T H E E L E C T R O N

NEWSLETTER OF THE INSTITUTION OF ELECTRONICS

Issue 26: Summer 2015

INFORMATION SECURITY

Information security has become a hot topic in today's electronic age with cyber crime now being estimated to be costing UK business around £50 billion every year. At a recent briefing on policing in the digital age Adrian Leppard QPM, Commissioner of The City of London Police identified the present time as being a 'watershed moment' with a need to change the present law enforcement model to meet the digital challenge.

In *City Security Magazine* (Issue 56: Summer 2015) Mike Gillespie of Advent IM poses the question 'how do you investigate and prosecute a crime, currently active for over two years, that has so far involved over thirty countries and more than a hundred different banks, where not all of the money taken was technically stolen from accounts?'

His article 'Cyber Crime: changing and challenging Business and Law Enforcement' points to 'cyber crime on a massive scale' in which various different methods have been applied, including hijacked CCTV systems, to execute grand scale bank theft. Kaspersky Labs, who have tracked the so-called Carbanak Gang, now estimate that over $1 billion has now been extracted from these banks.

He points to the proliferation of attack tools that are now available on the internet, the methods such as phishing emails to access accounts, and the fact only 2 per cent of cyber crime is actually being reported, as being major factors behind the attraction of this type of crime being set to expand even further.

The author states:

'In the case of this heist the criminals used several tools to ensure the maximum result. They hijacked the CCTV and used it to monitor staff for months; not only gathering login credentials but examining their behaviour with bank systems in order to mimic them during the execution of the plan.

The access to the banking systems was via a phishing attack in tandem with the CCTV attack, the harvested credentials being used to siphon targeted accounts, artificially inflate others and then remove the inflated amounts without the account owner's money being touched. ATMs were also hacked in order to spit out cash at designated times, straight into the waiting arms of gang

members. In some cases this was created money; a series of zeroes added by the criminals which they then managed to turn into hard cash via the ATMs.'

He points to a 'wild west' style cyberspace and concludes that what is needed is 'a holistic and integrated approach to managing all of the systems to make sure we are not inadvertently introducing insecure "back doors" onto our networks'.

Of course cyber crime of the kind described above is just one aspect of the broader subject of information security, and in this issue of *The Electron* the subject is explored in more detail with particular reference to *Infosecurity Europe*, Europe's largest information security exhibition and conference, which was held at London's Olympia Exhibition Centre from 2nd. to 4th. June

INFOSECURITY EUROPE

In introducing Infosecurity Europe, its Portfolio Director Kerry Prince stated that information security 'is no longer just about protecting the network against attacks' but also about 'building cyber-resilience to minimise business impact in the event of a breach'.

He says:

'Information security professionals face a multitude of conflicting, complex risks and priorities as enterprises become increasingly connected and collaborative, with extended network perimeters, and the adoption of new business practices. Against this backdrop, security practitioners are working to develop intelligent security strategies that are aligned with the individual organisation's risk profile and business priorities.

Knowing their business and understanding the context of the cyber security risks they face is fundamental to aligning security strategy with the business. Yet communicating risk to senior management, speaking the language of the business and developing an enterprise-wide security culture continue to be a challenge, and ineffective communication consistently stands in the way of intelligent security.

Recent incidents suggest that it is taking too long for organisations to detect breaches, as demonstrated by the JP Morgan breach of August 2014. But how do organisations even know that they have been breached? Most organisations don't have the resources to continually monitor and detect incidents, and if an organisation doesn't know that it has been breached, it cannot respond appropriately.

With potentially catastrophic repercussions for a business, the ability to respond to and recover from an attack rapidly and efficiently is critical to building cyber-resilience and an intelligent security strategy.'

Key features of the event included:

* The UK Cyber Innovation Zone in association with The Department for Business, Innovation and Skills and TechUK, showcasing eleven small innovative UK cyber security businesses.

* The Cyber Innovation Showcase featuring 22 presentations including 11 from the 11 shortlisted companies from the UK nationwide competition launched through the Cyber Growth Partnership, with the support of BIS and TechUK to find the UK's most innovative small cyber security company of the year.

* The Risk and Network Threat (RANT) Forum consisting of a unique community of information security professionals who work with end-user organisations addressing and commenting on user concerns.

* DevOps Connect, a full day of learning, networking and thought leadership focused on DevOps and security's role in the software development lifecycle, with 11 presentations and a case study

* Four in-depth security training courses on Cyber Security Fundamentals, DevOps Foundation Certification, Certificate of Cloud Security Knowledge and How to turn the Human Firewall on.

* 20 Keynote Presentations on subjects such as 'Building Cybersecurity for Tomorrow', 'The 2015 Cyber Security Breaches Survey: Official Launch, Key Findings and Analysis', 'Building Data Protection in the Cloud', 'Keeping pace with the Evolving Business: Building a Next Generation Cyber Security Roadmap', and 'Cracking the Cipher Challenge' (a recount on how ten encrypted messages were eventually cracked by a winning team to claim a prize of £10,000).

* Infosecurity Intelligence Defence European Technical Research Conference consisting of 11 presentations on topics including 'Frontline Analysis of POS Attack Toolkits', 'Detecting and responding to Advanced Threats: Exposing the Skeleton in your Closet', 'Advancing Security Evaluation of Network Protocols', 'Detecting malicious Typosquatting Domains' and ' Data Sanitisation: Effective Protection or latest Buzzword?'

* 31 Tech Talks including 'Opening Misfortune Cookie: The Hole in 12 million Internet Gateways worldwide', ' Tracking Malware in Criminal Internet Neighbourhoods', 'Android Live Hacking Demo: How common Coding Flaws, overly permissive Permissions and DIY Certificates can compromise Android Security', 'Building Security into your Data Centre DNA', ' DDoS Attacks: What you can't see can't hurt you', and 'a case study on 'Overcoming Challenges in deploying NAC Solutions in highly-distributed Networks with 100,000+ end-points.'

* 31 Strategy Talks including 'Overcoming Insider Threats to Intellectual Property', ' Where Flow Charts don't go: An Examination of Web Applications Process Management', 'Why Women in Security are being paid more', 'Simplifying the Adoption of Cloud Applications: Identifying, classifying and protecting your Organisation's Sensitive Information' , and 'Using Threat Intelligence to improve Security Response'.

* The Information Security Exchange with 14 presentations that included 'Securing Digital Applications', 'WLAN Security: Preparing Networks for BYOD and IoT' , 'What Security Pros can learn from Shadow IT: Lessons from the Infrastructure and Operations Playbook' , 'Can Technology save us from evolving Cyber Security Threats?' , and 'Securing the Mobile User: Have we really got it right?'

