

Europe's No.1 Information Security Event

www.infosec.co.uk

Infosecurity Europe 2011

Official Show Preview



Foresight in a complex environment

Organised by:





Welcome

Information security – Foresight in a complex environment.

The Cybercrime landscape is changing with the overall cost to the UK economy estimated at £27bn per year, by a recent report by the Office of Cyber Security & Information Assurance and Detica. The report reveals that whilst government and the citizen are affected by rising levels of cyber crime, at an estimated £2.2bn and £3.1bn cost respectively, business bears the lion's share of the cost at a total estimated cost of £21bn. The theft of Intellectual Property (IP) from business, which has the greatest economic impact of any type of cyber crime is estimated to be £9.2bn per annum, Industrial espionage has the second most impact at £7.6bn, followed by £2.2bn from extortion, £1.3bn from direct online theft and £1bn from the loss or theft of customer data. Now these figures are only estimates, but even if they are significantly overstated it is now time for UK business and government to take information security seriously. Government has already taken steps to do so with Cyber Security being the only government area to be given an increase in budget and businesses might do well to follow suit before it is too late.

Against this economic backdrop, Infosecurity Europe has assembled the top information security providers from around the world for you to compare and select the latest technology to protect your organisation, including 40 exhibitors who are exhibiting at the show for the first time this year. There are hundreds of companies exhibiting from across the globe with many launching new products and services. The event plays host to Europe's largest FREE three day educational programme addressing both strategic and technical issues facing information security professionals, drawing on the experience of senior end users, technical experts and real life case studies.

The **Technical seminars** feature specialists who will

cover the latest issues and technical advances. The **Business Strategy seminars** are led by senior executives who will speak about the challenges and issues facing management, CEO's and other board level directors. The **Security Workshops** will enable you to discuss your issues with your peers catalysed by a specialist facilitator to ensure you stay ahead of the game and leave with insights to inspire your colleagues. New for 2011 is the **Information Security Exchange** where you can get to grips with the latest and greatest innovations within the Information Security sphere in a practical, business-application format. Also new for 2011 is the **Technology Showcase** where exhibiting companies will take to the stage to demonstrate their capabilities of their solutions to you – the end-user. Take the opportunity to hear live about new and existing products, services and solutions - and come prepared with your questions to get the answers you need first-hand.

We will also be recognizing a nation's technical prowess in the field of information security with the new **Market Focus** – honouring the US for 2011 as the home of countless cutting-edge technological advancements. Over 50 companies will be exhibiting from the US, including exhibitors in the **US Pavilion**.

We trust that your visit to Infosecurity Europe will help you gain access to the additional resources your organisation needs to meet the challenges posed by cyber crime – and to help you gain the foresight you need in an increasing complex environment.

I look forward to seeing you there



Claire Sellick

Exhibition Director, Infosecurity Europe

infosecurity®



EUROPE

www.infosec.co.uk



Follow us on Twitter @Infosecurity



Join the Infosecurity Professionals
(Infosecurity Europe Network)



Join the Infosecurity Europe Facebook Group



View the Infosecurity Europe YouTube Channel

Reed Exhibitions®

Organisers of Infosecurity Europe
Gateway House, 28 The Quadrant, Richmond, Surrey, TW9 1DN
T: +44 (0) 20 8910 7976
F: +44 (0) 20 8910 7926
E: infosecurityteam@reedexpo.co.uk
W: www.infosec.co.uk

This magazine is produced on behalf of Reed Exhibitions by
Showtime Media Services Ltd
Managing Director: David Benson
Sales Office Manager: Lesley Maisey
Sales: Sarah Lelarge
Design: Andy Milsom
Accounts: Mark Benson
Editorial: Luke Murphy

SMS

Showtime Media Services Ltd

Showtime Media Services Ltd,
Suite 5, 37 Bury Mead Road, Hitchin, Hertfordshire, SG5 1RT, UK
T: +44 (0)1462 420 009
F: +44 (0)1462 642 464
E: enquiries@showtimemedia.com
W: www.showtimemedia.com

Environmental Statement - Sustainable paper
All publications produced by SMS are printed on paper from sustainable forests, manufactured using Elemental Chlorine-Free (ECF) bleach and 100% recyclable chemical fibres. The paper is also 100% recyclable and is from natural and renewable resources.

While every effort has been made to ensure the accuracy in the compilation of this magazine, the organisers and publishers cannot accept liability for content of any promotional material, errors and omissions.



Contents

Welcome	2
Travel Information	4
Infosecurity in flux	6
The Smartphone - A Real Bug in Your Bed	8
Don't Forget The Users - How To Make Them Your Biggest Ally	10
The Effectiveness of Information Security - when do you stop spending?	12
A-Z Exhibitor Listing	14
Floorplan	16
Seminar Timetables - Business Strategy Theatre	18
Seminar Timetables - Technical Theatre	20
Keynote Theatre	22
Security Workshops	27
New for 2011 - The Information Security Exchange Theatre	27
New Products and Services	28
New Product Launches	30
News	36
Essential Contacts	40

Infosecurity Europe Team

Contact us at: infosecurityteam@reedexpo.co.uk

Claire Sellick	Event Director	Tel: +44 (0) 20 8910 7907	Email: claire.sellick@reedexpo.co.uk
Malcolm Wells	Sales Manager	Tel: +44 (0) 20 8910 7718	Email: malcolm.wells@reedexpo.co.uk
David Paterson	Sales Executive	Tel: +44 (0) 20 8910 7047	Email: david.paterson@reedexpo.co.uk
Ben Race	Sales Executive	Tel: +44 (0) 20 8910 7991	Email: ben.race@reedexpo.co.uk
Kurt Rauner	US Sales Executive	Tel: +1 203 840 5821	Email: krauner@reedexpo.com
Sofia Pernikis	Sales Co-Ordinator	Tel: +44 (0) 20 8910 7106	Email: sofia.pernikis@reedexpo.co.uk
Laura Heather	Marketing Manager	Tel: +44 (0) 20 8910 7849	Email: laura.heather@reedexpo.co.uk
Ashvinder Bhamra	Marketing Executive	Tel: +44 (0) 20 8910 7962	Email: ashvinder.bhamra@reedexpo.co.uk
Emma Tommony	Content Manager	Tel: +44 (0) 20 8910 7943	Email: emma.tommony@reedexpo.co.uk
Neil Stinchcombe	PR Manager	Tel: +44 (0) 20 7183 2833	Email: neil@eskenzipr.com
Ruth Chevell	Operations Manager	Tel: +44 (0) 20 8910 7997	Email: ruth.chevell@reedexpo.co.uk
Sabrina Bonotto	Operations Executive	Tel: +44 (0) 20 8910 7796	Email: sabrina.bonotto@reedexpo.co.uk



Travel Information

How to get to Infosecurity Europe at Earl's Court.

Opening Hours at Earls Court

Tuesday	19th April	09.30 - 17.30
Wednesday	20th April	09.30 - 17.30
Thursday	21st April	09.30 - 16.00

Travelling to Earls Court

Earls Court is centrally located in London, and is easily accessible, especially by public transport.

This international venue is within steps of London Underground's District Line - Earls Court tube station, and also the Piccadilly Line. Take the Warwick Road exit out of the tube station and follow signs to the venue.

All major inward/outward-bound London rail routes, as well as air and road networks are within easy reach. For maps and more detailed information visit our website, www.infosec.co.uk/travel

Parking Details at Earls Court

To pre-book your parking please call 0871 871 9809 between 9.00 - 17.00, Monday to Friday or book online at www.eco.uk

Don't forget to book your hotel near Earls Court

The Infosecurity Travel Desk offers a free booking service and many discounted rates at hotels that are near to Earls Court Exhibition Center. Bookings can be made by email, online and telephone, and all successful booking requests and cancellations will be confirmed to you by email. Please quote the event code 'Infosecurity Europe' on all correspondence.

Contact:

infosec@exposetravel.com
 +44(0)1883 629177 - Telephone
 +44 (0)1883 346763 - Fax





Infosecurity

Infosecurity Network editor Jim Mortleman looks at the changing state of the industry and asks how visitors to the show should be approaching suppliers today.



From industry giants offering to help with all your infosecurity needs to niche specialists touting solutions to tackle specific threats, the range of companies, services and technologies on show at this year's Infosecurity Europe is simultaneously impressive and bewildering. Some visitors simply come to keep up with the industry trends, technologies and talking points, but others have more focused intentions - to meet suppliers or check out technologies that might be able to help with specific security challenges facing their organisations.

The infosecurity industry has always had a reputation as something of a black art. To a certain extent, customers have had to accept on trust its assessment of the nature and level of the threats that are "out there", as well as its assertions that particular products and services can help protect us adequately. But there are signs that today the industry is being forced out of the shadows and the practices that have served it well enough up to now may be set to change.

Savvy customers are no longer content to shell out for the latest whiz-bang technologies unless suppliers can understand their business requirements and explain how any proposed solution fits in with their wider organisational security and risk management strategy. In addition, more infosecurity stories are being reported by the mainstream media, putting the spotlight on current threat-protection provisions like never before.

Governments around the globe are also finally starting to realise the potentially disastrous consequences of cyber-attacks and are pouring resources into developing better defence strategies. Simultaneously - amid a growing profusion of new

connections, applications, devices and exploits - experts are warning that unless the industry helps customers address their security strategy from a human and business standpoint (as well as just a technical one) they will be incapable of adequately reducing the risk that those customers will be hit by some damaging "zero day" threat or clever new social engineering tactic.

Security expert and *Computer Weekly* blogger David Lacey, for instance, predicts that "2011 will see the start of a revolution in security thinking, which will last for most of the next decade", a period he says might prove to be a "new age of enlightenment" for the industry. However, he's under no illusions that this new dawn will either come quickly or be universally welcomed and accepted by suppliers.

So how can buyers ensure they select providers that do understand the need for change - and that are committed to more enlightened, co-ordinated thinking on infosecurity? The simple answer is that you can gain a pretty good idea by talking to the right people and asking the right questions - which is why a show like this presents a great opportunity to conduct your own informal market research.

