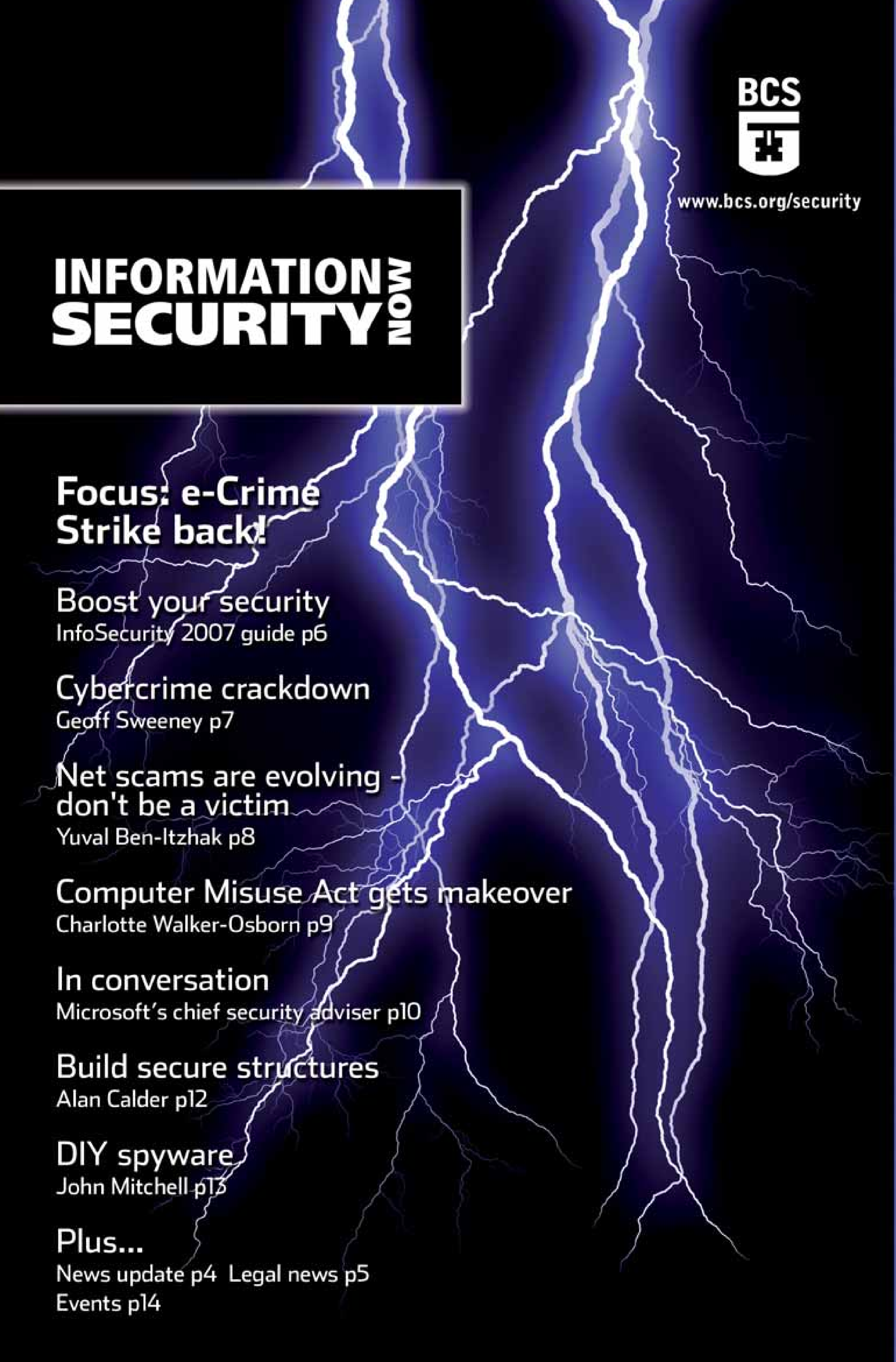
SPRING
2007

BCS

www.bcs.org/security

INFORMATION SECURITY NOW



Focus: e-Crime Strike back!

SUPPORTED BY THE BCS INFORMATION SECURITY SPECIALIST GROUP

INFORMATION SECURITY NOW is the quarterly magazine of the BCS security forum, incorporating the Information Security Specialist Group. It can also be viewed online at: **www.bcs.org/security/isnow**

Editor: Rupert Kendrick
Managing editor: Brian Runciman
Assistant editor: Henry Tucker
Designer: Marc Arbuckle
Graphics assistant: David Williams

Registered Charity No 292786

The opinions expressed herein are not necessarily those of BCS or the organisations employing the authors.

Printed in Great Britain by Holywell Press.
ISSN 1752-2455. Volume one, number three.

The British Computer Society
First Floor, Block D, North Star House,
North Star Avenue, Swindon SN2 1FA, UK
tel +44 (0)1793 417 417;
fax +44 (0)1793 417 444; www.bcs.org
Incorporated by Royal Charter 1984.

ISSG Chairman, Gareth Niblett, offers his hopes for Infosecurity Europe 2007

Welcome to the third issue of *Information Security Now.* This issue looks at Infosecurity Europe 2007 and what the future may hold.

Infosecurity Europe 2007

April brings the annual pilgrimage to London Olympia for information security professionals from around Europe and beyond. It just gets bigger every year, with over 11,000 visitors expected and around 300 vendors vying for attention in an increasingly crowded marketplace. Apparently, security is big business.

Personally, I'm hoping not to see the same vendors, on the same stand, in the same place, hawking the same solutions for yet another year. However, looking at the floor plan, I do get that familiar feeling and I think I know what's coming. That said, I'm glad to see that over 10 per cent of the exhibitors are new to the event.

I'd like to see the product space improve, more innovation, integration (not of the Heath Robinson kind as favoured by some building 'unified suites'). I also feel intuitiveness, ease of use, and intelligence, not just information, is needed, with less focus on niche point products that attempt to fill tiny gaps in the market left by others.