* Nine Security Workshops covering ' Developing Organisational Cyber Resilience' , ' Transforming Security through Micro-segmentation' , 'Developing Skills Capability to deal with ever-changing Cyber Threats' , and two workshops on CISSP Domain Refresh (effective from 15th. April 2015) covering security assessment, testing and risk management.

* A Technology Showcase featuring innovative technologies to address the latest information security risks and including 18 presentations such as ' How to think about Security: Cyber Attack or Inside Job?' , ' How to hack an App' ,' Transforming Security through NSX Micro-segmentation' , 'Securing Content in the Cloud' , 'Meeting CPA Standards for Endpoint Security' , and 'The World's first Privileged Activity Monitoring Solution'.

* The VIP Global Executive Lounge developed exclusively for Infosecurity VIP delegates as part of the Infosecurity Global Executive Leadership Programme with peer-to-peer round tables with eight discussion subjects, namely, ' Clever Tactics and meaningful Metrics for Effective Board Level Reporting' , 'Key Steps to Robust Incident Management and Response' , ' Mitigating Third Party Risk' , 'Securing the Mobile Enterprise' , ' Identifying the Critical Steps to EU General Data Protection Regulation Compliance' , 'Translating Threat Intelligence into Action' , 'Mapping the Cyber Horizon to support Security Strategy and Investment' , and 'Smart Strategies to manage the Social Engineering Threat'.

In addition to the above the supporting exhibition featured over 300 exhibitors making it a truly international event.

A selection of topical subjects and news items highlighted at the show are presented below.

ONSITE HARD DRIVE SHREDDING CCTV INNOVATION

DiskShred, a pan-European provider of onsite media shredding solutions, launched a unique hard drive shredding CCTV innovation at Infosecurity Europe.

DiskShred takes redundant, data bearing media and shreds it into fragments so that it is irreversibly and permanently deleted. The media debris is then disposed of safely and responsibly according to government regulations.

By utilising a fleet of state-of-the-art shredding trucks the media is safely shredded onsite at a customer's premises, reducing the risk of a security breach. A Certificate of Destruction is then provided to show that the customer has fulfilled regulatory obligations.

The DiskShred trucks, fitted with CCTV enable customers to view footage of the media undergoing the shredding process. This footage is sent to the customer for records and future audits. It can also be used for asset tracking of the media and can be filtered by the customer. This works by scanning the serial number of each item before shredding such that the customer can filter the footage to view a specific item being shredded.

DiskShred create an encrypted asset register for highly confidential hard drives and storage media. This includes the type of media (such as hard disks, media tapes or CDs), the Asset Tag (serial number or other identifier), the number of units and the date and time when they were shredded.

Details are available from DiskShred, Unit 1, Mallusk View, Newtownabbey, County Antrim, BT36 4FR, Northern Ireland. Telephone: 02890 844 400.

PROTECTING AGAINST MALICIOUS USBs: A NEW SOLUTION

A new solution for protecting against malicious USBs has been launched by the French cyber security and threat intelligence specialists Bertin IT.

The solution, known as WhiteN, offers decontamination and file format verification functionalities and enables whitelist filtering and device class authentication, ensuring the refusal of any device that has not been explicitly authorised. It is also equipped with partitioning properties which make it possible to confine the environment to which a peripheral device has access. Even if an attacker succeeds in stealing the identity of authorised equipment, the scope of harm that can be caused is restricted to the affected machine.

Executive Director of Bertin IT, Beatrice Bacconnet, states:

"Even when they are isolated from the internet, sensitive information systems and critical infrastructures remain vulnerable to the risk of injection of malevolent content via uncontrolled removable media, such as USB flash drives, mobile telephones and other portable storage devices. In order to address this core issue of all Essential Service Operator's security policies, we have developed WhiteN, a solution that makes it possible to check not only the harmlessness of content imported into a system but also the conformity of such removable media with the security rules in force within the organisation."

Further details are available from Bertin IT, Parc d'activities du Pas-du-Lac, 10 bis avenue Ampere, Montigny-le-Brettonneux, France. Telephone: +33 1 3930 6058. Email: stephanie.blanchet@bertin.fr

BAE SYSTEMS APPLIED INTELLIGENCE FIRST TO GAIN CBEST APPROVAL FOR DELIVERY OF BOTH THREAT INTELLIGENCE AND PENETRATING TESTING SERVICES

BAE Systems Applied Intelligence has become the first company in the world to secure approval to deliver both Threat intelligence and Penetration Testing services under the CBEST Scheme, which has been created by the Bank of England, HM Treasury, and The Financial Conduct Authority to deliver penetration testing that replicates the field craft of sophisticated cyber criminals that the threat intelligence has identified as presenting the greatest risk.

This intelligence-led penetration test framework is vital as such criminals are assessed by Government and commercial intelligence providers as posing a genuine threat to systemically important financial institutions. This is the next step in operational cyber defence and is the first such framework developed by industry body CREST to be led by a central bank.

The concept of an intelligence-led penetration test is one of the cornerstones of the CBEST Scheme and the BAE Systems Applied Intelligence service will draw on the library of information it has gathered on the specific tools and techniques known to be employed by attackers with the means, motive and opportunity to target financial services.

This intelligence can then be used to specify realistic attack scenarios, simulated by penetration testing, to provide a meaningful insight into the vulnerability of an organisation's network to cyber attack. These scenarios also provide a useful operational context which can be used to determine the consequences to the business should such an attack succeed.

Scott McVicar, Managing Director, EMEA Commercial Solutions for BAE Systems Applied Intelligence, states:

"Intelligence-led penetration testing has to be based upon rich contextualised intelligence which informs and guides how the test should be conducted, what attack methods should be simulated and where testers should focus their resources. This method of testing provides a more structured and effective approach for companies to mitigate their cyber risk and understand the real effectiveness of the key technical security controls they have in place."

The CBEST Framework works alongside the STAR (Simulated Targeted Attack and Response) scheme developed by CREST and for which BAE Systems is also an approved supplier. While CBEST is available to nominated financial organisations, and will be performed with Bank of England and Government involvement, the CREST STAR scheme is available to all organisations that want to benefit from intelligence-led penetration testing.

BAE Systems Applied Intelligence is the cyber security division of BAE Systems. Their intelligent protection solutions combine large-scale data exploitation, 'intelligence grade' security and complex services and solutions integration.

