FASTtalk

The Quarterly Magazine for FAST Members | Issue 2 | 2007

GAP ANALYSIS: FAST-TRACK YOUR REGISTRATION PROGRESS

VISTA IN FOCUS: SOFTWARE ESSENTIALS

GOLD SUCCESS: EXPERIAN HITS THE MARK

FileCruncher
FILE IDENTIFICATION SERVICE

Identify what your audit tool didn't!

Software discovery tools generate extensive lists of unrecognised files. It is nearly impossible to determine whether those unrecognised files are legitimate commercially licensable software that require the appropriate licence or if they are malicious programs such as spyware, password crackers, adware, keyloggers or viruses which present a risk to your organisation and must be removed immediately.

The process of identifying these files is a time-consuming, labour-intensive task for already stretched IT staff. In many cases the task is insurmountable.

Easing the File Identification Process

To address these issues and help speed the process of achieving software compliance (including achieving registration to the FAST Standard for Software Compliance: FSSC-1:2004), FAST provides FileCruncher, an Internet-based file identification service.

Aimed at organisations that want to guarantee the detection, management and elimination of rogue software files, the service:

- offloads the tedious and time-consuming task of file identification to the experts
- identifies and categorises files into those that require a licence and those that don't
- categorises files according to the level of risk they present to your organisation
- identifies malware including viruses, trojans and keyloggers
- detects memory sapping files on your network (such as games and music).

By using the file identification service you will benefit from:

- a significant reduction in the time taken to recognise unidentified files
- a shorter timescale to achieve software compliance
- reduced risk to your organisation
- the opportunity to repeat the exercise regularly to maintain compliance.

FileCruncher can also be used to audit your IT security. By examining the files that infiltrate your security defences, you assess their effectiveness and take action to remedy any shortfalls.

For more information

To find out more contact us on: +44 (0)1628 760359




FAST Consultancy Services Limited
York House, 18 York Road, Maidenhead, Berkshire SL6 1SF
Tel: +44 (0)1628 622121 Fax: +44 (0)1628 760350
Email: info@fastconsultancy.com www.fastconsultancy.com

FAST consultancyservices

FASTtalk
The Quarterly Magazine for FAST Members | Issue 2 | 2007

CONTENTS

REGULAR FEATURES

ARTICLES

Welcome

Welcome to the April edition of FAST*talk*. This quarter we are bringing you a number of topical articles and opinion pieces, together with news updates on recent important Intellectual Property legislation.

On page 6, following January's long-awaited launch of Microsoft Vista, Ed Cartier from Eracent takes a look at the critical IT decisions that the new Operating System presents, and on page 18 Dominic Saunders from NETconsent explains the impact that Web 2.0 is having on corporate Internet policies. Meanwhile, on page 22, Richard Hales from F-Secure looks at the growing importance of mobile security policies for organisations that have adopted flexible working practices and could be vulnerable to the 340 or so known mobile phone viruses.

For those of you who are keen to save time and money by keeping your Software Asset Management (SAM) progress on track, we have an in-depth feature on the value of (and key steps involved in) conducting a thorough SAM Gap Analysis on page 16. And on page 28, there's a detailed overview of the recommendations made by the Gowers Review of Intellectual Property, published in December 2006.

Additionally, in true FAST*talk* style, we are covering a wide range of IT and Software Asset Management issues, offering best practice guidance on: Real-time Asset Management (p11), Unified Threat Management Systems (p14), and Business-critical Networks and IT Audits (p25).

Enjoy the issue!

Peter Kay | *Director of Services*
FAST Limited
peter.kay@fast-ltd.co.uk

Increase in M&A activity rise in software misuse

The Federation Against Software Theft (The Federation) has warned companies undergoing Mergers and Acquisition (M&A) activity to check their software licence compliance, or face civil action or even criminal prosecution.

The latest figures released by Dealogic show M&A deals worth a record £1,774 billion have taken place since January this year, easily passing the last record set in 2000 of £1,762 billion.