Rather than simply loading up on glossy brochures until your complimentary bag splits, I recommend attending some of the excellent talks on offer. With around 100 keynotes, seminars on subjects such as technical and business strategy, and workshops on offer, there is no excuse not to boost your knowledge, and CPE points.

If you're bored with trying to lift decent freebies without being spotted by sales and marketing staff, come and visit the BCS stand – D220, close to the Technical Seminar Theatre on the ground floor. Some of the ISSG committee will be in attendance throughout the event.

What the future holds

Recently, I was invited to participate in an Infosecurity Europe Advisory Council meeting. Now, this doesn't mean I will take any blame if you don't enjoy it this year, but I hope that I contributed a little to the view that Reed Exhibitions now has the security drivers that attendees consider important.

After an incredibly open, wide-ranging and informative roundtable discussion, the group of senior security professionals agreed on what they considered, the ten security hot topic areas for us in the forthcoming year were.

These included, in no particular order: globalisation, governance, identity management, compliance, remote working, professionalism, education, budget / cost reduction, integration and management / managing risk.

I noticed immediately that not many of the topics relate to products, or directly to technology. The security profession has finally got to grips with the fact that security is more about people and process than technology, and now it's time to educate everyone else.

Gareth Niblett is head of information security at Kingston Communications.

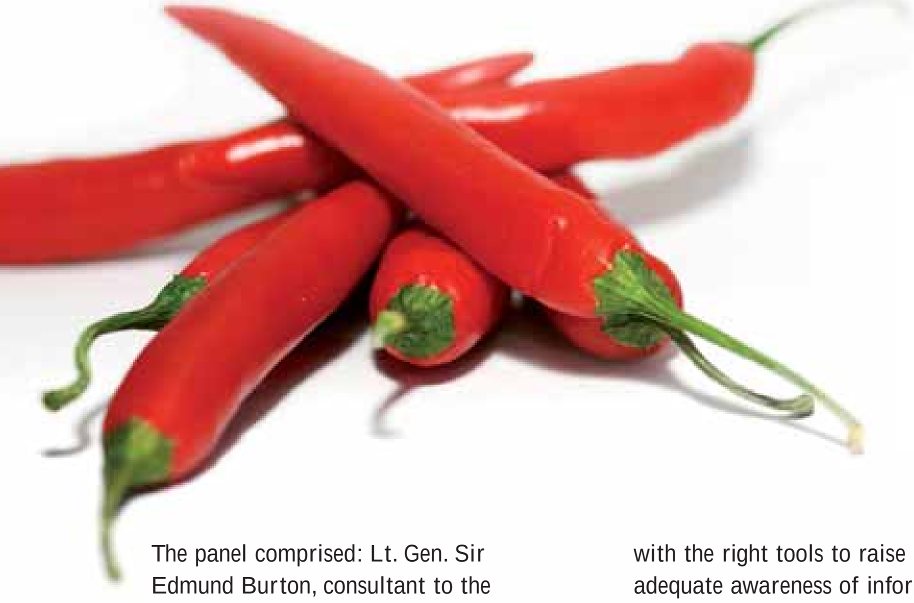
FURTHER INFORMATION

Information Security Specialist Group: **www.bcs-issg.org.uk**
Information Risk Management and Audit Specialist Group: **www.bcs-irma.org.uk**
BCS Security Portal: **www.bcs.org/security**
Information Security Now online: **www.bcs.org/forum/isnow**

More questions than answers

***ISNOW* editor, Rupert Kendrick, reports on the launch of the BCS 'Hot Topic' events series.**

Over 100 delegates packed into BCS's London offices at the end of January for the launch seminar in a series of Hot Topic events run by the BCS. The hot topic in question was information assurance, a key issue for every organisation. The debate focused on the need for effective communication of risk throughout an organisation. Should there be command and control of subordinates, or a collegiate approach?



The hot topic in question was information assurance, a key issue for every organisation.

The panel comprised: Lt. Gen. Sir Edmund Burton, consultant to the government's information assurance strategy; Professor Brian Collins, chief scientific advisor to the department of Transport; Dr. Paul Dorey, leader of digital security and business continuity planning for BP; and John Smith, head of group security at Prudential.

The panel began with the suggestion from one member that a mission command approach, in which leaders formulate the structure of a strategy, allocate resources and ensure understanding by subordinates. It's then up to them how they implement it with a minimum amount of control.

It was also suggested that information should be viewed as an asset. In this context, concern was expressed at the lack of effective processes for establishing the quality of software design, and beyond that, for managing it effectively. Information sharing, it was suggested, called for a consensual approach.

One panel member pointed to three communication issues to be addressed: the need for professionals and experts to communicate to the board in the right terms, so that the board has a clear grasp of the key issues; the need to provide end users of IT with the right tools to raise adequate awareness of information risk issues; and the need for transparency in the supply chain to ensure resilience.

It was also argued that different people in different places are now handling data that changes rapidly in volume, velocity and value. This can make it difficult to achieve information assurance. Nonetheless, if information assurance is treated seriously at board level, and with a less prescriptive approach, such a strategy has the potential to become a significant business enabler.

Taking questions, the panel expressed various views. Two panel members agreed on the need for greater education at subordinate level to raise awareness that information assurance should be seen as a corporate issue. Language needs to be in layman's terms as there is some evidence of ignorance over information risk at board level.

It was argued that security is already a business enabler - cash machines and exploitation of the internet were cited as examples, although, it was generally accepted that this message was difficult to transmit.

One panel member suggested the development of a dashboard solution which would enable employees to identify information vulnerabilities and compared this with the position of a finance director with total control of corporate finances at any given time.

A final conclusion was that robust action is needed at middle management level over attempts to block progress. Two panel members agreed that middle management are usually engaged on specific issues and need to take a more general view – and there was wide agreement that employees need educating to take ownership of risks within their organisations.

Although the debate was seen as a success by all attendees, as it raised a number of thought provoking points, in the end there just weren't as many answers or solutions.