Any supplier worth its salt should be able not only to answer questions about their technology and the threat landscape, but also to address your real business issues convincingly - such as how you can gain the touted benefits of cloud computing while ensuring the security of your organisation's information once it leaves the confines of your data centre; how you can attain the mobility and flexibility offered by smart mobile devices without users falling foul of the latest threats or scams; or how best you can ensure your customer-facing systems such as websites are protected from attack. And if their answers amount to little more than "buy our technology and you'll have no need to worry", you'll know they're probably not serious about change.

n flux

“ 2011 will see the start of a revolution in security thinking, which will last for most of the next decade

”

The Smartphone - A Real

The rise of the smartphone over the past few years has been a technology success story.



An almost perfect storm of advancing materials science, chip set development, software innovation and social networking has fuelled the progress in handset design and capability beyond that which could be imagined only a couple of decades ago. Having such tremendous computing power, alongside user's private data and contacts makes a tempting target for criminals. It could be argued that the security industry has been slow in recognising the threat to such devices so only now are we seeing products and services designed to improve smartphone security.

Very few businesses want their data to be less mobile, aside from those that have just gone through a major data loss incident and are hurriedly trying to bolt the doors after the data has gone. In fact many businesses seem to pride themselves on the mobility of their data, on the basis that their employees will be accessing work related data at all times of the day or night and will therefore be more productive. Whether employees are actually more productive is another discussion, but certainly the drive to mobilise data has resulted in the endpoint of most organisation's network being in the handbag or pocket of their employees.

One exciting part of data mobilisation is the tidal wave

of smartphones being used by businesses to access their data. But what are the particular security issues and opportunities that these smartphones present?

Of course data is more mobile than ever before. Few people pause to consider why we should automatically assume that all data should be made mobile. Very few computer security types are successful in stopping this demand, certainly outside a handful of top secret establishments. One of the first questions many a new employee will ask is how they can connect their smartphone to the data they use. After all the success of web sites such as salesforce.com is based on the fact that, like all cloud computing solutions, the data can be made available from anywhere. A young in age workforce knows nothing other than mobile computing.

Most businesses accept mobile computing and, during this inevitable embrace, need to decide how to best protect their data. After all, the smartphone is where it is happening.

Try to go into a phone shop and buy a phone that doesn't, at least, have some "smart" features and you will have a problem. Some organisations that try and equip their workforce with phones that don't have a camera for security reasons have a problem. Some manufacturers have woken up to this and are now producing basic phones, especially for the older generation that may need improved handset accessibility. Consider that the biggest growing group

“ But what are the particular security issues and opportunities that these smartphones present? ”

Bug in Your Bed

of Facebook users are the 35 year old plus, all of who will want to access their accounts long into the future. Even if the Facebook site isn't around a successor will be as social networking appears to be deeply entrenched into so many people's lives.

Smartphone hardware marches on relentlessly. Handsets are certainly getting more powerful, for example in 2010 LG announced the Optimus 2X with a dual core 1GHz processor. Research has shown that 2011 is the year when smartphone shipments will overtake PC shipments, and both PCs and smartphones lay neck and neck at around 400 million units each, per year . The amazing growth in these fantastically powerful devices presents us as security experts with a significant challenge.

On top of all their other concerns most Chief Information Security Officers (CISO) are now having to worry about a number of smartphone security issues;

- Are my smartphones going to be infected with malware?
- Is my smartphone based data secure?
- Will my mobile voice traffic be secure?
- Can my smartphones be remotely managed?

There is no longer a discussion about whether these devices should be allowed, now the conversation is how they can be accommodated safely and securely. Ultimately the CISO is worried about risk to the

business, and in particular how this new smartphone risk can be managed whilst at the same time the business productivity of users improved.

Cast one's mind forward 20 years and it boggles at the depth and breadth of attacks our mobile phones will be subject to. In the meantime anyone that conducts sensitive business using a mobile phone should seriously consider implementing preventative measures sooner rather than later. As more and more people use their mobile phones to run their entire lives, hackers and others will focus their efforts on getting the information they need from these devices. In many respects attitudes towards mobile phone data security reflect those held 20 years ago towards the humble personal computer. Back then attacks were minimal, anti-malware was yet to become established and hacking was in its infancy. Now we are in a maelstrom of attacks against the PC using sophistication and scale we previously thought impossible.

The smartphone is next on the list.

Nigel Stanley
Practice Leader - Security
Bloor Research

Nigel will chair the Keynote session: Can You Turn Mobile Devices To Your Advantage Or Are They The Next Big Security Hole on Tuesday 19th April at 12.30

Don't Forget The Users - How To

It's tempting to think that technological defences and monitoring solutions can be installed to prevent security incidents from occurring, but in reality we all know that no matter how much money is thrown at improving security within organisations, without educating employees in good security practices, that money is all but wasted.



Given basic training in security awareness, most employees will reward you with years of vigilance and timely responses to security events. At Allen & Overy LLP we ensure that all new employees globally are schooled in basic security awareness by attending a comprehensive presentation that is relevant to our industry and uses up-to-date examples of poor business security to illustrate the talk. There are no shortages of examples of poor business security! We aim to make the presentations as interactive as possible with real examples of social engineering and phishing attempts. Attendees complete a quick online questionnaire following the presentation to assist us in continually improving the content.

One of the areas that we explore in the security induction is 'Mistake' and the need for users to own up to minor incidents before they turn into major ones. I.T. users are particularly vulnerable to mistakes owing to their intrinsic need for experimentation and their need to try out new things. Many ordinary users fear straying outside the boundaries of a rigid set of instructions for using a particular program, but for I.T. staff their inquisitive nature will often lead them towards exploring



Make Them Your Biggest Ally

undocumented or unconventional ways of using software which can sometimes cause unexpected results. Also I.T. users are at risk of generating incidents simply because they require elevated privileges to complete their tasks, so it is

important to encourage a culture in which it is better to 'fess-up human errors than sweep them under the carpet of 'cover up'.

Social networking is a key subject area in the security awareness presentations simply because we cannot ignore that fact that users now see the work/life mix as a very blurred line and the long hours that many of our users work mean that attempting to limit social networking to core business hours is a fruitless operation, but it is important to educate employees that 'private' postings on social networking sites can cause reputational damage - to themselves or the company they work for. The 'Facebook Friend in Peril' scam is used to illustrate how scammers use social networking to fool gullible 'friends' into sending

“ Many ordinary users fear straying outside the boundaries of a rigid set of instructions for using a particular program

”

money to Internet miscreants. Understanding the downsides of social networking will help users utilize its power whilst taking sensible security decisions when using the sites.

To emphasise some of the key security messages, we also

developed a global poster campaign for all coffee areas - all posters are translated into local languages as well as English to highlight the importance of the poster messages and they have been well received. Some languages proved a challenge - Taiwanese and Arabic were particularly difficult for those of us who struggled with 'O' Level French!

*Martyn Styles
Information Security Team Leader
Allen & Overy LLP*

Martyn will join the Keynote panel on Tuesday 19th April at 13.45 for the session: Don't Forget The Users - How To Make Them Your Biggest Ally

The Effectiveness of Information when

Information security has matured over recent years; once sidelined and overlooked, we now find ourselves presenting to senior management and influencing corporate strategy.

With this higher profile comes responsibility and an increasing need to deliver a demonstrably effective solution that offers proven value for money.

We understand, however, that risk can be mitigated but it can never be eradicated completely, as such, it is possible to make a massive investment in security technology, process and resource and still suffer an incident. Few roles suffer the same challenge, where a well-conceived, well-funded and a secure solution may become vulnerable through no action, or inaction, from your staff - truly the modern IT Security Manager has a difficult balancing act to manage.

To understand the effectiveness of the security policy in place at your organization, it is important to appreciate both the global threats and the risks that apply to your firm and sector. Discussions with peers, industry research and viewing the controls from the user's perspective all help in this regard. Understanding and quantifying the risks arising from these threats provides a first baseline to measure effectiveness.

Once the threats are understood, the next key step

“ Once the threats are understood, the next key step is to recognize the risk appetite of your firm ”

Security - do you stop spending?

is to recognize the risk appetite of your firm. Risk appetite is a somewhat intangible element, however it is important that the security professional instinctively understands the risk tolerance for that particular firm. Documenting the risk appetite and building the risk management process around it can be hugely valuable to an information security team; such an activity drives a greater level of participation from business staff and ensures that information security can no longer remain just an IT issue. Although this degree of business involvement may be new for some firms, no CEO can have failed to notice the ever increasing press coverage of cyber threats and information and technology risks, as such, you may be surprised at how keen the business staff will be to contribute.

Effectiveness can only be described if the controls that are in place are scrutinized and measured. To this end, it is important to have the capacity to undertake IT audits from within the IT Security team. The increasing complexity of technology solutions means that the auditors role is becoming more and more challenging, however even with just a partial resource

allocated to IT audit, there is great value that can be added.

It is vital that your information security programme does not become a 'money pit' to the organisation, this baseline of recognized threats, defined risk appetite and audit capability enables the security professional to understand the developing risk profile within their firm and be able to target where they may best expend their efforts, resources and money to support the business. Only at this point can discussions about the effectiveness and value for money provided by your security policy start to have any real meaning.

The discussion at Infosec will consider how to help you ensure that your security controls are both effective and appropriate.