Contact:

BAE Systems Applied Intelligence, Waterside House, 170 Priestley Road, Surrey Research Park, Guildford, Surrey, GU2 7RQ. Telephone: 01483 816000. Email: learn@baesystems.com

BAE SYSTEMS APPLIED INTELLIGENCE LAUNCHES CLOUD-BASED CYBER SECURITY IN EUROPE

BAE Systems Applied Intelligence has brought cloud-based cyber security to commercial organisations in Europe for the first time.

Most cyber attacks start with an email message and the first set of cloud-based products to be introduced by BAE Systems will comprise BAE Systems' Email Protection Services (EPS) which provides comprehensive protection against:

* Zero Day Prevention

* Insider Threat Prevention

* Email Data Loss Prevention

* Email Encryption

* Email Anti-virus and Anti-spam

* Email Archiving

* Email Business Continuity

As these services are offered entirely from the cloud integration time and complexity are reduced and there is no need for on-premises hardware or software. Customers will gain access to the technology they need more quickly and easily and in a way that suits them.

With 70 to 90 per cent of malware being unique to any single organisation the most difficult attacks to defend against are Zero Day Attacks, that is, attacks that are unknown or have not previously been seen and that, as a consequence, require a much more advanced defence. A core element of BAE Systems' EPS solution is therefore Zero Day Prevention, which provides customers with the industry's most advanced protection against today's sophisticated threats. Most importantly, the technology is based on innovative and pioneering techniques that analyse the email in the cloud for malicious content or intent, before it reaches the recipient.

Another major risk is that of employees purposefully or inadvertently leaking data. The Insider Threat Prevention Service therefore makes it easier to find and investigate insider issues.

Dr. Scott McVicar states:

"Today we are introducing European companies to protection against the most sophisticated attacks in a way that is easy to buy, consume and manage, whilst being delivered within short timescales, on cloud-based infrastructure and with the inherent flexibility to scale up or down as required."

Contact details as above.

GENERATIONAL AND GENDER FACTORS CREATE ANOTHER THREAT ATTACK VECTOR

Blue Coat Systems Inc., a market leader in enterprise security, has published initial results of a study into the online behaviour of 1,186 UK employees across telephone, email and social media. The results show how ill-prepared most UK organisations could be for the increasingly sophisticated

cyber threats posed by 'social engineering', where personal information is gathered, often via social media, and used to deliver Advanced Threats to corporate networks.

The online survey showed that the behaviour of UK employees leaves them highly vulnerable to hacking. Overall, 54 per cent of respondents said that they would not connect with strangers on social media and 56 per cent have not set up access controls to their social media.

In recent cyber attacks basic information has been used to reset social media passwords, which then provides criminals with access to confidential, sensitive information that can damage brand reputations and compromise valuable business assets.

Another interesting finding was that UK female employees who use social media would appear to be more aware of the cyber threats. Of these 52 per cent set up privacy settings so that only certain people could view their full profiles, compared with only 36 per cent of UK male employees. But whilst female employees may be more diligent about privacy on social media sites, the survey did suggest that they could still be vulnerable with 12 per cent using pet names to generate online passwords as against just 5 per cent of male employees.

Findings also revealed that 62 per cent of 18 to 24 year olds take effective precautions to filter those who access their social media data on mobile apps by checking the identities of strangers before connecting with them. 18 to 24 year-olds also tend to share more work information on social media. By contrast, only 33 per cent of 45 to 54 year-olds (who typically hold more senior corporate roles and are therefore more likely to be targeted by cyber attacks) check requests before accepting invitations to connect.

Only 18 per cent of UK employees stated that they had never had IT security training. Of the people who had been trained, however, only 10 per cent said that they received regular training. Only 6 per cent of UK employees said that they had had training and guidance on phishing attacks.

Hugh Thompson, Chief Technical Officer and SVP for Blue Coat, concludes:

"This research shows how employees can be a gateway in to corporate systems. As they reveal more about themselves on social media, they become more 'knowable', which exposes them to higher risk of social engineering. As the seriousness and complexity of threats grows, businesses need to employ security measures, including training, that take into account the habits and behaviours of employees to better protect the enterprise. Security measures need to be seamless and tailored to enforce cyber-safe behaviour recognising that even the paranoid can be phished."

More information is available from bluecoat@positivemarketing.com or on 020 3637 0640.

CYBER DEFENCE CAPABILITY ASSESSMENT

The Cyber Defence Capability Tool CD CAT, developed by the Defence Science and Technology Laboratory (the trading fund of the MoD), is a means by which businesses can quickly assess their cyber defence preparedness, understand where any gaps in defence capability may exist, and what mitigations may be applied. This could make the complex world of cyber security more accessible and easier to understand for many organisations.

At Infosecurity Europe CD CAT was publicly exhibited for the first time by global accreditation body APMG International, whose CEO Richard Pharro commented:

"With cyber crime damages projected to reach £1.3 trillion by 2019, the cyber security industry has great challenges on its hands, products such as CD CAT will play a greater role than ever before on the front lines of cyber risk assessment and mitigation.

By enabling users to significantly reduce the time it takes to identify vulnerabilities and manage risk, CD CAT will expedite the process of raising cyber risk awareness within firms. For some firms this will mean reducing the time it takes to create risk mitigation strategies from months to mere hours.

We are moving to a higher stakes game as cyber threats continue to grow in sophistication, but, equally, we are becoming more empowered to make the right decisions and assess the risks as awareness of the issues increases."

CD CAT fuses multiple cyber security controls and inputs from commercial, military and intelligence operations around the world including NATO, ISO 27000 and the NIST Cyber Security Framework, together with leading independent bodies such as The Council on Cyber Security. CD CAT combines them to produce a list of standards associated with one of 145 different aspects of cyber defence.

These are mapped to the cyber defence lifecycle categories of Assess, Deter, Protect, Detect and Respond/Recover. Each control, such as Patch Management, has a definition that describes different levels of compliance based on the organisation's risk.

CD CAT captures risk control objectives in one single operational activity consistent framework supporting the fusion of:

(i) Protect (covering Information Assurance)

(ii) Defend (covering classic 'computer network defence)

(iii) Operate (covering end-to-end service management)

CD CAT will provide an assessment report developed into an action plan based on the organisation's chosen practice framework (MoD, NATO, ISO 27001, CES, CSC 20 or NIST). Business decisions can then be made by comparing the organisation's risks with the costs of an improvement plan.

More information is available from APMG, Sword House, Totteridge Road, High Wycombe, Buckinghamshire HP13 6DZ. Telephone: 01494 452 450. Email: servicedesk@apmg-international.com

GHOST VULNERABILITY ON LINUX SYSTEMS

Qualsys Inc., a pioneer and leading provider of cloud security and compliance solutions, has announced that its security research team has discovered a critical vulnerability in the Linux GNU C Library (glibc) that allows attackers to remotely take control of an entire system without having any prior knowledge of system credentials.