Behind the headlines

Legal news behind the Infosec headlines from Struan Robertson of Out-Law.com, part of law firm Pinsent Masons.

Sheriff awards £750 damages for spam

An individual has won a spam case in the UK for just the second time. Gordon Dick has won a damages award of £750 plus expenses against Transcom Internet Services after suing the ISP for sending him a single email. The case did not go to a full trial.

Out-law has seen the Sheriff Court's note of Extract for Payment ordering Transcom to pay Dick damages of £750 plus 8 per cent interest since May 2006, plus £618.66 expenses. However, the two parties are still in dispute over how the case was conducted and its outcome.

Lords question data sharing powers

Better safeguards are needed in new government data-sharing proposals, according to the Conservative spokesperson on home affairs in the House of Lords. Baroness Anelay of St Johns has tabled a series of amendments to a new government bill.

The Serious Crime Bill allows for the sharing of data for comparison as a crime-fighting measure. Called data matching, this involves public sector financial watchdog, the Audit Commission, comparing different records to try to detect fraud.

But the government's proposals are too wide-ranging and do not contain enough safeguards against the invasion of citizens' privacy, according to the amendments proposed by Anelay.

The proposed law currently states that the Audit Commission's activities should be governed by a code of practice. It says though, that the code of practice will be written by the Audit Commission itself.

Anelay has proposed a legislative demand that the Information Commissioner's Office, the body responsible for protecting people's privacy under the Data Protection Act 1998, should approve any code. She has also suggested that both Houses of Parliament approve any code or any changes to it.

New requirements on security breach notification

Charlotte Walker-Osborn, associate solicitor, Technology Group, Eversheds LLP.

The government's response to the EU Commission on the review of the EU framework on electronic communications has sparked a possible review of the Data Protection Directive.

The Commission proposes that network operators and ISPs should be required to notify security breaches to national regulators. The UK accepts this in principle, but wants it to go further than the electronic communications industry claiming for example, that security breaches within the conventional mail system can be as much of an issue as electronic breaches. It has urged the Commission to review the Data Protection Directive to make security breach reporting a general, rather than an electronic telecoms, data protection requirement.

Concerns have been raised that although such a requirement is reasonable in principle, the US experience has shown the practical application of this to be a difficult challenge for businesses.

In response to the Commission's proposal for more prescriptive security requirements for electronic networks, the government claims that security cannot be efficiently achieved by regulation alone and there should be a combined approach across regulators, governments and industry.

Similarly, the government does not consider the e-Privacy Directive is the only cure for the problem of spam, particularly as the harm done by the content of spam can extend to dissemination of viruses and scams. It therefore urges that spam is tackled both with the e-Privacy Directive and through global co-operation with enforcement agencies, technical solutions and promoting self-help by users.

As to whether the Commission adopts this approach in its forthcoming Communication on spam, or whether there will be a review of the Data Protection Directive, remains to be seen.

Charlotte Walker-Osborn, can be contacted on 0845 497 1220.

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

Boost your security

With InfoSecurity Europe only days away, Neil Stinchcombe, highlights what you will see at this year's event.

The theft of sensitive data can cause a loss of customer confidence, a failure to comply with legislation, or significant financial losses from fraud. There has been a shift in security threats, with organised criminal gangs now using tools developed by hackers, virus writers and spammers.

The result has been a spate of highly publicised attacks, such as identity theft, denial of service and blackmail, using techniques that are becoming ever more sophisticated. Two high profile cases have already been reported this year at banks in Sweden and in the UK.

As the stakes are raised, criminals become more determined. Information security is the defence against this growing threat. It impacts on every aspect of how we do business. Secure operations mean higher productivity and a real business advantage. It is essential that cybercrime does not undermine the confidence of consumers in digital communication as this could cost organisations across the world billions of pounds in lost revenue and cost savings from new services.

Infosecurity Europe is the primary event dedicated to information security. With over 300 exhibitors, the event is the most comprehensive showcase for the widest range of new and innovative products and services from the world's top information security experts and vendors.

Over 100 companies will showcase their new solutions at the show this year. The event enables security professionals and business managers to: establish a commercial justification for information security; refine their security policies; and select the most appropriate solutions to support their security strategy in order to safeguard their company's reputation and assets.

More than 11,000 visitors are expected to attend this year's event. Many will come from overseas to participate in the free education programme that addresses both strategic and technical issues drawing on the skills and experience of senior end users, technical experts and real world case studies.

Industry experts

The 2007 keynote sessions at Infosecurity Europe are the highlight of the information security industry's international calendar. They bring together the industry's leading independent experts and take an in-depth look at some of the hottest ideas in information security today. Here are a few highlights from the keynote programme.

Lord Erroll will lead a panel debate on identity management, examining how to pick the right tools for the job. The panellists will include Toby Stevens, vice chairman, BCS Security Forum, Andy Kellett, senior research analyst, Butler Group and Maury Shenk, partner, Steptoe and Johnson LLP.

The debate will provide a fascinating insight into the theories and application of identity tools and processes in government, trading applications and organisations.

Lord Broers, chairman, House of Lords Science and Technology Committee, will give the opening keynote on internet security.

In a special address Derek Wyatt MP, chair of the all party internet group, highlights some of the key measures that will be put in place to assure the security of the 2012 Olympic Games.

Jon Fell, partner, Pinsent Masons will chair the hackers' panel which returns in the wake of a year of legislative change.

The keynote 'Should you always report crime?' seeks to define the point at which it becomes worthwhile for you to report it. This will be chaired by Geoff Smith, head of information security policy, DTI.