*Andrew Rose
Global IT Risk Manager
Clifford Chance LLP*

Andrew will speak on the Keynote panel: The Effectiveness Of Information Security – When Do You Stop Spending on Tuesday 19th April at 11.15



A-Z Exhibitor Listing

(ISC) ² UK Ltd	A80	Dell SecureWorks	A74
365 iTechnology	AA50	Detica	K65
3M (UK) Plc	C82	DeviceLock, Inc.	D42
Absolute Software Corp	C20	Digital Assurance	K90
Accellion, Inc.	J75	ECSC	D80
Access Layers	B80	Elcomsoft	C32
Acme Packet	G50	Elsevier Ltd	L63
Activnetworks	H83B	Entrust (Europe) Ltd	D32
Acuity Risk Management	F81	ESET	C70
Acumin Consulting Ltd.	G37	Europeum Reseller	L71
AEP Networks Ltd	B50	Euro-Recycling Limited	E83
Algosec	A70	ExactTrak	F41
AnubisNetworks	G72	Exponential-e	AA51
API Technologies	K73	F5 Networks	B70
Application Security Ltd	A48	Falcongaze EU, Ltd	J74
ArcSight	H43	Faronics	J92
Astaro GmbH & Co. KG	F21	Feitian Technologies Co., Ltd.	F42
Astec d.o.o.	K96	FireMon	F70
Attachmate	E80	First Base Technologies	J60
Avecto Ltd	L70	Fortify Software	H75
Avira	L88	Forum Systems	F79
AwareGO	H96	Fox IT	F80
Barclay Simpson	H45	Fox Technologies, Inc	C30
Barracuda Networks	C10	French Trade Commission	H81, H83, H85
Barron McCann Technology Ltd	E30	FST	M76
BCS	A83	G DATA	B35
BeCrypt Ltd	B62	GlobalSCAPE	G84
BeyondTrust Corporation	H95	GlobalSign	G90
Bit9	A38	GrIDsure Limited	G94
BlackBelt/Smartphone Defence	J95	Grid-Tools Ltd	H42
BlockMaster	F60	Hewlett Packard	D60
Bloxx	E40	HID Global GmbH	C81
BSI Group Headquarters	E93	High Density Devices	H80
BT Global Services	C92	Hitachi Europe Ltd	E90
Canon Europe Ltd	B63	HSM	K91
Caretower Limited	F20	IBM UK Ltd.	E20
Cassidian	B41	Idappcom Ltd.	B92
Celestix Networks (UK)	C40	Identiware B.V.	L87
Certgate GmbH	H68	Imperva	B60
Certification Europe	L74	Institute of Information Security Professionals	F91
CESG	A91	Intel	G75
Charismathics	E42	IntraLinks	F82
Check Point Software Technologies	F40	IOactive	H39
CiRRUS Management Solutions	H76	Ipswitch File Transfer	H70
Ciphercloud	K92	IronKey, Inc	F30
Cisco Systems Limited	C11	ISACA	H41
City University London	J51	ISF	A52
Codenomicon	L93	iStorage Limited	A39
Commissum	H40	IT Governance Ltd	B91
Computer Network Defence Ltd	C25	Ixia	J76
Conscio Technologies	H85B	K7 Computing	J80
Continuity Shop	J94	Kaspersky Lab UK	C41
Core Security Technologies	J52	Kingston Digital Europe Limited	D91
CRYPTOCARD Europe Ltd	B43	Kobil Systems GmbH	E50
Cryptosoft	J79	L-3 TRL Technology	D41
Cryptzone UK Ltd	A64	Lancope Inc	B29
Cyber-Ark Software (UK) Limited	J50	LANDesk	B10
Data Encryption Systems Ltd	D22	Lieberman Software Corporation	F52
Data Robotics, Inc	K75	Login People	H83A
Deep-Secure Ltd.	A40	LogLogic Ltd	G60

LogRhythm Ltd	G51	Secunia	B81
M86 Security	B40	SecurEnvoy	E60
Mancala Networks	J88	Signify	G30
McAfee International	C60	Sipera Systems	H50
Metacompliance Ltd	G35	SiVizion	J90
Mimecast	D90	Skybox Security Ltd.	B51
Mobiquant Technologies	H83C	SmoothWall	A30
Mozy	L80	SMS PASSCODE A/S	F31
MXI Security	G78	Software Box	B61
NetAgent Co., Ltd.	J70	SonicWALL	E61
Netheos	H81A & H81B	Sophos Ltd	D50
NetWitness	F72	Sourcefire Ltd	B21
Network Computing	M78	Spamina	K74
Neustar Inc	K76	Spectorsoft Corp	K70
nitrosecurity	A44	splunk	H66
Nogacom	J81	SSL247	K88
Norman Data Defence Systems (UK) Ltd	F61	Stonesoft Networks	B20
NRI SecureTechnologies, Ltd.	K77	Stonewood Group Ltd	E41
NS Focus	J73	SUD De France Export	H81A & H81B
NTS (UK) Limited	G44	Sunfive SA	B22
nuBridges Inc.	E82	SureCloud	F92
Oikialog	H83D	Swivel Secure Ltd.	D30
Open Systems Management	L60	Symantec (UK) Ltd	D70
Oracle Corporation UK Ltd	AA90	Symantec.cloud	C31
Origin Storage	F83	Syngress Publishing, Inc	K60
Oulu Regional Business Agency	L93	Systematic Development Group	F73
Outpost24 UK	E92	Thales	E71
Overtis Group	B23	The Open University	E81
Owl Computing Technologies	H60	Thycotic Software Ltd	F78
PaloAlto Networks	A34	Tier-3 Security Ltd	J65
Paycool Development	H81A & H81B	TigerScheme	L85
Pen Test Partners	E43	TITUS	J61
Pentura Limited	C51	TM3 Software GmbH	J98
Phoenix Datacom	D31	Tradepage Pty Ltd	G52
PixAlert	A73	Trend Micro (UK) Ltd	D10
Pragmatic Defence	B93	Tripwire	E31
Preventia Limited	B80	Trusted Computing Group Administration	D92
Proofpoint Limited	F50	Trustmarque Solutions	A90
Qualys	E70	Trustwave	AA40
Quest Software	B80	Tufin Software Technologies Ltd	G82
Quotium Technologies	J86	U.S. Commercial Service	G73
RandomStorm	G46	University Of Oxford - Software Engineering Programme	A50
Real Status	L75	Vade Retro Technology	H85A
Red Island Consulting Ltd	E91	VADition	D21
Red Lambda	L97	validEDGE	L76
Ricoh UK Limited	B72	Vasco Data Security SA	C21
Rittal Limited	D81	Venafi, Inc.	AA52
RM5 Software Oy	L93	Veracode, Inc	B90
RMS IT Security	C80	Voltage Security	F75
Royal Holloway, University of London	H73	V-Sub Solutions	J92
RSA, The Security Division of EMC	G65	Vulnit	H85D
S2S Electronics Ltd	L83	W L Gore & Associates (UK) Ltd.	F90
Safend Inc.	B30	Wallix	H85C
SafeNet UK Ltd	C50	Watchguard Technologies	C91
SafenSoft Corporation	G71	Waterfall	AA85
SAIC LIMITED	C45	Webroot Services Limited	D40
Sangfor	A53	Websense UK Ltd	E10
SANS Institute	AA74	Wibu-Systems LTD	L87
SC Magazine	A51	Wick Hill Ltd	D20
SearchSecurity.co.uk	L61	WinMagic Data Security	B71
SEC Consult Unternehmensberatung GmbH	J78		
SECnology	G45		
Secunet	F51		

Floorplan



Seminar Timetables

Business Strategy Theatre

This theatre will focus on the challenges and issues facing management, CEO's and other board level directors.

Day One - Tuesday 19th April 2011

- 10:00-10:25 **The Dangers Of Laptops, Smartphones & Social Media To Enterprise Security**
Dr. Paul Judge, Chief Research Officer, Barracuda Networks
- 10:40-11:05 **Do You See What I See - Controlling Data Accessed Via Web-Based Applications**
Case Study
Dr. Steve Garnett, Chairman & Co-President, Salesforce.com
Mr. Ed Macnair, CEO, Overtis
- 11:20-11:45 **Session reserved for theatre sponsor Oracle**
Spkr. TBC
- 12:00 -12:25 **Infrastructure Attacks - The Next Generation**
Mr. David Harley, Senior Research Fellow, ESET LLC
- 12:40-13:05 **Reasons To Be Cheerful - Part 4: What To Expect From A Data Loss Prevention Solution in 2011**
Mr. Lior Arbel, Managing Consultant, DLP, Websense UK Ltd
- 13:20-13:45 **The Cost Of Compliance**
Case Study
Dr. Larry Ponemon, Owner & President, Ponemon Institute
Mr. Dwayne Meloncon, Director Of Products, Tripwire
- 14:00-14:25 **You Cannot Afford To Ban It, So How Do You Live With Social Media?**
Miss Sian John, Distinguished Engineer, Symantec
- 14:40-15:05 **Driving Efficiency & Cost-Savings With A Secure Web Gateway: A Case Study By Institute Of Directors**
Case Study
Mr. Richard Swann, Head Of IT, Institute Of Directors speaking on behalf of M86 Security
- 15:20-15:45 **Concerns About The Cloud: What Keeps You Up At Night?**
Mr. Eugene Kaspersky, CEO, Kaspersky Lab
- 16:00-16:25 **The Hidden Security Danger - Don't Let Email Be Your Downfall**
Case Study
Mr. Justin Pirie, Cloud Strategist, Mimecast
- 16:40-17:05 **Are We Approaching A Skills Gap? If So, What Skills Are We Talking About?**
Mr. John Colley, Managing Director EMEA, (ISC)®

Day Two - Wednesday 20th April 2011

- 10:00-10:25 **Preventative Security Through Behaviour Modification - A \$100 Billion Solution**
Mr. Gorka Sadowski, Principal Solution Architect, LogLogic
- 10:40-11:05 **Success Strategies For ISO 27001**
Case Study
Mr. Boris Goncharov, IT/IS Manager, G4S Security Services
Mr. Stephane Charbonneau, CTO, TITUS
- 11:20-11:45 **Session reserved for theatre sponsor Oracle**
Spkr. TBC
- 12:00-12:25 **Dealing With Data Motility - What To Do When Your Data Decides To 'Leave'**
Mr. Rik Ferguson, Senior Security Advisor, Trend Micro
- 12:40-13:05 **Power To The People: How Empowering Your Users Will Increase Your Security Stance**
Mr. Terry Greer-King, UK Managing Director, Check Point
- 13:20-13:45 **The Top Ten Risks To Mobile Security & What You Can Do To Avoid Them**
Mr. Chris Wysopal, Founder & CTO, Veracode
- 14:00-14:25 **Users Are The Weakest Link - Goodbye!**
Mr. Greg Day, Director Of Security Strategy, McAfee
- 14:40-15:05 **Secure Mobility: Why Employees Won't Give Up iPhones & Why You Shouldn't Care**
Mr. Mark Guntrip, Product Manager, Cisco Security
- 15:20-15:45 **Convergence - The Security 'Trojan Horse'**
Mr. Ian Kilpatrick, Chairman, Wick Hill Group
- 16:00-16:25 **Setting Your Watch By Targeted Attacks: Preparing For The Worst**
Mr. Martin Lee, Senior Software Engineer, Symantec cloud
- 16:40-17:05 **Compliance Vs. Security: How Compliance Requirements Can Compete For Resources With Needed Security Projects**
Mr. Ron Perris, Chief Technical Officer, Outpost 24