The vulnerability known as GHOST (CVE-2015-0235), as it can be triggered by the gethostbyname functions, impacts many systems built on Linux starting with glibc-2.2 released on November 10th. 2000. Qualsys researchers also identified a number of factors that mitigate the impact of this bug including a fix on May 21st. 2013 between the releases of glibc-2.17 and glibc-2.18. Unfortunately, however, this fix was not classified as a security advisory and, as a result, most stable and long-term support distributions were left exposed including Debian 7 (wheezy), Red Hat Enterprise Linux 6 and 7, CentOS 6 and 7, and Ubuntu 12.04.

Qualsys have advised that their customers can detect GHOST by scanning with the Qualsys Vulnerability Management (VM) cloud solution as QID 123191. This means that Qualsys customers can get reports detailing their enterprise-wide exposure during their next scanning cycle, which allows them to get visibility into the impact within their organisation and efficiently track the remediation progress of this serious vulnerability.

Wolfgang Kandek, Chief Technical Officer for Qualsys Inc. states:

"GHOST poses a remote code execution risk that makes it incredibly easier for an attacker to exploit a machine. For example, an attacker could send a simple email on a Linux-based system and automatically get complete access to that machine. Given the sheer number of systems based on glibc, we believe this is a high severity vulnerability and should be addressed immediately. The best course of action to mitigate the risk is to apply a patch from your Linux vendor."

Qualsys Inc. (NASDAQ:QLYS) is a pioneer and leading provider of cloud security and cloud security and compliance solutions with over 6,700 customers in over 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualsys Cloud Platform and integrated suite of solutions help organisations to simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications. Founded in 1999, Qualsys has established strategic partnerships with leading managed service providers and consulting organisations including Accenture, Accuvant, BT, Cognizant Technology Solutions, Dell SecureWorks, Fujitsu, HCL Comnet, InfoSys, NTT, Tata Communications, Verizon and Wipro. Qualsys Inc. is also a founder member of The Cloud Security Alliance and Council on Cyber Security.

More information on GHOST, including a podcast, can be found on the Qualsys Laws of Vulnerability blog.

Contact: Qualsys Inc., 100 Brook Drive, Green Park, Reading, Berkshire, RG2 6UJ. Telephone: 01189 131 516. Email: info-uk@qualsys.com

NEW CLOUD-BASED LOSS PREVENTION SERVICE

Atos, an international leader in digital, have launched an innovative new cloud-based Data Loss Prevention Service that prevents data loss, whether it be from unauthorised insider activity or external threats such as advanced malware.

Organisations are increasingly threatened by both insider threats and by advanced malware. A single incident can have catastrophic consequences including loss of revenue, negative publicity, and reduced brand equity. In today's massively interconnected world it is increasingly difficult to protect confidential information and this new service helps to solve this problem by combining the advantages of both data loss prevention and advanced malware detection using Digital Guardian's unique single agent technology.

As a cloud-based service it is deliverable anywhere in the world enabling rapid deployment, scalability and a short payback period. It is fully managed incorporating Atos' Security Operation Centre and expertise in DLP to provide a robust risk management service. It vastly simplifies deployment and ease of integration into already existing environments. It can also be deployed on-premise or as part of a risk management systems integration programme. Benefits include:

* Cloud delivery for accelerated deployment and rapid investment recovery

* Protection of critical business information

* Regular reporting for improved management of critical information protection

* Escalation of critical events

* Combination with advanced malware detection technologies to combat sophisticated attacks

Chris Monet, Vice President of Cyber Security at Atos commented:

"What is particularly exciting is how this service is delivered via the cloud and combines Digital Guardian data loss prevention technology and Atos SOC capabilities to provide an end-to-end service that's available to monitor, detect and mitigate data leakage 365 days a year, 24 hours a day."

Doug Bailey, Chief Strategy Officer for Digital Guardian, added:

"Sensitive data is the lifeblood of organisations today - whether intellectual property, trade secrets or confidential client information. Many companies do not have the resources and expertise to implement a data protection solution in the required timeframe. Atos' world class delivery capabilities combined with Digital Guardian, the market's most comprehensive data protection solution, offers customers the fastest time to protection of their critical assets."

More information is available from Atos, Rue Jean Jaures, Les Clayes-sous-Bois, Ile-de-France, France 78340. Telephone: +33 6 66 68 00 10. Email: anais.crouzat@bull.net

CHECK POINT CAPSULE: COMPLETE MOBILE SECURITY

The massive surge in mobile device usage within businesses continues to challenge IT and security teams as they face the increased complexity of mobile security management and are at greater risk for data loss incidents.

In Check Point Software Technology Limited's 2014 Mobile Security Survey, which surveyed over 700 IT professionals, over half of the respondents said that they managed business data on employee-owned devices. 82 per cent of the security professional surveyed expected mobile security incidents to rise in 2015, 72 per cent said that the number of personal devices connecting to their networks had more than doubled in the last two years, and 42 per cent noted that mobile security incidents had cost their organisations more than $250,000.

Check Point Capsule addresses these challenges by offering a complete mobile solution that ensures seamless security regardless of where the data or device goes. It is a single solution that offers multi-layer security including:

(i) Secure access to work - protects business data on mobile devices without having to manage the entire device. Capsule creates a secure business environment and separates business data from personal data and applications on mobile devices enabling users to securely use business applications through a simple user interface, where users have one-touch access to corporate email, files, directories, corporate contacts and calendars without affecting their personal data.

(ii) Safe business documents - prevents internal and external data leakages by attaching security that travels with the document. Capsule secures business documents everywhere and authorised users can access a protected document seamlessly and transparently on any device.

(iii) Universal protection from threats - extends the corporate security policy to protect devices from threats when outside the corporate network. Capsule scans all traffic from mobile devices in the cloud and prevents access to malicious files and web sites, bot damage and other cyber threats. This cutting-edge security supports various device platforms and operating systems including iOS, Android, Windows and MacOS.

Dorit Dor, Vice President of Products for Check Point Software Technologies, states:

"Protecting information, regardless of device or location, is a clear necessity for all organisations so we are offering a multi-layer solution that is both seamless and secure. With Check Point Capsule an organisation gets unmatched security that goes on any device and any document everywhere. The use of mobile devices on corporate networks will only continue to rise, and Capsule extends Check Point's industry-leading enterprise security for increasingly mobile workforces."