Keynote presentations

www.infosec.co.uk/page.cfm/Action=Seminars/CategoryID=4

Seminars

www.infosec.co.uk/page.cfm/Action=Seminars/CategoryID=2

Technical stream

www.infosec.co.uk/page.cfm/Action=Seminars/CategoryID=3

Vendor keynotes

www.infosec.co.uk/page.cfm/link=111

Microsoft forefront security academy

www.infosec.co.uk/page.cfm/link=110

New product launches

www.infosec.co.uk/page.cfm/Link=327/nocache=true

Exhibitor list

www.infosec.co.uk/page.cfm/Action=ExhibList/t=m/goSection=5

Latest floor plan

www.infosec.co.uk/page.cfm/Link=15/t=m/goSection=5

If you require a high-res version email **infosecuritypr@eskenzipr.com**

Opinion articles

www.infosec.co.uk/page.cfm/Link=245/nocache=true

Photographs of last year's show

www.infosec.co.uk/page.cfm/Action=PhotoLibrary/libID=162/t=m/goSection=6

White papers

www.infosec.co.uk/page.cfm/Action=ExhibitorLibrary/libraryID=20/t=m

Case studies

www.infosec.co.uk/page.cfm/Action=ExhibitorLibrary/libraryID=22/t=m

Infosecurity Europe takes place at the Grand Hall, Olympia, London, from 24 to 26 April 2007. For free entry and further information please visit: **www.infosec.co.uk**

Cybercrime crackdown

Geoff Sweeney, CTO, Tier 3, offers some strategies for avoiding and reducing your company's exposure to cybercrime.

IT security has come a long way in a short space of time, but cyber-criminals have developed their techniques further and faster than much of the technology pitted against them.

While conventional IT security applications have their place, Tier-3's experience suggests few IT managers are enhancing their security systems with a multi-faceted security application.

Multi-faceted applications both oversee and control existing legacy security systems and augment them with new heuristic based hybrid threat/malware analysis and protection technology.

The optimum solution is the introduction of a behavioural analysis systems that can analyse and manage information from legacy security systems, as well as acting as the glue to bind and integrate new security technologies, as they are added or developed.

Using behavioural analysis techniques enables organisations to future-proof their security systems, whether those systems are legacy, modular or integrated, or even a mixture of each.

Hybrid and multi-vectored attacks

Conventional cybercrime has evolved to the point where hackers and criminals are pooling their interests to create hybrid and multi-vectored attacks designed to subvert and break through the most complex of security defences.

Protecting against such attacks involves harnessing and integrating multiple security technologies to produce an overall defence system that is greater than the sum of its parts.

Tier-3 believes that behavioural analysis technology needs to be at the core of any organisation's IT defences. This is based on experience with real world customers. Recently, we encountered a major life assurance firm with a number of legacy IT security defences installed on its network. These were ill-equipped to handle the new and unknown types of security threats being developed by hackers and criminals.

Not only was the company poorly equipped to deal with next-generation security incursions and attacks, but its IT staff were also unaware, initially at least, of the potential risks they faced.

In fact, once criminals have invested time and money into breaking into an organisation's IT resource, the last thing they will do is draw attention to themselves. They will quietly exploit the situation and the first that is known of it is when significant losses are made, or the CEO reads in the press about a report of customers' identities being stolen.

Recommendations

IT managers should be looking for an all-embracing approach to security that draws together multiple defence technologies and uses them as a resilient coordinated shield to minimise the risk of a cybercrime against their organisation.

There are clear parallels between cybercrime protection and conventional crime prevention. If an organisation's physical defences are strong enough, criminals will look elsewhere, as is the case with cybercrime protection.

It is important to realise that IT managers should not be too involved with the specifics and minutiae of security technology. They should allow their security suppliers to carry out due diligence. Overall, a good IT manager needs to look at their organisation's security technology holistically and make sure they understand the big picture. This is what cyber-criminals do when developing new attack methodologies. By taking a leaf from the hacker's book in this respect, an organisation can go a long way to help minimise its cybercrime risks.

Tier-3 is exhibiting at Infosecurity Europe 2007, 24 – 26 April 2007, Grand Hall, Olympia.
www.infosec.co.uk

Effective protection against cybercrime - your essential checklist

- Carry out an IT and systems' audit - research and planning is everything
- Know your enemy - conduct a comprehensive threat analysis
- Complete a risk analysis - some threats are greater than others
- Design and deploy effective protection against the cybercrime threat
- Use behavioural analysis technology as a core defence

Net scams are evolving don't be a victim

Yuval Ben-Itzhak, CTO, Finjan, examines new methods of engaging cyber-criminals in combat.

Cybercrime techniques are changing rapidly, driven by a criminal fraternity that employs advanced programmers to develop new types of malware attack vectors.

Conventional signature-based analysis of internet activity, as well as traditional antivirus, anti-spyware and anti-malware applications have their place, but hackers are now using encrypted data streams and code obfuscation techniques to hide their tracks.

We have found that 70 per cent of hacker data streams are now encrypted, not all to SSL standards, of course, but it is clear that hackers are hiding their tracks from casual and/or basic data stream analysis.

Code obfuscation

As regards code obfuscation, which is defined as program code that is almost impossible to read or understand, our observations suggest that criminals are using this to prevent reverse engineering or similar analysis of their malware. However, this invalidates a growing number of real-time IT security analysis systems.

The use of encrypted data streams and code obfuscation creates the perfect environment for cybercrime to take place. It enables almost any form of web-loading malware to be started without most existing IT security systems, and software, being aware of the problem.

The only methodology capable of detecting a web-loading malware attack in real time is a proactive behaviour-based protection system, although it is worth noting that anonymously pooling data between internet users also has a place.

Low-value transactions

We have also observed that the criminal use of data obtained by web-loading malware is changing. The old system of manual misappropriation of e-banking funds has given way to automated low-value transactions, carried out by servers which continually harvest malware-obtained data and fire off rapid salvoes of minor e-banking transactions that can drain an attacked bank account within a few hours.

These automated e-banking transactions are usually small enough not to trigger a bank's security systems for several hours. By the time the hapless customer or the bank discover the fraud, it is usually too late to take action.

We believe an integrated solution does not work efficiently enough for major organisations. For this reason, we recommend that major companies install a discrete email protection system alongside a proactive web browsing analysis and control system.