Day Three - Thursday 21st April 2011

- 10:00-10:25 **Is Corporate Espionage Undermining Your Business?**
Mr. Giri Sivanesan, Head Of Policy, Risk & Compliance, Pentura Limited
-
- 10:40-11:05 **Ventura: A Case Study In PCI DSS - Beyond The Checkboxes**
Case Study
Mr. Mark Wityszyn, IT Security Manager, Ventura speaking on behalf of LogRhythm
-
- 11:20-11:45 **Session reserved for theatre sponsor Oracle**
Spkr. TBC
-
- 12:00-12:25 **Security, Privacy & The Generation Gap**
Mr. Bruce Schneier, Chief Security Technology Officer, BT
-
- 12:40-13:05 **Steps To Prevent Unauthorised Employees From Accessing Sensitive Data**
Mr. Adam Boshian, EVP Americas & Corp. Development, Cyber-Ark Software
-
- 13:20-13:45 **Are You Still Using Live Customer Data In Test & Development?! At The Forefront Of Data Security For Non Production - Yorkshire Building Society Presents A Case Study On The Successful Implementation Of A Data Masking Solution Within The Organisation**
Case Study
*Mr. Huw Price, Managing Director, Grid-Tools Ltd.
 Mr. Abid Ali, Senior Software Specialist, The Yorkshire Building Society
 Mr. Mark Bickerdike, Database & Environment Support Services Manager, The Yorkshire Building Society*
-
- 14:00-14:25 **Social Engineering VIII - Hacking The Cloud**
Mr. Ian Mann, Senior Systems Consultant, ECSC Ltd.
-
- 14:40-15:05 **Making A Difference: How Both CSOs & CISOs Are Positioning Security On The Corporate Agenda**
*Mr. Simon Marvell, Partner, Acuity Risk Management LLP
 Mr. Alan Jenkins, Director Security Risk Management & Chief Security Officer (UK & Ireland), CSC Computer Sciences Limited*
-
- 15.20-15.45 **Google's Italian Job: A Case Study In (Failed) Data Protection Risk Management**
Mr. Robert Carolina, Senior Visiting Fellow, Royal Holloway



Seminar Timetables

Technical Theatre

This theatre will cover Information Security issues and technical advances.

Day One - Tuesday 19th April 2011

10:00-10:25	Standard Controls For Standard Services - Opening Up Use Of The Cloud <i>Mr. Nick Humphrey, Security Analyst, Tier-3</i>
10:40-11:05	Defeating The Latest OddJob Virus With State Of The Art 2FA <i>Mr. Phillip Underwood, Worldwide Pre-Sales Manager, SecurEnvoy Ltd</i>
11:20-11:45	Remote Access: How Aintree University Hospital Trust Transformed Remote Access <i>Mr. Ward Priestman, Director Of Informatics, Aintree University Hospitals speaking on behalf of Cryptzone Group</i>
12:00-12:25	Can Data Be More Secure In The Cloud? <i>Mr. Andres Kohn, Vice President, Technology & Product Management, ProofPoint</i>
12:40-13:05	Reclaim Your Network Bandwidth With Application Intelligence & Control <i>Mr. Florian Malecki, EMEA Enterprise Product Marketing Manager, SonicWALL</i>
13:20-13:45	Cybercrime Is Happening All The Time - The Real World View Of Organised eCrime <i>Colonel (Ret.) Barry Hensley, Vice President Counter Threat Unit, SecureWorks</i>
14:00-14:25	Security Testing In An Age of Austerity <i>Mr. Peter Wood, Chief Executive Officer, First Base Technologies LLP</i>
14:40-15:05	The Safety Dance: How Retailers Can Achieve PCI Compliance At The Point Of Sale By Protecting Cardholder Data <i>Mr. Dave Stunt, Technical Project Manager, Marks And Spencer speaking on behalf of Bit9</i>
15:20-15:45	Securing Cloud Access Beyond Enterprise IA&M <i>Mr. Vikas Jain, Director Product Management, Cloud Identity & Security, Intel SOA Products Group</i>
16:00-16:25	Field Notes On Enterprise VoIP & UC Application Security & Vulnerabilities <i>Mr. Jason Ostrom, Director VIPER Lab, Sipera Systems</i>
16:40-17:05	Risk Assessment Is A Must For Your Organisation - Puffery Or A Reasonable Investment? <i>Ms. Mina Zele, Security Consultant, Astec D.O.O.</i>

Day Two - Wednesday 20th April 2011

10:00-10:25	Calculating TCO On Intrusion Prevention Technology <i>Mr. Graham Welch, EMEA Managing Director, Sourcefire Ltd</i> <i>Mr. Dominic Storey, EMEA Technical Director, Sourcefire Ltd.</i>
10:40-11:05	Session reserved for theatre sponsor SecurEnvoy <i>Spkr. TBC</i>
11:20-11:45	How Virgin Media Boosted Network Security Operational Efficiencies By 30% <i>Mr. Colin Miles, Head Of Technical Services, Virgin Media. Mr. Robert Civil, Regional Director UK & Ireland, Tufin Technologies</i>
12:00-12:25	A Virus Research Lab In Every Computer <i>Mr. Kuljeet Kalkat, VP Product Management, ValidEdge</i>
12:40-13:05	Opening An Organisation To Partners Not Hackers <i>Mr. Jonathan Martin, Field Technical Director EMEA, ArcSight</i>
13:20-13:45	How to be an Expert Malware Hunter in just 3 Easy Lessons <i>Mr. Alex Cox, Principal Consultant & Security Researcher, NetWitness</i>
14:00-14:25	The State Of Browser Security <i>Mr. Wolfgang Kandek, CTO, Qualys</i>
14:40-15:05	The Deployment Of Strong Authentication To Secure SEB's Online Applications <i>Mr. Niklas van Ingelandt, Head Of Identification Solutions, SEB speaking on behalf of VASCO Data Security</i>
15:20-15:45	Cyber Vigilantes: How Security Researchers Are Hurting The Business Of Hacking <i>Mr. Amichai Shulman, CTO, Imperva. Mr. Rob Rachwald, Director Of Security Strategy, Imperva</i>
16:00-16:25	How To Monitor Network Performance & Security On The College Campus <i>Mr. Adam Powers, CTO, Lancope</i>
16:40-17:05	Journey Of A Social Media Attack <i>Mr. Peter Wood, Member Security Advisory Group, ISACA. Mr. Peter Bassill, Member Security Advisory Group, ISACA</i>

Day Three - Thursday 21st April 2011

- 10:00-10:25 **How Do You Secure A 'Clouderprise'?**
Mr. Franklyn Jones, Director EMEA Marketing, Palo Alto Networks
-
- 10:40-11:05 **Two Factor Authentication Meets Self Service Password Reset**
Mr. Phillip Underwood, Worldwide Pre-Sales Manager, SecurEnvoy Ltd
-
- 11:20-11:45 **21st Century Bank Robbery: The Cybercriminals' Toolkit, Their Roadmap & How To Fight Back**
Mr. Kapil Raina, Senior Product Manager, Ironkey
-
- 12:00-12:25 **Integrated Security Vs. Best Of Breed**
Mr. Oliver Pinson-Roxburgh, Senior Sales Engineer Manager, Trustwave
-
- 12:40-13:05 **Data Leak Prevention In & Around The Cloud**
Mr. Alexei Lesnykh, Business Development Manager, DeviceLock Inc.
-
- 13:20-13:45 **Real-life Scenarios Using Tokenisation**
Mr. Gary Palgon, Vice President Product Management, NuBridges Inc.
-
- 14:00-14:25 **Penetration Testing: Is Your Website An Open Door To Cybercrime?**
Mr. Alan Calder, Chief Executive Officer, IT Governance
-
- 14:40-15:05 **25 Years Of Malware: International Cyberattacks To Turn Corporate?**
Mr. Eddy Willems, Security Evangelist, G Data
-
- 15:20-15:45 **The Fundamental Failures Of End-Point Security**
Mr. Stefan Frei, Research Analyst Director, Secunia



Keynote Theatre

The 2011 Keynote Theatre will address the security issues and pressures that organisations face in an increasingly mobile and global working environment.

It features leading experts giving analysis, end-user experience, strategic advice and predictions to ensure that you have the information you need to protect the operations of your company. From cyber-terrorism to the rise of the consumerisation of IT, the immediate threats that exist at the cutting-edge to the business community as a whole will be expounded upon.

Our increasingly technological age has made information security a critical issue that affects individuals, organisations, industry and governments alike. It is this factor that has allowed Infosecurity Europe to become a vital hub of expertise for industry professionals - creating an exciting and vibrant meeting of minds, and this year's show promises to be the most exciting yet!

The Keynote Theatre will also see the return of the Hall of Fame for 2011 - celebrating the people that the industry has voted as being the leading contributors to the advancement of information security. They will address the audience on the 20th April.

Day One - Tuesday 19th April 2011

10:00-11:00

Day 1 Keynote Address

Details for this session will be released in due course, once topic and speaker have been confirmed.

11:00-11:05

White Hat Ball Cheque Presentation

Ms. Sue Minto, Head Of ChildLine

11:15-12:15

The Effectiveness Of Information Security - When Do You Stop Spending?!

The typical information security policy of an average business today is often complex, and can therefore become inflexible and expensive, but how much of what we do do we truly need - is it simply 'cover your back security'? If so, is that actually o.k. if it's managing the perceived potential risks? Or is it simply a case of seeing beyond all the noise that's out there to what's truly important. Can you ever put the genie back in the bottle?

The session speakers will be considering these fundamental questions to determine if your information security policy is as effective and streamlined as it could be. The panel will be seeking to address:

- How do you decide if your information security policy is performing at an operational level?
- How do you decide what to monitor and measure?
- How do you audit your policy properly?
- Are we still just responding to incidents rather than the risks themselves?
- How do you know if your security is good enough?