Further details may be obtained from Check Point Software Technologies Limited, 6th. Floor, 4 Ckiswell Street, Westminster, London EC1Y 4UP. Telephone: 020 7628 4211. Email: ukinfo@checkpoint.com

ENSURING DOCUMENT SECURITY

Attacks are evolving and increasing continuously, and documents are a high risk for many organisations. Check Point found that 84 per cent of companies downloaded an infected document in 2013, and concluded that the only way to ensure complete protection was to preemptively remove threats by reconstructing documents with known safe elements.

In order to do this Check Point have introduced Threat Extraction, a radical new security approach that proactively ensures that documents are delivered to a network with zero malware in zero seconds.

Active content, embedded objects and other exploitable content are simultaneously extracted and the document is then reconstructed without potential threats to provide 100 per cent safe content. This enables organisations to protect themselves against both known and unknown threats.

Dorit Dor states:

"Because the traditional approach of protecting against infected documents by looking for malware and blocking it does not provide absolute protection, organisations need a way to preemptively remove the threat of malware altogether. With Check Point Threat Extraction organisations can now defend their networks against threats with a radical new technology that delivers 100 per cent safe documents immediately."

In addition to receiving zero malware documents organisations need to know if they are under attack. For this Check Point have developed Threat Emulation Anti-Bot, Intrusion Prevention and Antivirus all to complement Threat Extraction by detecting malware and providing full visibility of event information about any attack attempts.

Check Point 2015 Security Report

In addition to the above, Check Point have released their 2015 Security Report based on analysis of real security events, attacks and breaches from over 16,000 gateways and over 1,000 endpoints worldwide during 2014. This highlights the risks that organisations are exposed to and the growth of threats on enterprise networks.

The report shows that on an average day in an average enterprise business:

* every 34 seconds unknown malware is downloaded onto networks (48 more times than in the previous year)

* every 60 seconds a bot infection on a network communicates with its command centre (three times more than in the previous year)

* every 6 minutes known malware is downloaded onto company networks (almost double the previous year)

*every 30 minutes a DDoS attack is launched against an organisation (six times the previous year)

*every 36 minutes sensitive data is sent outside the organisation (37 per cent higher than the previous year)

Contact details as above.

EVASIVE MALWARE GOES MAINSTREAM

Research by US based Lastline Laboratories has found that evasive malware that was once largely restricted to advanced, targeted attacks by powerful threat actors has now become much more common.

What has been found is that, increasingly, malware that is used by Advanced Persistent Threat (APT) groups is leveraging sophisticated evasive manoevres so as to conceal its true malicious nature from traditional sandboxes until it reaches a specific target machine. The research showed that the percentage of malware samples that were evasive more than doubled from January 2014 to December 2014.

Lastline state:

' *Evasive malware is shifting from a seldom-used, sophisticated weapon in the hands of a few to a highly proliferated, popular tool used by many attackers in many ways. The barriers to entry for building and disseminating evasive malware are apparently now more easily surmounted.*'

Another observation has been that individual malware samples are incorporating more evasive behaviours, often using a combination of over 500 different behaviours. This means that where a year ago only a small fraction of malware showed any signs of sandbox evasion, now a sizeable proportion is evasive. Also, where a year ago evasive malware tended to leverage at most two or three evasive tricks, now much of it is tailored to bypass detection using as many as ten or more different techniques.

The four most common types of evasive behaviours observed by Lastline Labs over the past year are:

(i) Environmental awareness

(ii) Confusing automated tools

(iii) Timing-based evasion

(iv) Obfuscating internal data

At the same time signature-based antivirus AV scanners are falling further behind. From April 2014 to March 2015 not one scanner observed had a perfect day detecting every new sample. In addition,

the most difficult to detect malware has become even more elusive. After a full year 64 per cent of the AV engines failed to detect the 1 per cent of least detected malware, compared to last year when it was only 10 per cent.

Christopher Kruegel, Chief Scientist for Lastline Labs concludes:

"The configuration of the various antivirus scanners used by VirusTotal is not necessarily optimal and it is always possible that a better detection rate could be achieved by relying on external signals or using more 'aggressive' configurations.

Ultimately the more evasive behaviours malware employs the more likely it will succeed in bypassing both signature-based and behaviour-based detections. While much of the average malware can still be detected using signature-based tools and standard sandboxing (those built on OS emulation or virtualisation with limited visibility into malware execution), evasive malware is bypassing both. Malware authors are always cramming more tricks into their code, and the only way for security professionals to weed them out is to continually adapt. If we build tools tailor-made to detect evasive malware, integrate across security systems and share threat intelligence it is possible to get ahead of advanced threats."

In response to these challenges Lastline are innovating the way companies detect active breaches caused by targeted attacks and evasive malware with their software-based Breach Detection Platform. Inspection of suspicious objects occurs at scale in real-time using a full system emulation approach to sandboxing that is superior to virtual machine-based and OS simulation techniques.

More details may be obtained from Lastline Inc., Eagle House, 167 City Road Office 1.11, London EC1V 1AW. Telephone: 020 7749 5156. Email: lsimonelli@lastline.com

NEW MONITORING TOOLS TO DETECT HIDDEN MALWARE

A major problem with cyber attacks is the fact that a breach can remain undetected within a network for weeks, months or even years. This time provides hackers with the ability to move laterally within the network so as to acquire better credentials, compromise more systems and search for the most profitable and the most damaging information.

A further deficiency is the fact that perimeter defence tools are virtually worthless once hackers are at work within the system.

John Breeden II of *Network World*, however, in his article 'New Weapons offer hope against Advanced Cyber Attacks' (Network World, February 23, 2015), observes that despite these hazards the malware itself somehow has to communicate back to the hackers, and consequently new monitoring tools have been developed in order to detect this traffic.

Damballa Failsafe

This tool monitors 35 per cent of all Internet traffic worldwide every day and 55 per cent of all US-based DNS traffic. It is therefore 'a pretty safe bet' that any freshly created malware is going to flow through a gateway monitored by Damballa at some point early in its lifecycle.

Damballa uses this extensive reach, a team of data scientists and machine learning capabilities to profile malware. It is not, however, signature-based. It samples over 100,000 new variants of malware every day, but is only concerned with the characteristics of the malware as it pertains to network traffic.

The company then generates each component of HTTP requests from the samples, looking at the requests by data type, encoding and length. In this way the characteristics of malware are identified because even though the control server, destination and camouflaging techniques used by malware are changing all the time, the communication structure is always going to be the same. That information is then shared with Failsafe appliances that are protecting networks.

Failsafe is installed as a single appliance with one sensor device deployed at each Internet access point so that every communication to or from a network can be monitored. Damballa engineers then monitor the network to ensure that devices are placed at the correct locations and that no rogue communication streams exist.