Cybercrime predictions

While it is almost impossible to predict the full extent of what will happen to cybercrime attacks in the next 12 to 24 months, our analysis suggests hackers will progressively develop the ability to eavesdrop on SSL protected web sessions.

This prediction is based on a growing number of vendor solutions, many based around Broadcom's ASIC technology, possessing the hardware capability to eavesdrop on multiple SSL sessions.

Logic suggests a bot-based analysis, perhaps spread across several hundred or thousand hacked PCs, could develop enough computing power to decrypt one or more SSL sessions for hackers in real time.

Web surfing analytical software solves this potential problem, since it can monitor, advise and lock down employee web sessions in real time. This is a draconian, but efficient, approach.

We also predict that next-generation hybrid attacks resulting in cybercrime, using multiple attack vectors and methodologies to extract company or employee data in small amounts from different sources, are also likely in the near future.

By integrating this information with publicly available web resources, compiled using intelligent internet spider techniques, using artificial intelligence (AI) style software, hackers will be able to apply the resultant data with criminal intent.

The solution to this category of cybercrime threat is to use conventional IT security technology, combined with effective email protection, secure/controlled web access and best practice company procedures.

Finjan is exhibiting at Infosecurity Europe 2007 **www.infosec.co.uk (www.finjan.com)**

Computer Misuse Act gets overdue makeover

Charlotte Walker-Osborn explains the long-awaited updates to the Computer Misuse Act.

Computer misuse has traditionally been covered by the Computer Misuse Act 1990 (CMA). The CMA covers two key offences: section 1 criminalises unauthorised access to computer material, and section 3 prohibits unauthorised modification of computer material.

Section 2 creates a more serious version of the section 1 basic hacking offence, which arises where there is intent to commit or facilitate further offences. Following public debate over the applicability of the CMA to current technologies, and as to whether it adequately covers denial of service attacks, the Police and Justice Act 2006 (PJA) seeks to address these concerns.

Section 3 of the CMA is replaced by section 36 of the PJA. It says:

'It is now a criminal act knowingly to commit an unauthorised act with the intent or with recklessness as to whether it will impair the operation of any computer or hinder access to any program or data held on any computer or impair the operation of such a program or the reliability of such data.'

This widens the types of activities that might be caught. In particular, it overcomes previous concerns as to whether a denial of service was an unauthorised modification, as some argued that a computer, by its very operation, invites connections to it. The new definition also captures unauthorised acts which are committed recklessly. Those who post malware or distribute passwords on the internet with reckless disregard for its use may be caught under the new offence. The new wording is also wide enough to capture those paying someone to commit an offence.

The PJA also introduces a new offence of obtaining, supplying or offering to supply any article believing that it is likely to be used to commit, or to assist in the commission of an offence. This places an onus on distributors of hacking tools to decide if they will be used for illegal purposes. There have been fears this could criminalise legitimate IT security activity though.

The maximum term for summary offences under both sections 1 and 3 of the CMA is raised from six to 12 months' imprisonment (six months in Scotland under section 3). The maximum term for an indictable offence under section 1 of the CMA is increased to two years. The maximum term for an indictable offence under the amended section 3 increases from five to 10 years. The maximum sentences for the new offence of making, supplying or obtaining articles for use in a computer misuse offences is 12 months on summary conviction or two years on indictment. In all cases, a fine can be applied. A date has not yet been set for the commencement of the substantive provisions of the PJA, it is likely to be this year.

It is hoped this will act as an additional deterrent to potential offenders. However, security professionals are concerned that the law may inhibit the development of security tools for legitimate use, those which may be viewed as helping hackers. It is also queried whether the penalties are proportionate and a sufficient deterrent, especially given the current problems of over-crowding in UK prisons. A larger question mark remains in relation to deterrents across the world. This is a global issue which must be tackled on a world-wide basis.

Charlotte Walker-Osborn, can be contacted on 0845 497 1220.

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

In conversation

Ed Gibson, chief security adviser, UK, to Microsoft, talks to Rupert Kendrick, about the importance of security at Microsoft and how he sees his new role.

'It's all about people, all about people,' Ed Gibson stresses, as he leans forward, to emphasise his view of the key issue in addressing information security.

With over 20 years' experience in the fight against cybercrime, a significant amount of this with the FBI, he's well qualified to make assessments on the importance of aligning people and process with technology. In his role as chief security advisor at Microsoft UK this is exactly where his focus lies.

'Microsoft firmly believes it has a duty to provide guidance to help businesses and consumers act and secure their behaviour online. The previous holder of this position (Stuart Okin) was extremely well qualified from a technology perspective. I bring something different, my experience in cybercrime, which I hope will give me the necessary expertise to fulfil this duty.'

He defines his role as essentially that of a liaison person. 'As a company, we believe that innovation goes beyond the development of technology and includes development of process that is aligned to people. You see, security is too complex for most users so we've undertaken efforts to reduce complexity and encourage people to embrace security at all levels. My role is to liaise between customers and our internal development teams, finding out what the problems are and seeing how they can be resolved.

'The nature of security issues also means that Microsoft must work in partnership across the board to help thwart an evolving security threat. I consult with government, IT security organisations, private industry and the public and try to raise awareness of the important security issues and what the latest developments are,' he explains.

And one of the most important issues is the rise in the sophistication of cybercrime. He talks to all manner of senior executives about the problems arising in this area. 'They need attuning to the threats. Even by leaving their home computers inadequately protected, they can expose their own organisations to vulnerabilities such as botnets and the usual ploys of phishing and social engineering. They need to understand IT, and I sometimes think some of them don't have time to focus on this as they have equally important matters to contend with, and "IT is someone else's problem, not mine."