Facilitator:

Ms. Wendy Nather, Senior Analyst, Enterprise Security Practice, The 451 Group

Panellists:

Mr. Jim Heard, Head Of Group Information Risk, Centrica PLC

Mr. Vesa Tupala, Chief Information Security Officer, SOK Corporation

Mr. Andrew Rose, Global IT Risk Manager, Clifford Chance LLP

12:30-13:30

Can You Turn Mobile Devices To Your Advantage Or Are They The Next Big Security Hole?!

Much is written and speculated around the increasing risks to the business, such as the adoption of the latest smart devices, but turning the debate on its head - Can mobile devices actually be used to improve security? Could they, for example, be used for improved authentication? There is currently less mobile malware around than that to the standard PC, and although this will inevitably change with time, the security controls available to use with smart devices, such as encryption can offer some protection - However, the fundamental question we all need to be asking is: Are smart devices secure enough for what they are currently being used for? Do the benefits to the business outweigh the risks and ultimately, how do you turn their use to your business advantage?

The session speakers will all put their arguments for and against improved security using mobile devices in

what will surely prove to be a lively debate!

Facilitator:

Mr. Nigel Stanley, Practice Leader Security, Bloor Research

Panellists:

Mr. Michael Everall, Chief Information Security Officer, LAMCO LLC - Lehman Brothers Holdings Inc.

Mr. Gary Cheetham, Chief Information Security Officer, NFU Mutual

Mr. Andrew Turner, IT Security Officer & Information Governance Lead, NHS Dumfries s& Galloway

Mr. Louis Gamon, Information Security Officer, John Lewis Partnership

13:45-14:45 **Don't Forget The Users - How To Make Them Your Biggest Ally**

A business, as everyone knows is only ever as successful as those people it employs. When it comes to effective information security your workforce are your number one asset and with the right training and risk awareness they can be the eyes and ears for the business beyond the IT security infrastructure that is in place. However, without the proper risk awareness they can also pose a significant threat - be it knowing or unknowingly - especially today as we start to see the increased use of employee-owned IT in the workplace and the explosion of social media.

This discussion will highlight the key factors to incorporate into any employee awareness training, especially how best to make people care by making them relate to the corporate risks in the same way they would towards personal risk.

Facilitator:

Ms. Jinan Budge, Senior Analyst, Forrester Research

Panellists:

Mr. Mark Logsdon, Director, Information Risk Management, Barclays

Mr. Martyn Styles, I.T. Security Team Leader, Global I.T. Service Delivery, Allen & Overy LLP

15:00-16:00 **The Economics Of Security - Can You Cut Your Budget And Bolster Security?**

It's true to say that for the majority of organisations we are all operating in a very different financial environment post-recession. Budgets have been cut and restructured, but on the other hand we have also seen large sums committed to security from the Government too! So where exactly are we? How

can you deploy technologies that maximise your existing security infrastructure and where are the smart investments?

The panel will consider all of these core issues and pose the opening conundrum: "If you had to lose 30% of your security budget in the next 24 hours, what would you lose and why?"

Facilitator:

TBC

Panellists:

Mr. Tom Whipp, Head Of Security, Governance & IT Compliance, The Oval Group

Mr. Spencer Mott, CISO, Electronic Arts

Mr. Matt Holland, Head Of Information Security, NSPCC

16:15-17:15 **Advanced Persistent Threats - Hype Or Reality?**

Much has been, and continues to be written and spoken about today's modern threat landscape, but one thing is clear: It's vast, complicated, sophisticated and cybercrime is seriously big business! However, just how persistent are the threats? Do we need to be so concerned or should we go so far as to say that cybercrime truly is the scourge of the 21st Century? It seems fair to say that any under-defended business that finds itself faced with a coordinated attack could risk so much damage to both reputation and therefore livelihood that it is simply essential to take an accurate assessment of your current defences!

This session will therefore undertake an accurate review of the types of attacks and threats faced over the last 12 months, looking at trends and the geographics of attacks for example, as well as the costs incurred to allow you to consider if your security strategy is currently enough and what contingencies you should be putting in place!

Facilitator:

Professor John Walker, Professor Of Science & Technology, School Of Computing & Informatics, Nottingham Trent University

Panellists:

Mr. Mario Kempton, D/DSO & Head Of Information Security, Serious Organised Crime Agency

Mr. Ionut Ionescu, Head Of Threat

Management, Betfair

Mr. Stephen Kerslake, Group Information Security Governance, Virgin Media

Day Two - Wednesday 20th April 2011

10:00-11:00 **Keynote Address: Data Protection: Stronger Enforcement, Greater Encouragement & A Bright Future**

Following on from David's presentation at last year's Infosecurity Europe, where he considered the then new powers of the Information Commissioner and the potential impact and likelihood of fines, David will summarise the developments over the last 12 months, providing an update on the increased powers of the Information Commissioner to assess organisations compliance with data protection laws and new powers to impose fines of up to £500,000 for significant breaches.

Furthermore, the Commissioner's new tools and guidance to help organisations ensure compliance in the first place will also be featured, as will the changing data protection landscape and, in particular the outlook for compulsory breach notification in the UK.

Speaker:

Mr. David Smith, Deputy Commissioner & Director Of Data Protection, Information Commissioner's Office

11:15-12:15 **The Great Debate: Social Media - What's The Problem?**

In today's modern business the use of social media within marketing strategies is becoming commonplace, but can an organisation ever fully adopt social media into its working practices, or are the perceived risks to the business too great?

This session will put forward arguments both for and against incorporating social media into business practice, covering some of the core issues such as:

- How can you control the risks posed to your brand?
- How do you successfully incorporate the use of social media into your IT policies?
- Can blocking ever truly be a real protection / solution and what are the legal implications of doing so?
- How do you control inappropriate behaviour?
- Privacy and managing anonymity in a business context
- Employee education - Is your acceptable use policy social media proof?
- Where has it worked - Success stories

Facilitator:

Mr Bryan Glick, Editor-In-Chief, ComputerWeekly

Panellists:

Mr. Graham Taylor, Head Of IT Security (UK & Asia Pac), Michael Page International

Mr. Steve Whittle, CTO,

The Cobra Group Of Companies

Mr. David Cripps, CISO, Investec Bank Plc.

Mr. Adrian Price, Head Of Information Security (Pol), MoD

12:30-13:30 **Hall Of Fame 2011**

The history of computing and information security has attracted many brilliant minds that have dedicated their lives to its advancement. This year's Infosecurity Europe is proud to once again host the Hall of Fame in the Keynote Theatre, where internationally recognised inductees will be sharing their expertise. The speakers in the Hall of Fame are voted for by professionals in the industry as having met the following criteria:

- He/she is an internationally recognised and respected information security practitioner or advocate
- He/she has had a clear and long-term contribution to the advancement of information security
- He/she has provided intellectual or practical input that has shifted the advancement of information security
- He/she is an engaging and revolutionary thought leader in information security

Facilitator:

Mr. Edward Gibson, 2010 Hall of Fame Inductee & Director – Forensics Technology Services,

PriceWaterhouseCoopers

Ms. Neira Jones, Head Of Payment Security, Barclaycard

Inductees:

Mr. Graham Cluley,

Senior Technology Consultant, Sophos

13:45-14:45 **What Compliance Juggernauts Are Coming Down The Road For Security?**

There is a huge raft of legislation and regulations surrounding the information security industry, and when you consider a globally-operated business environment, it can feel confusing and difficult to see where you need to comply and invest, turning

what's originally intended to protect and assist into something that can almost be seen as a threat - a regulatory threat!

The panel will therefore carefully assess where to prioritise and also what's coming down the road in terms of legislation and compliance that we all need to be aware of, including:

- How good security delivers compliance
- The legality of email and eDiscovery
- Forensics
- The challenges and opportunities of PCI DSS
- Cloud and the Data Protection Act
- BS27001 and other standards
- The implications of employee-owned IT in the business environment
- The privacy debate and implications to business

Facilitator:

TBC

Panellists:

Ms. Gaynor Rich, Head of Infosec and Payment Services - GRBA, Capita Group Plc.

Mr. Marc Goodman, Senior Advisor, Steering Committee On Information Technology Crime, Interpol

Mr. Stewart Room, Partner, Field Fisher Waterhouse LLP

Mr. Simon Salmon, Head Of IT Strategy & Security, Nottingham City Council

implications to employer and employee

- The HR issues to consider
- Forensics issues and how to trace
- Evolving the role of the IT department
- Classification of data - Its now more than ever about the data than the devices
- Dealing with assurance and trust around the data transfer
- How do you provide adequate support and maintenance for a multitude of devices?

Facilitator:

Mr. Paul Dorey, Chairman, Institute Of Information Security Professionals

Panellists:

Mr. Mark Brown, Group CISO, SABMiller

Mr. Chris Parker, Senior Vice President & CIO, Business Information Management, LeasePlan Corporation N.V

Mr. David Ripper, Head Of Information Systems & Technology, Sue Ryder

Mr. John Harris, Chief Architect & VP Of Global IT Strategy, GlaxoSmithKline

15:00-16:00

The Consumerisation Of IT -

The Dawn Of The B.Y.O. Business

One of the biggest trends in recent months has been the rising tide of consumerised IT, largely fuelled by the latest smart phones and 'must have' devices, such as the iPad, crossing the boundary from home to the office environment. The boundaries are in fact now often so blurred it can be difficult to see where one starts and the other ends! However, the business can see huge cost-savings from the adoption of employee-owned IT to its IT infrastructure - But do these savings ever outweigh the posed risks and additional support costs?

Clearly the issues around security need very careful consideration in order to create a roadmap for successful employee-owner IT adoption. The speakers on this session shall therefore consider:

- The legal situation - Risk ownership and



Day Three - Thursday 21st April 2011

10:00-11:00 Day 3 Keynote Address

Details for this session will be released in due course, once topic and speaker have been confirmed.

11:00-11:05 White Hat Golf Day Cheque Presentation

Mr. Steve James, Group Chief Executive, Avenues Trust

11:15-12:15 Can An Insider Really Take Your Business Down?

