the embarrassing items. Lo and behold that was exactly what happened and the company recovered about 20 per cent of its total disk capacity without firing a shot. However, I was amazed to find that when we did the subsequent check the only real offender was the CIO himself. At his dismissal hearing I asked why he hadn't taken advantage of the warning. His response was that it never occurred to him that we would check his files. A strange, but not a totally unexpected, response from a senior manager.

I once had to deal with a Chief Executive who shared his access credentials with his secretary despite this being a dismissible offence. His response was similar to the CIO's; the policy did not apply to him. We can control the technology pretty absolutely, but we can only manage the people, but control and management are not quite the same thing.

We manage people by implementing policies, standards and procedures, but until we can implant a controlling chip, which is what most governments would probably like, we are still unable to control them. It's not the computer that steals the money, but the person. It's not the computer that causes the data leak, but the person. A computer does not carry out a denial of service attack unless subverted by a person. That abnormal program termination is caused by the programmer, not the program. The covering of tracks by deleting a log file is person inspired and not the idea of the computer. So people management is really important. Actually, it is quite critical and that is one reason why I have argued, quite unsuccessfully for some years, that security is a human resource challenge. After all, it is HR that conducts the initial background check. It is HR that sets the employment policies and staff review processes and it is HR that drives the termination process. All in all, it is a pretty solid case for HR driving security. Indeed, perhaps the Chief Security Officer (CSO) should be part of HR?

I am aware that neither HR, nor IT, are happy with this idea, but there is no doubt in the mind of the International Standards Organisation that information security is a corporate and not an IT responsibility. Currently, information security tends to be driven by IT and the CSO is usually an IT professional who would see his career prospects severely limited if he were part of HR. Likewise, the HR professionals see technology as an IT responsibility and do not have the necessary knowledge, or inclination to get involved. However, if information is a corporate responsibility, then it stands to reason that information security should be integrated into the business processes with a much enhanced prospect of preventing and detecting insider threats.

Security is really is a soft people problem rather than a hard technological one. People are the soft underbelly of the enterprise and the role of HR is to ensure that processes are in place to manage them.

For more information visit:
www.bcs.org/security

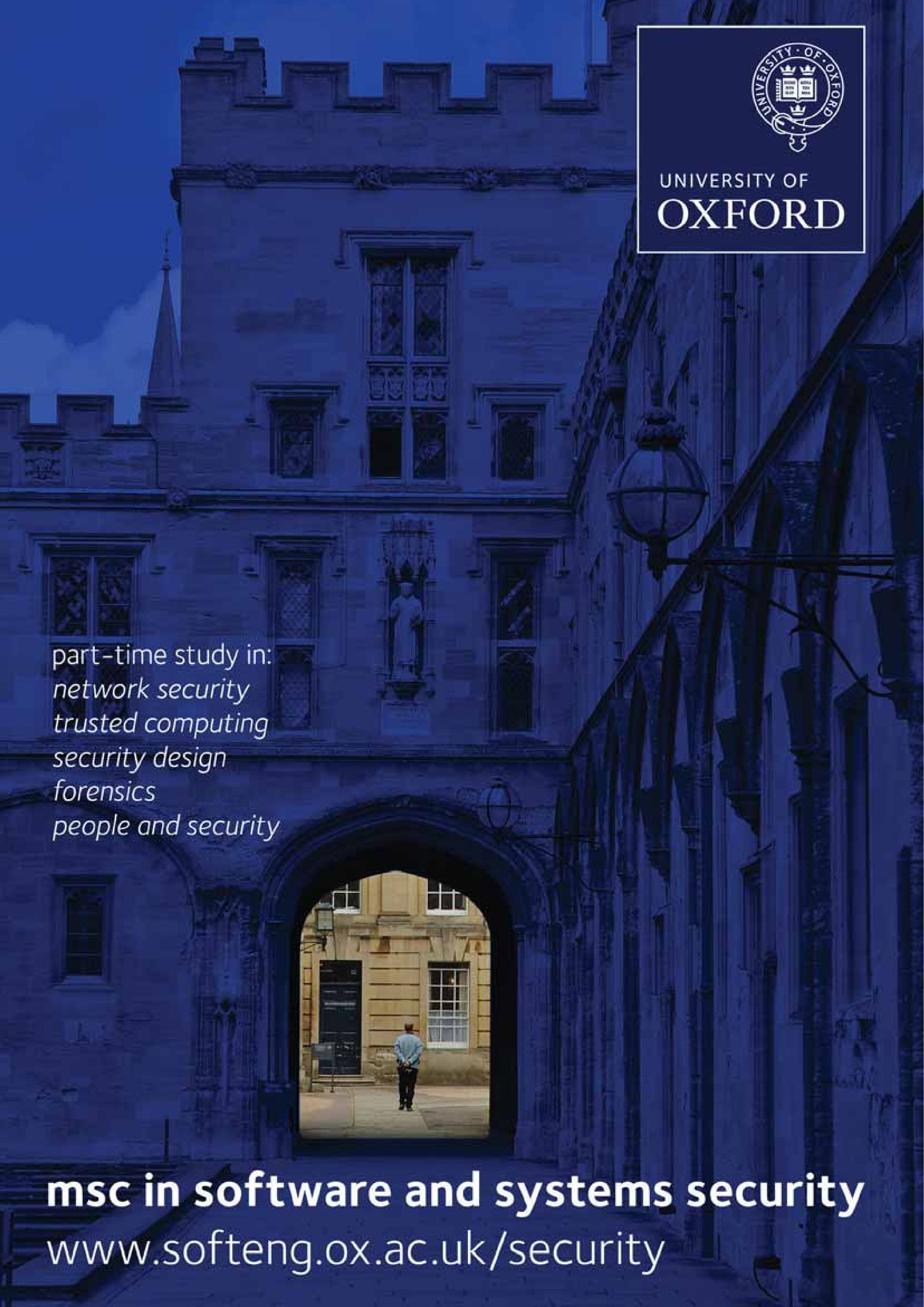
>INTRODUCING EMAIL VIRUS NETSKY
>IT PROPAGATES THROUGH EMAIL TO INFECT HOST FILES

>WE ELIMINATED IT
>AND IT FELT GOOD

>WE DISCOVER & DESTROY THOUSANDS OF UNIQUE VIRUSES EACH MONTH
>THE ANTI-VIRUS COMMUNITY RELIES ON OUR ADVANCED INTELLIGENCE
>WE HAVE A 100% GUARANTEE AGAINST ALL VIRUSES
>VISIT MESSAGELABS.COM/THREATS FOR A FREE TRIAL

MessageLabs | Now part of Symantec

IMAGE GENERATED USING SOURCE CODE FROM EMAIL VIRUS NETSKY



UNIVERSITY OF
OXFORD

part-time study in:
network security
trusted computing
security design
forensics
people and security

msc in software and systems security

www.softeng.ox.ac.uk/security