Not for the last time does he illustrate the scenario of 100,000 computers being controlled by an infected command and control server and the worrying consequences that this could have at corporate or governmental level. He explains that he's kept up-to-date with discreet listservs which he has maintained into his current role, some of which provide hourly reports of threat developments. 'As the security threat matures from hobbyist to the professionally driven, as an industry, we must seek ways of continually outthinking the cyber criminal. From an organisational perspective, security is not easy. Nor is it impossible. It is merely a risk decision. It requires a mandate from the top and must be positioned as enabling the organisation to do more with less risk.'

He likens the reluctance of companies to talk about their security vulnerabilities or hacking attacks, to the tradition years ago when people didn't discuss depression because of the stigma attached. 'It's the same with organisations. They think they are the only ones being subjected to security attacks and that they'll be singled out for it. But, of course, they're not. We're all under attack. If there is something you have of value, criminals will try and steal it, and it makes no difference what operating system you use.'

He feels unable to categorise motives for security attacks. 'Some say they are political, but I don't necessarily agree with that. Others say it's geographical and others say it's groups from organised crime. I say it could be all of those, and other causes as well.

'But in its simplest terms, it's up to every organisation to put in place the basic measures of protection, email spam filters, antivirus software and firewalls to ensure that people in the organisation manage them and behave properly with the technology.'

He argues that in some areas there are real differences between large and small organisations in terms of managing security risk. 'I think larger organisations are probably better able to manage security issues because they have the resources in terms of money and personnel, while smaller businesses have to focus on economic survival in the marketplace.

'But there are some similarities. In both types of organisation, there's sometimes little attempt to understand the nature of the threats, often it's "someone else's responsibility". But whatever the size of an organisation, security is always about people, processes and technology, in that order.'

He's surprised to hear it when it is suggested that Microsoft has been relatively slow to address security issues. 'Microsoft is often picked up for not doing this, or doing that,' he retorts.

'But in fact it has made great efforts to address security issues. For instance, there's been the Trustworthy Computing initiative and the monthly security updates that demonstrate how we are trying to address the issues, and Vista, launched for businesses on 30 November, has end-to-end security protection built in.'

While he's supportive of information security standards as a general principle, he accepts that their proliferation, especially the various certification and accreditation schemes can be confusing. 'However, one organisation cannot be the panacea when it comes to dealing with the security threat so we have to find a balance.'

Looking ahead at security issues for the future, he returns to the issue of 'more virulent viruses infecting and completely taking over vast numbers of computers, soaking up bandwidth, creating botnets of hundreds of thousands of computers.'

He finds this scenario sinister and repeatedly asks 'what is going on that we may have missed?' One of his duties is to spot trends and keep on eye on crime statistics, which he says, are on the rise. The uncertainty concerns him and 'the potential capability to create large scale disruption is a real worry.'

It's up to every organisation to put in place the basic measures of protection.

Build secure structures

Alan Calder, managing director, IT Governance Ltd, considers how to manage information security systems effectively.

Planning and implementing an information security management system (ISMS) to conform to ISO/IEC 27001:2005 can be a daunting task. While an ISMS implementation project is often seen as primarily an IT-related and IT-dependent project, it is actually a significant business-change project. If it is to succeed, it needs to be structured to reflect that fact.

There are five essential components to a successful ISMS project. The project must be business-led, have support from the top of the organisation, be appropriately resourced, be able to draw on the correct range of skills, and allow for operational requirements of the organisation.

Business-led

A senior business manager should chair the project team. Information security controls have three elements: technology, individual behaviour and procedures. Implementation of information security controls requires behavioural change across the business and these are more likely to occur if business users believe their needs have been accommodated. Business leadership makes this happen.

Committed board sponsor

At the heart of an ISMS is a detailed, asset-level risk assessment out of which comes specific control decisions that relate to that asset. Individual asset owners, users of the IT systems and data bases around the organisation, have to commit time and energy to risk assessment and control implementation and, if they know the project is seen as important, they are more likely to address these requirements.

Resources

This means that adequate time and money must be allocated. A properly trained and competent project manager should be assigned to the project, with the know-how and experience to identify roles and responsibilities, agree task objectives and delivery dates, and ensure that they are delivered. A competent project manager will ensure that adequate resources are identified and allocated to the project.

The vast majority of these resources already work within the organisation. Also most project managers will ensure that sufficient resources are available, both internal and external, for the project. They will also need to apply a realistic planning timeline.

Of course, identifying the full project budget requirement and winning the war of budget allocation is critical. No under-funded information security project ever delivered an optimum, cost-effective ISMS.

Skills

The project team should draw on skills from across the organisation. It should include influential members from every major function within the scope of the ISMS. Senior HR staff will also need to be involved. This is because job descriptions will have to be re-written, and the recruitment process overhauled. Procurement will also need to be addressed as information security needs building into the procurement process. Staff training should be looked at and on the legal side, confidentiality agreements may need redrafting. Finally they should also consult with those involved in network security and with the user community.

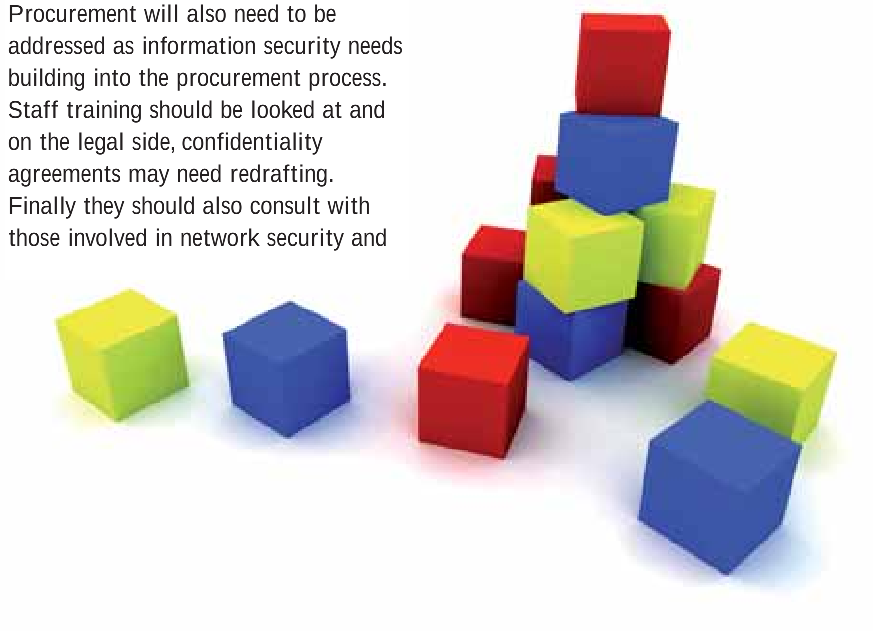
The project team needs to co-ordinate competing and overlapping activities across a complex project to ensure success and to ensure that the ISMS delivers an appropriate balance of confidentiality, integrity and availability.