It could be said to be one of the biggest risks faced by any organisation - insider threat from those working for you - but what percentage of actual incidents can be attributed to a disgruntled or infiltrated insider? With ever widening security perimeters no one would disagree that there are many more factors to consider these days, particularly with an extended enterprise and deciding how much and what to share with your suppliers and customers. So what about your own people?

The panel will be considering insider threat in 2011, particularly with the adoption of employee-owner IT to the workplace and how you can best manage the risks, including:

- Event monitoring and management
- Supplier sourcing and due diligence
- Identifying vulnerable staff
- User behaviour analysis and privacy issues
- Strategies for redundancy programmes and managing those left behind
- Staff education and awareness to the security risks, including social engineering
- Social media policies and mitigating the risks
- Senior management policy enforcement and the importance of setting the trend

Facilitator:

Mr. Andrew Kellett, Senior Research Analyst, OVUM

Panellists:

Ms. Vladislava Toukalek, Head Of IT Infrastructure & Support Services, Information Technology Division, World Meteorological Organisation

Mr. Robin Smith, Head Of Information Governance, Northampton General Hospital

12:30-13:30 Securing The Cloud - Shining A Light Through The Fog!

Cloud computing - The buzz word on everyone's lips, however it would seem that everyone has a different opinion about it, especially when it comes

to the thorny issues around security in the cloud!

The speakers on the panel will be attempting to cut through the fog and provide some guidance to consider when debating cloud, such as:

- How many clouds are there anyway?
- BC planning - thinking wider than your infrastructure
- The transparency debate and who owns what and when?
- The geographic's of cloud - Compliance issues and jurisdiction
- How to push the debate beyond cost-savings
- What's the value of network security when you move to the cloud?
- How NOT to build a cloud?

Facilitator:

Mr. Bob Tarzey, Director, Quocirca Ltd. & Blogger, Infosecurity Network

Panellists:

Ms. Neira Jones, Head Of Payment Security, Barclaycard

Mr. Jason Witty, Senior Vice President, International Information Security Executive, Global Information Security, Bank Of America Corporation

Mr. Johannes Denissen, Head Of Information Security, DAF Trucks

13:45-14:45 It Wasn't Me, It Was Bennett Arron

A real life identity theft case study. Bennett Arron was in debt. He owed thousands of pounds to phone companies, department stores and banks. Only, it wasn't him.

Bennett is an award-winning writer and stand-up comedian. In his talk he gives a disturbingly true and funny account of what it's like to have your identity stolen.

Speaker:

Mr. Bennett Arron



Security Workshops

The Security Workshops are an educational forum for both discussion with your peers, and individual learning, catalysed by an industry-expert facilitator.

Each and every session is carefully designed to ensure you stay ahead of the game with the latest industry trends and developments, leaving the session with the right tools to take back to the office for both your own personal development and to share with your colleagues.

The Infosec Europe Security Workshops are an invaluable, free-to-attend opportunity for those visitors looking to gain a little more knowledge into the current

hottest industry trends – but don't just take our word for it, here's what some of last year's attendees had to say about the workshops that they attended:

"A great use of my time!" –

2010 Workshop attendee from HBOS

"Very good speaker – short, sharp and to the point.

Very informative and relevant session!" –

2010 Workshop attendee from Symantec

Places are limited; therefore pre-registration will be available in advance – Please check www.infosec.co.uk for further details and registration information.

New for 2011 The Information Security Exchange Theatre

The new Information Security Exchange theatre offers both high-level debate around the latest, cutting-edge technical developments and challenges, as well as insight into the most controversial and difficult business-issues currently faced within the end-user community.

This new theatre for 2011 will put together a combination of end-user and vendors speakers, to share experiences on their latest projects and challenges in a host of varying formats – From stand-alone presentations, to presidential-style debates, panel discussions and chat-show style interviews!

Discussions therefore promise to be lively and progressive, and will certainly leave you talking long after they are over!

To see the full agenda, please visit www.infosec.co.uk



New Products and

Infosecurity Europe is the event where new products and services are launched, here is a brief glimpse of what you can see at the show.

ACUITY

RISK MANAGEMENT

Stand F81

Email info@acuityrm.com

Visit www.acuityrm.com

Call +44 (0) 20 7297 2086

Acuity Risk Management

Acuity launches a free single-user version of STREAM Integrated Risk Manager. From March 2011, the popular GRC product is available for download from Acuity's website www.acuityrm.com together with documentation and training.

This fully functional product will allow users to build their own GRC solution or download Acuity's pre-configured applications which include ISO 27001, BS 25999 and ISO 9001. You can use STREAM to automate individual risk applications, such as an Information Security Management System (ISMS), or as an integrated Enterprise Risk Management (ERM) system.

STREAM provides real visibility into your risk and compliance status for business managers, translating risk assessments, key control performance metrics and incidents into easily understandable management information.

Easy to configure and intuitive to use, STREAM provides actionable intelligence and assurance that your GRC processes are meeting your business need. Optional support, training and consultancy services and upgrades to the Enterprise edition are all available from Acuity.

NETWITNESS

Stand F72

Email info@netwitness.com

Visit www.netwitness.com

Call +1 (703) 889-8950

NetWitness – Introducing Spectrum and Visualize

NetWitness Spectrum™ – A Revolutionary Approach

Spectrum revolutionizes malware identification, prioritization and workflow. Built upon the award-winning NetWitness® network monitoring platform, Spectrum has the unique advantage of pervasive enterprise-wide visibility and complete knowledge of all network activity. Spectrum identifies executable content wherever it exists, and can answer any question about the behavior of files within the full context of your organization's network.

NetWitness Visualize™ - Instant Visualization

Visualize presents application and user content in a revolutionary way. Visualize is an extremely powerful analytical capability that enables a user (e.g. an analyst, incident responder, investigator) to zoom in and out of collected traffic using their mouse or fingers, if equipped with a multi-touch monitor, and to drill down and see exactly what transpired over the course of time. Visualize enables users to leverage all the rules, keyword searches, and other filters created in Informer to further refine and process the presented information.

Services



NRI SecureTechnologies, Ltd.

SecureCube Secret Share - Secret Sharing based Data Management Service. The cloud computing has already become commodity, and many organizations are expecting the cost effectiveness by its deployment. However, a lot of security issues prevent organizations from leaving the data in the cloud. We introduce a new way that adapts "the secret sharing scheme" to the cloud computing.

This service manages to store the company's sensitive information by dividing data files into several data center locations. It solves many problems such as data leakage, data management, disaster recovery, mobile computing etc.

With SecureCube Secret Share, you gain the following business benefits:

- Ultimate Backup and No Need Server Operations
- Flexible Operations from Individual to Company Share Folders
- Anytime, Anywhere and Any PCs to Access the Files Safely with the Secured Connection

We are seeking a OEM/Sales partner with the skill of adapting this new technology.





New Product Launches

Here is a brief glimpse of some of the exhibitors launching new products at Infosecurity Europe 2011.

3M (UK) Plc [C82] 3M showcases laptop privacy filters that help protect business professionals and security executives against visual security breaches when working in public environments. Available in black and gold, the filters are simple, reliable protection tools that fit neatly over laptop and desktop screens, and can be readily removed and stored when privacy is not required.

Acuity Risk Management [F81] Acuity launches a free single-user download of STREAM Integrated Risk Manager. From March 2011, the popular GRC solution is available from Acuity's website www.acuityrm.com. This fully functional product allows users to build their own GRC solution or use Acuity's pre-configured applications which include ISO 27001, BS 25999 and ISO 9001.

Astec d.o.o. [K96] 'ARAT 4.0' is the latest release of Astec Risk Assessment Tool, featuring audit trail logs and information asset grouping. Audit trails provide complete traceability of all actions performed by application users. Information asset grouping simplifies risk assessment procedure and improves results overview. ARAT can be fully adapted to organizational needs.

Avecto [L70] Avecto showcases 'Privilege Guard' technology which enables organizations to empower Windows based desktop and server users with the privileges they require to perform their roles, without compromising integrity or security of their systems.

AwareGO [H96] AwareGO launches a multilingual, flash based security awareness training solution for hassle free security awareness deployment for international corporations. Customized training, subtitles and branding available.

Caretower Limited [F20] Caretower Limited's 'AuthenWare Technology' is an Identity Authentication Solution that verifies that the person typing a user ID and password is the actual owner of those credentials, based on innovative, proprietary biometric technology that requires nothing but a normal PC logon. It practically eliminates the risk of Identity Theft without the need for any additional hardware or any change in the most popular logon method.

City University London [J51] City University London's Centre for Software Reliability (CSR) has led research into the assessment of dependability of computer-based systems since the 1980s, offering consultancy and training to government, regulators and industry. At Infosecurity Europe, CSR is launching a new Masters course to prepare experienced professionals for management roles in information assurance, security and risk.

CRYPTOCARD Europe Ltd [B43] CRYPTOCARD provides the ability to access networks and applications without compromising security by using appropriate authentication to secure digital identities. Offering an innovative combination of token and token-less solutions via a cloud service or server application, CRYPTOCARD supports organisations' existing security policies and desired authentication frameworks in over 70 countries.

Cryptosoft [J79] Cryptosoft encryption service platform. Cryptosoft launches first encryption service platform, for scalable on-premise, virtualised, hosted and cloud deployment which reduces cost and complexity of managing cryptography while retaining the value of existing security management tools and processes. Cryptosoft offers scalable encryption for any data type, from any application delivered to any destination.

Data Robotics, Inc [K75] Built on proven BeyondRAID technology, Data Robotics, Inc. showcases iSCSI SAN storage, for SMBs, with advanced capabilities usually reserved for enterprise solutions. It's designed to provide reliable and high performance storage for business-critical applications like server virtualization. The powerful 12-bay B1200i model adds Data-Aware Tiering and redundant, hot-swappable components to ensure high-availability of business applications.

Deep-Secure Ltd. [A40] Deep-Secure showcases the 'Deep-Secure Network Management Guard' which controls the flow of network management traffic passing between separate networks and enforces strong data sharing policy. Built upon the EAL4 DeepSecure® technology platform it lowers the cost of network management; improves operational efficiency and compliance; and provides high assurance and risk mitigation.