In order to reduce false positives Failsafe does not immediately elevate suspicious activity into an alert, although administrators can look at everything that the program currently considers to be suspicious. Two engines run on the main appliance to prevent security alert overloads, one for breach detection and one for risk analysis. Both require suspicious activity to cross a certain threshold before an alert is generated.

The breach detection engine covers three areas: behavioural analysis, content and payload analysis, and threat intelligence. Behavioural analysis looks, for example, at how automated a process is, if it is using the new domain fluxing technique employed by advanced malware, per-to-peer communications and what is being executed. Content and payload analysis is mostly concerned with the type of requests being generated. Threat intelligence uses all of the Internet traffic data collected by Damballa to compare the queries and connection makeups against malware variants.

The risk profiler uses machine learning and human intelligence to determine if suspicious behaviour is actually malicious. It uses variables such as how much data is being transferred, if the communications were successful, if it was part of a spanning process, the importance of the protected endpoint within the organisation, the threat actor being communicated with, and possible alerts from antivirus coverage. The risk profiler does not just elevate threats once they are confirmed, it also ranks them in terms of severity. Persistent malware, for example, can remain hidden from traditional monitoring tools with domain fluxing, introducing jitter into their communication windows, or only releasing a couple of kilobytes of data at a time.

Damballa Failsafe also works with other security programs such as TippingPoint and Splunk, integrating their capabilities and allowing full control over them from a user-friendly interface. This

means that Failsafe can be dropped into any existing security architecture and become complementary rather than competitive.

LightCyber Magna

The LightCyber Magna platform is designed to separate normal user behaviour from the anomalous kind used by attackers. It does not merely deal with outgoing and incoming traffic, it detects, evaluates and, if possible, mitigates the attacker's activity once inside the network.

The platform is installed in components and not every organisation would need every one.

The Magna Master collects data from all other parts of the system and is what users would log into in order to configure their protection and receive alerts.

The Magna Detector monitors traffic and connects to a span port in a switch or tap.

A Probe appliance may be used to connect the traffic monitoring at branch offices back to the main master console. Most deployments are hardware-based, but virtual installations of all components are also available.

Pathfinder performs agent-free endpoint analysis to complement network information in the automated decision-making process and to find the root cause of suspicious behaviour within endpoints.

Once installed Magna typically waits for two to three weeks before taking any actions. During that time the software monitors all network traffic to establish baselines for each group, user or device. These baselines are used as part of a very detailed plan to prevent false positives.

The interface for the Magna platform is very simple at first, then drills down into increasing complexity as needed. The main dashboard then shows how many known breached hosts and devices exist on a network, how many suspicious hosts Magna is monitoring, if any systems have been quarantined, and how many incidents have been fixed and closed.

Magna does not elevate incidents to alert status unless they have been verified by several sources.

The tool is noted to be particularly suited to organisations concerned with advanced persistent threats or attacks that are initiated from inside a network. It is especially good at detecting lateral movement or activity within an enterprise that would not ordinarily trigger traffic monitoring tools that were only concerned with packets that cross a network threshold.

Lancope StealthWatch

This tool exclusively monitors flow data. all flow formats are supported including Netflow, IPFIX, sFlow, jFlow and others.

A Flow Collector records all transactions whilst a Management Console opens up an SSL connection and allows for user interaction. Flow is a Layer 3 process, therefore every router and communication device will make use of it. There is, however, another smaller appliance that can be used for the few hardware configurations, mostly in the high-performance computing environment, that do not support flow.

Flow is an interesting way to record traffic because a flow represents a single end-to-end transmission over a network. As such, a single transmission can generate many flows as it moves in and through devices within the network. The StealthWatch Collector, which can handle up to 240,000 flows a second, also removes duplicate information so that administrators only see one record per communication. One Management Console can handle up to 25 Flow Collectors enabling a very large amount of flow data to be processed.

This flow data shows a complete picture of what communications are taking place within a network, but it takes time to sort everything into meaningful information. Devices need to be identified to StealthWatch by a variety of criteria. While the group definitions are optional, the more there are the better is the chance that a network administrator will be able to identify anomalies in the system that could point to a hacker.

Populating a group in StealthWatch can be done using a third party network IP management system, importing a .csv file or right clicking and specifying an IP range.

Lancope StealthWatch is noted for its ability to provide a highly detailed view of network connectivity, as well as its distinct advantage of being able to define relationships between devices and groups and specifically monitor that traffic. Thus, if an organisation has regulatory requirements whereby certain devices are not allowed to communicate with each other, defining that restriction to StealthWatch will set up a communications map and alert administrators if any traffic occurs between restricted devices or groups.

Further Information

The author John Breeden may be contacted at jbreeden@techwritersbureau.com

Damballa and Lancope were both exhibitors at Infosecurity Europe and their details are:

Damballa Inc., 817 W. Peachtree Street NW, Suite 800, Atlanta, Georgia, USA 30308. Telephone: +1 404 961 7404. Email: jillian.ungerdamballa.com

Lancope Inc., 88 Wood Street, London EC2V 7RS. Telephone: 020 8528 1757. Email: International@lancope.com

FIRST INTELLECTUAL PROPERTY THREAT DETECTION INTEGRATED WITH SOURCE CODE AND CONTENT MANAGEMENT

The first intellectual property threat detection tool integrated with source code and content management has been launched jointly by Perforce Software and Interset.

Helix Threat Detection uses behavioural analytics to safeguard source code and other intellectual property against insider threats, account takeovers and malicious attacks. It is a security solution for the Perforce Helix source code management and content collaboration platform that quickly and accurately identifies internal and external security risks related to intellectual property managed in Perforce Helix.

Sophisticated behavioural analytics patented by Interset monitor interactions with source code, product designs and related assets managed in Perforce Helix. Interactions receive a risk score, generating alerts that indicate high-risk activities, users, machines, projects and data.

Early customers have demonstrated the potential return on investment of the product by detecting:

* attempts to steal source code by employees in the process of leaving a company

* contractors attempting to access unauthorised projects and data

* external agents using compromised accounts to access internal files

Helix Threat Detection eliminates reliance on rules-based thresholds and simplifies configuration and deployment. A plain-language user interface enables IT, engineering and security teams to quickly understand their greatest IP risks and why, all with minimal training.

Christopher Seiwald, CEO and Founder of Perforce, states:

"Source code, product design and similar intellectual property are a company's most valuable assets. Government research estimates that more than $300 billion is lost annually to theft of these assets in the US alone, a loss that can be dramatically reduced by the protection provided by Helix Threat Detection."