Operational requirements

While qualified information security technologists are among the experts on whom the project team must be able to rely, the crucial expertise is that of the information security manager. They should understand the concepts of risk management, of continuous improvement, and the management system environment. Preferably they will have previous experience of implementing and managing an ISO 27001 ISMS.

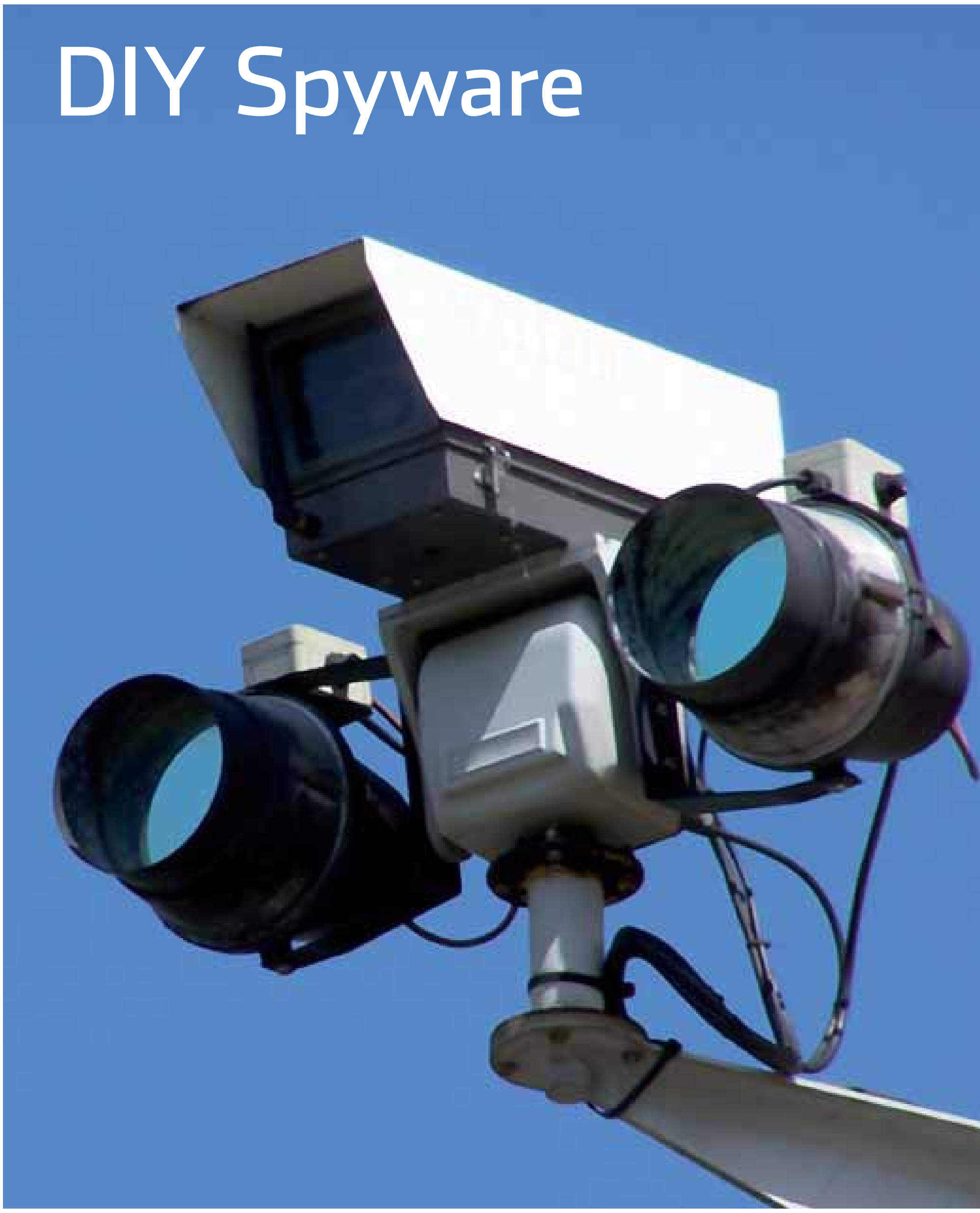
While a project that has these five elements is not guaranteed to succeed, one that lacks even one of them is guaranteed to fail. The message for organisations contemplating information security to ISO 27001 is the same as that for any business considering a significant change program.

Alan Calder can be contacted on 0845 070 1750.
www.itgovernance.co.uk



DIY Spyware

John Mitchell, managing director of LHS Business Control, examines the possession of articles for potentially fraudulent use.



I saw a little device advertised the other day with the tag line that it 'allows you to monitor what your kids, employees, or anyone using your computer is doing while on the internet and you can monitor them live, in real time, from anywhere in the world'.

The software resides on a USB device, but once loaded onto the target machine, you remove the USB host and therefore leave no visible trace of the Trojan you had inserted. No technical knowledge is required and it is not a bad investment at £30 to enable you to subvert a machine or two.

The icing on the cake is that you get two-way communication which enables you to block the target machine's internet access from any other machine with an internet connection, spyware and denial of service, all in one easy to use device, sold openly and legitimately.