DeviceLock, Inc. [D42] DeviceLock, Inc. is launching the latest version of its product – 'DeviceLock 7.0 Endpoint DLP Suite'. In addition to its device access control features, functionality is extended with content filtering and network communication control. This gives businesses an effective and economical solution for protecting endpoint computers against data leaks.

ElcomSoft [C32] Elcomsoft showcases the 'Elcomsoft Phone Password Breaker' (EPPB) gets access to password-protected BlackBerry, iPhone, iPad and iPod backups. Supporting all versions of BlackBerry and Apple smartphones released up to date, EPPB is the first GPU-accelerated tool, which employs NVIDIA & ATI cards, as well as Tableau TACC1441, to obtain original passwords.

Faronics [J92] Faronics showcases 'Anti-Executable 4' that halts even the most advanced malware threats, such as zero day and targeted attacks including spear phishing, by only allowing approved applications to run on a computer. Any other programs - whether they are unwanted, unlicensed, or simply unnecessary - are blocked from ever executing.

Gridsure Limited [G94] Gridsure's new 'Gridsure Authentication Platform' (GAP) enhances the security of remote access and web applications by replacing traditional passwords with a unique, pattern based authentication method. By asking users to select an individual sequential pattern on a grid with randomly generated numbers, the software solution creates a one-time passcode at every login.

Identiware B.V. [L87] Identiware's 'Diggtrade HS256' is a new line of external hard drives with two-factor authentication and 256-bit AES encryption. Before access is granted to the data individuals must utilize a SmartCard & input a corresponding pincode. The HS256 is fast, safe and easy — the ideal solution for safe storage of data for large enterprises & government.

Imperva [B60] Imperva will demonstrate new attack schemes and models as uncovered recently in their research labs. Their findings are a result of their hacker intelligence initiative (HII). This work allows Imperva to recognize the source of attacks, and subsequently, to provide an out-of-the-box defense against automated attacks. Imperva's offering of ThreatRadar, an add-on to their Web Application Firewall (WAF) provides automated, reputation-based defense against large scale industrialized cyber attacks. By integrating credible, timely information on known attack sources into the WAF defense, ThreatRadar can quickly and accurately stop traffic from malicious sources before an attack can be launched.

IronKey, Inc [F30] Ironkey will be launching its 'Trusted Access for Banking' (TAB), which allows commercial banks to protect their users and transactions. TAB allows clients to use their existing online accounts and money transfer systems within the confines of a locked-down, portable virtual environment. To protect users from ever-changing malware, TAB does not rely on potentially compromised and vulnerable applications on the user's host computer.

Ixia [J76] Ixia's 'IxLoad-Attack' measures the performance of network security appliances validating that they effectively and accurately block attacks while delivering high end-user quality of experience for mission-critical applications. IxLoad-Attack delivers the security testing depth and scale needed to satisfy both device validation and continuous protection of cloud infrastructures as well as enterprise, government, and service provider networks. IxLoad-Attack is the only product that provides malicious traffic over both encrypted (Ipsec and SSL) and non-encrypted links.

Kobil Systems [E50] mlDentify 3G - Stay connected. Be secure. mlDentify 3G is a unique smart card reader with encrypted memory with an integrated 3G modem all in a compact USB form factor. mlDentify 3G ensures highly secure and easy global communication whilst simultaneously its state-of-the-art security technologies protect your data and digital identity against third party attacks

LANDesk [B10] LANDesk will be previewing its 'Service Desk 7.4', a significant upgrade to the LANDesk IT Service Management solution, which allows organisations to automate processes, reduce IT costs, and deliver outstanding service to both employees and customers. Specific enhancements include LANDesk Self Service; the addition of the LANDesk Service Catalogue; and enhancements to LANDesk Web Desk

Lieberman Software Corporation [F52] Lieberman Software Corporation, the Pioneers of 'Privileged Identity Management', will release significant product upgrades including new cloud security capabilities, out-of-the box integration with leading SIEM, helpdesk and incident recording solutions; and expanded wizard-driven support for the largest number of hardware and software infrastructure platforms of any supplier in the marketplace.

LogRhythm Ltd [G51] LogRhythm showcases 'Advanced Intelligence Engine' (AI Engine) is a next-generation analytics platform providing highly scalable, real-time, in-memory analysis of all log data. AI Engine enables organisations, without writing any scripts, to detect sophisticated intrusions, fraud, insider threats, zero-day attacks, advanced persistent threats (APT) and other suspicious activity that would otherwise go unnoticed.

Mancala Networks [J88] Mancala Networks will be showing off 'The Network Controller' which enables real-time, automated network behavior analysis and security policy enforcement. Its unique combination of device identity profiling and dynamic control flow analysis enables it to detect abnormal behavior, and to immediately mitigate security breaches anywhere in the network.

McAfee International [C60] McAfee is the world's largest dedicated security technology company. Backed by McAfee Global Threat Intelligence, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling regulatory compliance, data protection, disruption prevention, vulnerabilities detection, and continuous security monitoring. McAfee secures your digital world.

MXI Security [G78] MXI's 'Stealth Key M600' is the first encrypted flash drive to receive CESG CAPS accreditation. Offering encrypted storage of your most critical data, along with superior manageability, the device is a cost-effective USB portable security device for organizations of all sizes.

NetWitness [F72] NetWitness' 'Spectrum' revolutionizes malware identification, prioritization and workflow. Built upon the award-winning NetWitness® network monitoring platform, Spectrum has the unique advantage of pervasive enterprise-wide visibility and complete knowledge of all network activity. Spectrum identifies executable content wherever it exists, and can answer any question about the behavior of files within the full context of your organization's network.

nitrosecurity [A44] NitroRSC Correlation Engine - NitroSecurity will be demonstrating the revolutionary 'NitroRSC Correlation Engine' which can calculate a "risk score" based on the asset value, vulnerability profile and event scoring. IT managers can proactively evaluate risks and effectively identify emerging threats based on the scores.

NitroView ESM X3 SIEM Appliance - The 'ESM X3' can collect up to 150,000 network events per second and can concurrently analyze up to 40 billion events. The ESM X3 has blazing fast performance and keeps months of data online and instantly accessible with 320GB of SSD and a 7TB hard disk drive balance speed with reliability.

nuBridges Inc. [E82] nuBridges will be launching the 'nuBridges Protect Tokenization as a Service' (TaaS), which is the first cloud-based data tokenization service for national and multi-national companies that want to protect Personally Identifiable Information (PII), Electronic Health Records (EHR) or cardholder information to improve security, reduce risk, ease compliance and minimize data security costs.

Oracle Corporation UK Ltd [AA90] Oracle Corporation's new 'Database Firewall' offers organisations a first line of defence that can stop internal and external attacks from reaching databases. Easy to deploy, the Firewall helps reduce costs and complexity of securing data across the enterprise without changes to existing applications and databases.

Origin Storage [F83] Origin Storage, the UK based IT storage solution provider will be launching 'DataLocker 3' an external USB 3 pin encrypted hard drive at Infosecurity Europe 2011, also on show will be Enigma SED (latest generation) range which can be inserted into PC laptops to automatically secure any stored data on the move.

PixAlert [A73] PixAlert help protect organisations against the risk of unsecure, critical or sensitive data loss and inappropriate image content storage/distribution. PixAlert showcases unique auditing and real-time monitoring solutions improve business practice and compliance to international standards. Helping safeguard corporate integrity and reputation through market leading data and image discovery software and services

Rittal Limited [D81] RiZone, Rittal's new IT management software, along with Microsoft's System Centre Operations Manager (SCOM), represents the first commercial software which extends beyond the infrastructure components and allows the power consumption monitoring of all devices enabling real energy savings to be easily achieved.

SAIC LIMITED [C45] Ranked 3 by FORTUNE among the World's Most Admired IT Services Companies 2010, SAIC is one of the world's leaders in IT and telecommunications networking. SAIC's approach to cybersecurity services provides government and commercial enterprises with solutions to effectively manage risk and protect business-critical data.

Sangfor [A53] Sangfor's range of WAN Optimisation solutions delivers significant improvement in WAN performance for all types and sizes of business. Sangfor's solutions can realistically achieve 30-60% reduction in data transmitted, bandwidth utilisation increases of 30-80% and data transfers up to 60 times faster.

SearchSecurity [L61] The editors of SearchSecurity.co.uk, SearchSecurity.com and Information Security Magazine Online are now publishing INFORMATION SECURITY EZINE EUROPE, an EZINE developed exclusively for our European audience. Each quarter our award-winning editorial will provide practical strategies and tactics that will help IT Security Professionals secure their organizations' data, networks, applications and users.

Secunia [B81] Secunia's 'Vulnerability Intelligence Manager' (VIM) is a powerful next generation Vulnerability Intelligence and Management tool for rapid handling of emerging threats - an integral part of the overall risk management process. It delivers key intelligence to effectively analyse, track, and eliminate vulnerabilities in IT infrastructures from a centralised dashboard interface.

The Secunia 'Corporate Software Inspector' (CSI) simplifies the patching of third-party programs with automated patch repackaging, integrated with Microsoft WSUS and SCCM. It is a non-intrusive authenticated vulnerability and patch scanner which identifies the security status and missing security patches for thousands of installed vendor programs and plug-ins.

SecurEnvoy [E60] SecurEnvoy showcases SecurEnvoy Suite 5.4, a collection of four two-factor authentication solutions including SecurAccess and SecurPassword. Part of this updated suite of programs is SecurMail, which gives users the option of sending FIPS140-approved AES-256 encrypted emails to any recipient even if the recipient doesn't have any encryption software. All that is needed to send a safe, secure email is the recipient's email address and mobile phone number- SecurMail does the rest.

Sipera Systems [H50] Sipera Systems is unveiling the 'UC-Sec v4' security appliance, providing comprehensive security in a single appliance for VoIP, IP video conferencing, collaboration, and other real-time communications applications. With UC-Sec, for the first time, security managers have complete security control over Unified Communications (UC) applications moving through their networks in real-time.

SiVizion [J90] SiVizion is an Email & Documents exchange solution that prevents data leakage. SiVizion's innovation is a DVI dongle. The dongle links between a computer and a monitor. At the server Email's content is converted into encrypted images. These images are captured by DVI dongle, decrypted and sent directly to display.