Dale Quayle, CEO and President of Interset, added:

"A long time gap in the security market has been the lack of understanding of threats across critical IP repositories. Most companies, even those with mature SIEM deployments, have little or no visibility into what risks exist in these critical data stores. Through our work with Perforce we have delivered an important new approach to threat detection that uses data science to analyse the millions of events captured in Perforce logs and surface the high-risk events that define insider theft and targeted attacks."

More information may be obtained from Perforce Software, West Forest Gate, Wellington Road, Wokingham, Berkshire RG40 2AT. Telephone: 0843 450 116. Email: sglover@perforce.com

PROTECTING DATA IN THE CLOUD

The adoption of cloud SaaS platforms has brought new challenges for enterprises in the area of protecting sensitive and confidential corporate data. In addition to an enterprise's own information security policies regulated business data is frequently subject to legal and regulatory compliance requirements that make use of the cloud difficult.

These obligations have led to a rapid growth in enterprise adoption of Cloud Data Protection Platforms, which have proven to be a critical component for enabling enterprises to fully leverage the benefits of leading cloud SaaS applications such as Salesforce. They allow enterprises to fully leverage cloud applications without losing control of their confidential and regulated data, because sensitive information remains securely stored within their own firewalls.

Organisations have discovered that understanding how data compliance and internal information security governance will be addressed while adopting cloud applications is just as important as the features and functions of the SaaS applications themselves.

The Perspecsys Approtex™ Cloud Data Protection Platform resides transparently between the enterprise's own users and the Salesforce cloud platform, intercepting data before it is passed to the Salesforce cloud, enabling data protection policies to be enforced at a field or document level before the sensitive information leaves the enterprise.

On a document or field level, sensitive data that needs to be protected is replaced with a surrogate tokenised value before it leaves the organisation's control. This replacement token value is then processed and stored in the Salesforce cloud so that enterprises can be assured that information will be meaningless if accessed by any unauthorised individual or parties. The Perspecsys Platform, however, still ensures that critical Salesforce functionality, such as Searching on data within a field that has been tokenised, is retained.

Tokenisation is a process by which sensitive data fields, such as PII, email addresses, documents, images and call notes are all replaced by a surrogate value in the form of a token. The sensitive data and corresponding token values are stored in a secure Token Vault database, which is itself encrypted, located within the enterprise's network. It is impossible to determine the original clear text value from a surrogate token unless access is granted to the Token Vault. This is a fundamentally different approach to encryption, which uses a cipher algorithm to mathematically transform clear text data's original value to an encrypted value. The core of the approach relies on a mathematical relationship linking the original clear text data to the encrypted value. This mathematical relationship, combined with the fact that encrypted data can be easily reversed if an entity has possession of the encryption keys, has led to concerns by regulators and security professionals that encrypted data in the cloud does not fully deliver in terms of residency and privacy.

The tokenisation system, by contrast, uses a sequentially generated token creation method that randomly allocates tokens to data that needs to be protected. There is no mathematical relationship. The token can only be 'redeemed' for the original value by looking in the Token Vault within the enterprise to match a token to the true value. Tokenisation is also unique in that it

completely removes the original data from the cloud SaaS systems in which the tokens reside. The Token Vault is under the complete control of the enterprise and only authorised users have access to it via the Perspecsys AppProtex Platform.

Perspecsys state:

'Use of tokenisation essentially creates a hybrid cloud data-model for enterprises using public cloud SaaS applications. Sensitive data remains completely on-premise within the enterprise. The enterprise has sole and ultimate control of its data at all times since it is never in the clear outside of its environment - surrogate tokens replace the data in transit, at rest and in use within the cloud.'

There is no trade-off between core functionality and data control for Salesforce users and a local search engine allows preservation of search functionality. Search of obfuscated data is performed in the local Search Index within Perspecsys and not in the cloud, and users experience seamless search operation regardless of data obfuscation types.

For more information contact Perspecsys, 68 Lombard Street, London EC3V 9LJ. Telephone: 020 7868 2037. Email: amy.marchiando@perspecsys.com

KEYS TO THE CLOUD

Cloud computing offers major benefits to businesses, such as reduced cost of in-house operations and improved operational flexibility, but to gain these benefits a certain amount of control has to be relinquished to the cloud. Multiple organisations use the same core infrastructure and a lot of trust has to be placed in the cloud provider, which impacts heavily on security.

The recent report 'Thales Encryption and Key Management Trends' has revealed that inadvertent exposure and 'e-discovery' has now become a greater concern than actual attacks.

John Grimm, Senior Director of Product Marketing for Thales e-Security (ref. *Business Technology Information Security Supplement*, May 2015) states:

"Currently, the problem is that if keys are unnecessarily exposed they can easily be found, stolen or substituted. Even if attackers can't actually steal the keys they can still attempt to misuse them, typically by corrupting the applications that have the rights to access them. It's therefore important to minimise the group of individuals that can manage your keys, and that means isolating them from cloud service providers and potentially from app developers, testers and contractors as much as possible."

The safest option is to keep control in-house, encrypting and decrypting data and managing the keys within the enterprise. Once the keys are used in the cloud, however, there comes the question of where they are managed, by and in the enterprise, by the enterprise but in the cloud, or by the cloud service provider.

A recent development is 'Bring Your Own Key' (BYOK) whereby organisations have complete ownership over their own keys, protecting both the customer and the cloud provider simultaneously. An example of this is the Microsoft Key Vault Service, which essentially creates a 'crypto-as-a-service' capability within Azure.

The author says:

"Keys that are managed in on-premises Thales HSMs can be securely uploaded to Azure-based HSMs to provide end-to-end assurance. Any Azure-based applications can use the Key Vault Service to access a variety of key management applications, such as key creation, backup and rotation as well as basic crypto operations like encrypt/decrypt and sign, and have the option to perform all operations within the secure boundary of the HSM."

The Key Vault creates true separation between security operations teams and application owners.

Information about the Thales BYOK deployment service for Microsoft Azure Cloud Applications may be obtained on 01223 723 600 or www.thales-esecurity.com

TRAINING TO REDUCE RANSOMWARE ATTACKS

Ransomware is now being localised for Asia with the new Crypt010ocker variant translating its menu screens according to the victim's IP address. The Canadian market has already been targeted with the Koler mobile ransomware which locks up screens with fake government warnings and demands a ransom to return functionality. Another target has been local police departments where ransoms of $300 and $600 are being demanded to prevent critical data loss.