Legislation

Well, maybe not so legitimately in the UK. The Fraud Act 2006 provides for 'possessing making and supplying articles for use in fraud'. This is a catch-all clause to cover the use of technologies not in existence when the Act was conceived. The problem is that even data analytical tools used by computer auditors could, in theory, fit into this definition. As could the search engines. It's not all bad news however, as the intent is the deciding factor.

Data analytical tools and search engines were not intended to be used for fraudulent purposes. The fact that they can be used in such a way is down to the intent of the user and not the design of the tool itself. So, although this little device could be used for computer crime and it does fit neatly into the unauthorised access and unauthorised modification clauses of the Computer Misuse Act 1990. It is the use to which it is put that counts.

It is advertised as a way to keep your eye on what your children are up to and enables you to block access to undesirable websites. Very laudable, but somewhat less charitable is the phrase that refers to snooping on your employees too.

Employee vetting

This raises the vexed subject of employee vetting. Vetting goes beyond simply asking for references and copies of their exam certificates. It is a more in-depth examination into the probity of individuals.

Some IT staff have unhindered access to a company's secrets and can also materially damage a company's data and software. It makes sense for the company to monitor them with more diligence than the average clerk.

However, in many cases the company is relying on a third-party to vouch for their integrity. What due diligence has been undertaken? I have long argued that security is primarily an HR issue, but I have received little welcome from HR when I have asked questions regarding the vetting of key IT staff.

The situation becomes more complicated where a service has been outsourced. What checks does the service company make on its staff? Can we rely on the Statement on Auditing Standards (SAS) 70 statement where an organisation has been through an in-depth audit of their control activities, including controls over IT and related processes for this? It depends on what is included in the SAS 70. None of the SAS 70 statements I have reviewed have explicitly covered staff recruitment, but there is no reason why you should not ask for this to be included.

John Mitchell can be contacted at:
john@lhscontrol.com, or 01707 851454.
www.lhscontrol.com

Forthcoming events

ISSG Events

www.bcs-issg.org.uk/events.html

17 April 2007
Identity Issues - Identity Card and Personal Security
University of Wales, Newport
Joint meeting organised by the BCS South Wales Branch

The fields of computer forensics and identity management have grown closer out of necessity, partly through the sharing of common objectives. While forensics is a particular speciality of our speaker, he is also a member of the information security research group at the University of Glamorgan, whose areas of research also include other topical security issues such as intrusion detection and computer evidence visualisation.

From the public perspective, the most visible evidence of the response to the threats from identity theft are massive increases in the sales of paper shredders and the possibility of wanting to switch bank. The minefield that is identity management in 2007 is one that will bear closer consideration.
http://southwales.bcs.org/events.htm

16 May 2007
Annual General Meeting
QinetiQ, Malvern, Worcestershire

Every year we hold a free event in conjunction with our AGM, usually at the premises of a major player in the world of information security. A number of presentations on topics related to the business area of our host are followed by the formal business of the meeting.

11 July 2007
Privacy Matters
BCS London Office

19 September 2007
Enigma Variations
Bletchley Park

IRMA Events

www.bcs-irma.org.uk

April 2007
16:30 - Control Self Assessment as an Audit Tool

1 May 2007
16.00 - AGM & Using Software for Risk Based Auditing

5 June 2007
16:30 - Network Security

3 July 2007
16:30 - TBA

9 October 2007
10:00 (all day) – Computer Crime Update

6 November 2007
17:30 - TBA

4 December 2007
17:30 - TBA

BCS Events

www.bcs.org

24 April 2007
2nd Security Forum Hot Topic Event Confronting the Challenges of Implementing an Enterprise Approach to Information Services in Defence

Defence is a complex, information rich, information hungry environment with a hugely diverse infrastructure.

From an organisational context the MOD is constantly evolving to respond to new opportunities and challenges and faces a number of immediate issues in supporting mobile and deployed Networked Information Environments.

It has been recognised that information architecture, supported by appropriate people and processes, is required in order to deliver an integrated information environment.

This event brings together industry and defence professionals to stimulate debate on the realities of delivering an enterprise approach.
www.bcs.org/security

Public Events

24-26 April
Information Security Europe 2007
Reed Exhibitions
Earl's Court, London

This is Europe's most comprehensive convergence of security professionals. It showcases a diverse range of new and innovative products and services and addresses today's strategic and technical issues. The event delivers an audience hungry for education and information on how, what, why and when to purchase the solutions on offer.
www.infosec.co.uk

30 April-4 May 2007
(Edinburgh, Manchester, Birmingham, Reading and London)

AIIM Roadshows – a series of events focusing on enterprise content management and the technologies used to capture, manage, store, preserve and deliver content and documents related to organisations.
www.aiimroadshow.org.uk

23-24 May 2007
The Wireless Event
Olympia Exhibition Centre, London

The Wireless Event is about delivering effective enterprise applications using wireless networks and mobile devices. If you are looking for ways to cost, plan and deploy technologies such as Wi-Fi, WiMAX, 3G, RFID and WVoIP to enhance business communications, then this is the event for you.
www.thewirelessevent.com

UCL

M.Sc. in Information Security

UCL's MSc in Information Security is an advanced programme for computer science, mathematics and electronic engineering graduates. The programme is organised around Computer Security, Cryptography and Digital Intellectual Property. Full-time and part-time study is available.

Programme Outline

- Cryptography
- Network security
- Computer security
- Electronic intellectual property
- Operating systems
- People and security
- Systems requirements engineering
- Communications and networks
- Software engineering
- Human computer interaction
- Specification and verification of distributed systems

The programme is directed and supervised by Professor Ingemar Cox and Professor Yvo Desmedt .

Location

Students can enrol at either UCL's main Bloomsbury Campus or UCL's Adastral Park Campus in Martlesham, Suffolk. Most classes are taught from Adastral Park with live videoconferencing to Bloomsbury.

Contact Information

Brian Riley 0147-366-3710

http://mscinfosec.adastral.ucl.ac.uk