SonicWALL [E61] SonicWALL showcases SuperMassive E10000 Series - SonicWALL's Next-Generation Firewall platform designed for large networks to deliver scalability, reliability and deep security at multi-gigabit speeds. Built to meet the needs of enterprise, government, university, and service provider deployments, the SuperMassive E10000 Series is ideal for securing enterprise networks, data centers and server farms

SureCloud [F92] SureCloud is launching its new Risk and Compliance Management modules; further enhancing vulnerability management by incorporating business asset risk. Increased functionality also enables IT managers to automate labour intensive manual processes; thereby expediting the process of compliance with standards such as PCI DSS and GCSx CoCo.

Systematic Development Group [F73] The Systematic Development Group is launching its 'LOK-IT Secure Flash Drive', which is now FIPS 140-2 Level 3 Certified. LOK-IT delivers unparalleled security and convenience, utilizing an onboard PIN-pad for authentication. LOK-IT is the first truly platform independent secure USB drive and additionally features 256-bit AES hardware encryption and a waterproof anodized aluminum casing with filled epoxy.

Titus Labs [J61] Titus Labs are launching its new product TITUS Aware, which prevents email data loss by bringing user driven security to the desktop, where users are educated on security policy and given the ability to remediate potential data breaches before they happen. Integrated into Microsoft Outlook, the solution complements an organization's data loss prevention strategy by involving the most important part of security: the user.

Trend Micro (UK) Ltd [D10] Trend Micro launches 'SecureCloud 1.1' – a policy-based key management and data encryption solution for public and private cloud-computing environments. Users can manage encryption keys from Amazon EC2, Eucalyptus and VMware vCloud environments from Trend Micro's hosted SecureCloud service or from a SecureCloud key server running in their data center.

Tufin Software Technologies Ltd [G82] Tufin Technologies, the leading provider of Security Lifecycle Management solutions, will showcase, version 5.3 of its award-winning 'Tufin Security Suite' (TSS), which features enhanced firewall operations management functionality and updated PCI DSS 2.0 compliance reporting. They are also the first firewall management company to offer comprehensive support for next-generation firewalls from market leaders such as Palo Alto Networks.

Venafi, Inc. [AA52] Venafi showcases its 'Encryption Director 6TM'. This provides automated management for the widest range of enterprise digital certificate and encryption key technologies including symmetric keys, SSH keys, asymmetric keys and digital certificates. Venafi provides the only platform that allows organisations to automate discovery, monitoring, validation, management and security of encryption assets.

ViaSat UK, previously Stonewood [E41] Eclipt Orion Central Management System ViaSat UK, previously the Stonewood Group, is proud to announce that Eclipt Orion, the Central Site Manager for Eclipt Internal, Eclipt Freedom and Eclipt Nano hardware encrypted drives, is now shipping in volume. Eclipt Orion allows easy-to-use remote initialisation and central management of configuration and authentication parameters and audit functions.

News

SureCloud achieves PCI ASV re-certification

SureCloud has achieved its PCI Approved Scanning Vendor (ASV) re-certification, meeting the new stricter ASV Program Compliance Guidelines, intended to combat the evolving global fraud and theft threat to the payment card industry.

“Our commitment to our customers is to ensure that they can rely on our expertise to simplify and de-mystify the compliance process and enable them to achieve mandatory

compliance, whatever market and regulatory changes occur, and without incurring unnecessary costs or delays,” said Richard Hibbert, CEO, SureCloud Ltd.

The PCI DSS v.2.0 is a multi-faceted international security standard covering people, processes and technology that must be adhered to by all organisations that store, process or transmit cardholder data or sensitive authentication data.

Ixia unveils test system

Ixia has recently unveiled IxLoad-Attack, its network vulnerability test tool. With a comprehensive database of more than 6,000 unique attacks, IxLoad-Attack recreates malicious traffic that exploits vulnerabilities and generates Internet-scale distributed denial of services (DDoS) attacks in a controlled environment.

IxLoad-Attack measures the performance of network security appliances, validating that the technologies effectively and accurately block attacks while delivering high end-

user quality of experience. It also includes an update service to keep pace with current security threats, ever-increasing in type, number and virulence. Jeff Wilson, Analyst at Infonetics, commented: “This highly dynamic security environment drives the need for continuous testing with solutions like Ixia’s”. Ixia’s scalable technology allows network equipment manufacturers to ensure their devices provide the protection and performance needed by enterprises and service providers.



Secure mobile VPN for iPhone® and iPad®

Cryptzone's Appgate solution extends mobile support with the release of a mobile client for Apple iPhone® and iPad®. Users are now able to log securely into the network and safely gain access to corporate information.

More "intelligent" and versatile smart phones virtually eliminate the need for many mobile workers to carry a laptop. However security concerns have deterred some IT departments from supporting a new generation of roaming information workers.

With Cryptzone's Appgate Secure Mobile VPN, organizations can be confident that their smart phone users have secure access to corporate information and network applications quickly and easily.

The latest mobile client enhances the wide range of mobile platforms already supported by Cryptzone's Appgate Security Server, offering a real opportunity for people to work more productively and securely whilst on the move.



ActivIdentity joins HID Global

HID Global has announced the completion of its parent company ASSA ABLOY's acquisition of ActivIdentity. The acquisition will expand HID Global's logical access offering and create a unique portfolio of converged physical and logical access solutions. These solutions will enable existing and future enterprise, financial services and government customers to meet their security and compliance requirements with a broad range of user authentication products.

ActivIdentity's solutions are used to confidently establish a person's identity for digital interactions, also known as logical access control. There is growing demand to combine this capability with the kinds of solutions that HID has traditionally offered for physical access control and secure card issuance. These converged solutions will enable a single smart card to support multiple authentication methods and enforce policies throughout the enterprise, providing multilayered security across company networks, systems and facilities.

Newly discovered threats

Stonesoft has announced the discovery of new, advanced evasion techniques (AET) that can pose a serious threat to existing network security systems worldwide.

Discovered in Stonesoft's research labs in Helsinki, AETs essentially provide cyber-criminals with a master key to access any vulnerable systems and as a result, companies may suffer significant data breach including the loss of confidential corporate information.

Stonesoft cautions that hackers may already be using AETs in advanced, targeted attacks. With only a select few products available to provide protection, organisations may be challenged to protect their systems quickly.

The best defence against the dynamic and ever-evolving nature of AETs is delivered through flexible, software-based security with remote update and centralised management capabilities, such as Stonesoft StoneGate network security.

Secure remote v

Marc Hocking, Chief Technology Officer, Becrypt, discusses one answer to meeting the Government's Austerity Measures.

The public sector is facing rationalisation of a magnitude never seen before. To meet the new austerity measures it is not just a case of cutting budgets by 10 or 20%, different ways of working must be found.

Financial resources are now focused on providing front line services, quangos are being cut and the government is planning to rationalise its property portfolio. With offices closing and the drive to reduce costs, there is a push to remote working - whether hot desking or working from home.

However, remote working introduces new challenges. Organisations need to think carefully about the solution; the initial purchase, the total cost of ownership; how the software is deployed to employees; how assets are managed; and the ongoing management of the solution, as well as data security.

For government departments, local authorities and the NHS security is high on the agenda. The Codes of Connection, DPA, PCI Compliance (particularly for local authorities that process payments from citizens) or compliance with the HMG Security Policy Framework, mean that any deployed solution must be accredited.

Whether issuing laptops or allowing today's IT savvy employees to use their own home computer, both options must offset mobility against the security risks. The government has also stated a desire to move to the G-Cloud (industry and private sector are also

moving this way) and hosted virtual desktops.

So what type of solutions are available? The traditional approach for staff working from their home PC is that a virtual environment is run on the host PC. A host checker examines the host operating systems (OS), but as it is going through any malicious code on the PC, it can be misled into thinking that everything is OK. Some key loggers can be installed as root kits, and are not detected by virus scanners, enabling screen grabs to be taken of the virtual environment and compromising security. This, as well as data leakage, is one of the many risks of remote working.

An alternative approach is a solution that assumes that the host computer is compromised and restarts it, booting into a corporate OS image. This provides a trusted environment from the start, because it is totally isolated from the host computer's OS. As the host hard drive is not accessed, there is no cross contamination of malicious code.



working

No data can be saved locally which stops data leakage.

Such a solution can be used equally well with an employee's home PC (or with work- issued Netbooks or laptops for additional security) as only the keyboard and mouse are used. Users have access limited to the

Some forward looking local authorities already have introduced business cases for flexible working policies to improve partnership working, particularly in the areas of social care and children's services. By deploying an effective, secure solution, these projects have also addressed other targets including green travel objectives, reducing office space, reducing costs, improving staff morale and increasing staff productivity.

“ The government has also stated a desire to move to the G-Cloud (industry and private sector are also moving this way) and hosted virtual desktops ”

network drives and files that they need to do their job and they are not able to install any additional applications.

These centrally deployed solutions are of low cost to purchase and to manage. Security aspects are built in to meet government controls and they can be integrated with VMware and Citrix.

Central deployment saves considerable management time and cost and because users can have the same version of the software, whether they are using it in the office or at home, user uptake is maximised and training minimal.



40% of Global Executives Block Move to the Cloud

Forty percent of C-level executives have stated that they are not planning to adopt cloud computing, according to the fourth Global Status Report on the Governance of Enterprise IT conducted by ISACA.

Respondents who do not plan to use cloud computing at all in the near future list security (47%) and privacy concerns (50%), followed closely by legacy infrastructure investments (35%), as barriers to adoption. Of the executives who use or plan to use cloud computing for IT services 60 percent was non-mission critical and 40 percent would also trust the cloud for mission-critical IT services. Organizations are also actively employing outsourcing, with 93 percent fully or partially outsourcing some of their IT activities.

Other findings include:

- 60 percent of respondents use or are planning to use cloud computing for non-mission-critical IT services, and more than 40 percent use or are planning to use it for mission-critical IT services. For companies that do not have plans to use cloud computing the main reasons are data privacy and security concerns.
- The use of Facebook or Twitter at work is not highly prized; only one out of five respondents believes that the benefits of employees using social networking outweigh the risks.

ISACA are presenting a seminar on the “Journey of a Social Media Attack” at Infosecurity Europe