The CEO of KnowBe4, integrated security awareness training and simulated phishing specialists, Stu Sjouwerman, states:

"Users can become complacent or can be tricked by social engineering into clicking on a malicious link in a spear-phishing email or being redirected to a bad site and clicking on something they shouldn't. It departments may believe their anti-virus has them covered, but the average window of exposure is 17.5 hours before a signature that blocks the phishing attack becomes available. And surprisingly often backups turn out not to work or it takes days to restore a system. Today an essential additional security layer is to train your users to become part of your human firewall."

Recent research sponsored by KnowBe4 shows that email phishing attacks are now the number one source of data breaches, with 67 per cent of respondents saying that malware has successfully penetrated their corporate networks through email, with web surfing a close second at 63 per cent. Another 23 per cent said that malware had infiltrated their networks but that they did not know how. The latest Verizon report shows that approximately 23 per cent of recipients click on a phishing email and most of that occurs within the first hour of receipt. Recovering from this, even if the backup works, can take hours or days.

Over a twelve month period KnowBe4 analysed 3,600 phishing tests sent to 291,000 seats. The results showed the top four click-bait emails were LinkedIn Inmail (19.9 per cent), an email from 'IT' to change a password (18.8 per cent), Amazon (13.7 per cent) and UPS (11.4 per cent). A recent Proofpoint study says 1 in 10 users typically click on a malicious URL, whilst the most recent Verizon report puts the open rate of phishing emails average at 23 per cent and the click-through rate at 11 per cent.

Sjouwerman adds:

"For compliance reasons too many companies still rely on a once-a-year breakroom 'death by PowerPoint' training approach or just rely on their filters, do no training and see no change in behaviour. Our Kevin Mitnick Security Awareness Training is an integrated platform for awareness education combined with an extensive library of templates that allow IT managers to schedule regular phishing tests to keep users on their toes with security top of mind. After our training we see a rapid decrease in clicks on phishing emails from an initial average of 16 per cent to a phone-prone percentage of just 1.28 per cent after 12 months."

KnowBe4 are the only company so far to offer a 'crypto-ransom guarantee', offering to cover any ransom in Bitcoin if a customer gets hit by ransomware after training its users.

For further information contact KnowBe4, River Court, Albert Drive, Woking, Surrey GU21 5RP. Telephone: 01783 227 600.

SECURITY THREAT TO AUTO INDUSTRY

Driverless cars may soon become a reality and several car manufacturers such as Audi, BMW, Ford, Renault and Volvo are now making vehicles which have some form of connectivity in them. There is a problem, however, because this increased connectivity is also accompanied by an increased vulnerability to cyber attacks.

Last year software security firm Kaspersky Labs, in collaboration with Spanish marketing and digital media company IAB, undertook a study that was designed to establish if such vehicles were really secure. Findings showed, for example, that embedded within BMW's Connected Drive System there were several areas that were at risk, notably the fact that third parties could potentially gain unauthorised access to user information as well as the vehicle itself by means of phishing, key logging and social engineering.

The study also found that privacy, software updates and car-oriented apps could potentially leave connected vehicles vulnerable to cyber criminals and provide hackers with access to remote services to the vehicle as well as the ability to drive it.

In the article 'Connected Thinking' in *Business Technology Information Security Supplement*, May 2015, David Emm, Principal Security Researcher for Kaspersky Labs, comments:

"Connected cars can open the doors to threats that have long existed in the PC and smartphone world. Several areas of risk have already been identified. For example, by obtaining a vehicle owner's identity credentials, thieves could remotely unlock, and take possession of, a vehicle. By intercepting and tampering with mobile communications and over-the-air software updates, cyber criminals could transmit malicious cod or, in a worst case scenario, send new and dangerous instructions to the vehicle's software systems."

Mr. Emm warns especially of the dangers of poor password protection 'leaving the door open to criminals' and the fact that vehicles can be exposed to cyber threats during production, making it essential that the systems involved in car production are also protected. He also asserts that current methods for real-time tracking, detection, analysis and resolution of cyber-threats for computers and mobile devices are insufficient by themselves, and that it could take just seconds to completely disable or destroy a connected vehicle with disastrous consequences.

He argues the case for prevention by identifying and dealing with the vulnerabilities before such electronic technology is extensively integrated into vehicles. For this he says that the auto industry needs to look to the software industry for guidance on how to deal with things such as malware and hacking, and work is ongoing, for example with the Scuderia Ferrari racing team to ensure the safety of cars and drivers.

For further information contact Kaspersky Labs, River Court, Albert Drive, Woking, Surrey GU21 5RP. Telephone: 01783 227 600. Email: Kaspersky@wickhall.co.uk

IDENTITY 3.0

The Global Identity Foundation is working with the security industry to develop a single, open source globally accepted digital ecosystem called Identity 3.0, which can be used to make secure and trusted online and offline transactions.

The objective is to be able to understand the context in which an entity (person, device, code, agent or organisation) is operating to a known level of trust. The entity (typically a person) only shares the attributes and information that is essential to the transaction that he or she wishes to undertake. This allows the parties involved in the transaction to make a risk-based decision about whether to undertake the transaction, or whether they need additional information before proceeding.

It is anticipated that Identity 3.0 will become the overarching ecosystem that will be accepted by governments and corporations internationally.

The development work builds on that done by The Jericho Forum on identity (now disbanded), and is focusing on measures that move beyond passwords and basic web security.

The Global Identity Foundation is seeking vendors, academics, and security experts to contribute to the development of Identity 3.0 as research sponsors and partners.

CYBER INSURANCE : UK LAGS BEHIND

A recent report, co-authored by the government and insurance broker Marsh, has revealed that just two per cent of UK firms have cyber-insurance even though 81 per cent of firms stated that they had had a breach over the last 12 months.

The same report, which was based on input from 13 London insurers and various large companies, found that while the London cyber-insurance market is worth £160 million, more than 10 per cent of the global market, policies for UK companies only account for around £20 million to £25 million.

In response to this the UK Government is now teaming up with the Royal Bank of Scotland and Marsh to try to develop the UK cyber-insurance market. Participating insurers are to include the Cyber Essentials certificate as part of their cyber-risk assessment for SMEs, when backed by a suitable insurance policy to improve their supply chain resilience.

Marsh will launch a new cyber-insurance product for SMEs which will absorb the cost of Cyber Essentials certification for the majority of firms and the Government is encouraging other brokers to do the same.

Lloyds will work with The Department of Trade and Investment to market the cyber capabilities of the London insurance market globally.

Cyber insurance policies currently fluctuate considerably with coverage typically six times more expensive than property cover.

[Reference: 'UK bangs the Drum for Cyber-Insurance'*, SC Magazine*, May-June 2015].