John Lovelock, Director General of The Federation explains: "Software is an area which can get overlooked in the middle of a take-over deal. Lawyers need to ensure software is licensed and such licences are included on the asset register – often the total cost of software licences can be considerably more than hardware. If all parties involved are clear about what is being exchanged, the legalities of software licensing won't become an issue."

OPERATION TRACKER ACHIEVES CORPORATE SOFTWARE CRACKDOWN

The Federation Against Software Theft (The Federation) has targeted a company in the UK where illegal sharing of software over Peer-to-Peer (P2P) networks was happening right under the nose of its senior management. The company, which cannot be named for legal reasons, was contacted directly by The Federation and initially denied any illegal activity was taking place on its network. It argued that it had in place a highly effective 'lock-down' policy on the entire corporate network, denying users the ability to install software or share files.

However, once The Federation began an investigation, it became clear that employees and contractors not only had access to ports on the network, but employees – both full time and external contractors – also had access to USBs. Furthermore, the company claimed it was running an active software audit tool, but this did not give it the security it required to monitor the entire network and its ports.

John Lovelock, Director General of The Federation, comments: "We want to make an example of perpetrators to stop them from stealing and passing on the Intellectual Property of our Members for good. Users can be found at any time during activities of this nature and we will continue to monitor and search for our Members' products being illegally shared. This is not a one-off-wonder."

risks

Gowers Review puts power behind copyright offences

The recently released Gowers Review on Intellectual Property (IP) has strongly recommended the implementation of section 107A Copyright, Designs and Patents Act 1988, giving Trading Standards the duty and the power to enforce criminal copyright offences. This means that Trading Standards now have a duty to investigate copyright offences and can enter your workplace, to inspect your software, with no warrants or prior notice needed.

The Review has also recommended that the penalties for theft over the Internet should match those for actual theft from a shop or person... so being convicted of a copyright offence now means being liable for 10 years in jail and unlimited fines. As a result of the ruling, any successful civil action against a company may result in damages greater than the subsequent cost of purchasing the correct number of licences.

Given that Gordon Brown is giving an extra £5 million for Trading Standards to tackle copyright infringement, and IP crime has now been recommended for inclusion on the National Community Safety Plan (putting it on the measurement criteria for Police Forces to crack down on it as a crime), there's probably never been a better time to fast-track your software compliance programme.

Read more about the Gowers Review in our Legal Update on page 28 of this issue of FAST*talk*.

Contacts

Editorial & Advertising

- Lisa Cann *lisa@c8consulting.co.uk* +44 (0)118 900 1133
- Pritam Chakravorti *pritam.c@fast-ltd.co.uk* +44 (0)1628 760320
- Clair Darke *clair.darke@fast-ltd.co.uk* +44 (0)1628 760318

Design Agency *Page Visions* www.pagevisions.co.uk

- John Tromans – Design Services Manager *john@pagevisions.co.uk*

Departmental Contacts

- Membership *membership@fastcorporateservices.com* +44 (0)1628 760357
- Events *events@fast.org* +44 (0)1628 760354
- Legal *fast@fast.org* +44 (0)1628 760351
- Marketing *marketing@fast.org* +44 (0)1628 760354
- Accounts *accountsteam@fast.org* +44 (0)1628 760356
- FAST Consultancy Services *info@fastconsultancy.com* +44 (0)1628 760359

General Enquiries:

FAST Corporate Services Limited
York House, 18 York Road, Maidenhead, Berkshire, SL6 1SF

Tel: +44 (0)1628 622121 Fax: +44 (0)1628 760350
Email: *contactus@fastcorporateservices.com*
Web: *www.fastcorporateservices.com*

FAST*talk* is a publication aimed at helping FAST Corporate Members learn more about the issues surrounding software and IT compliance. We are always interested to hear about your software compliance experiences. Please email any ideas, articles or comments to ***marketing@fast.org.***

Contributors

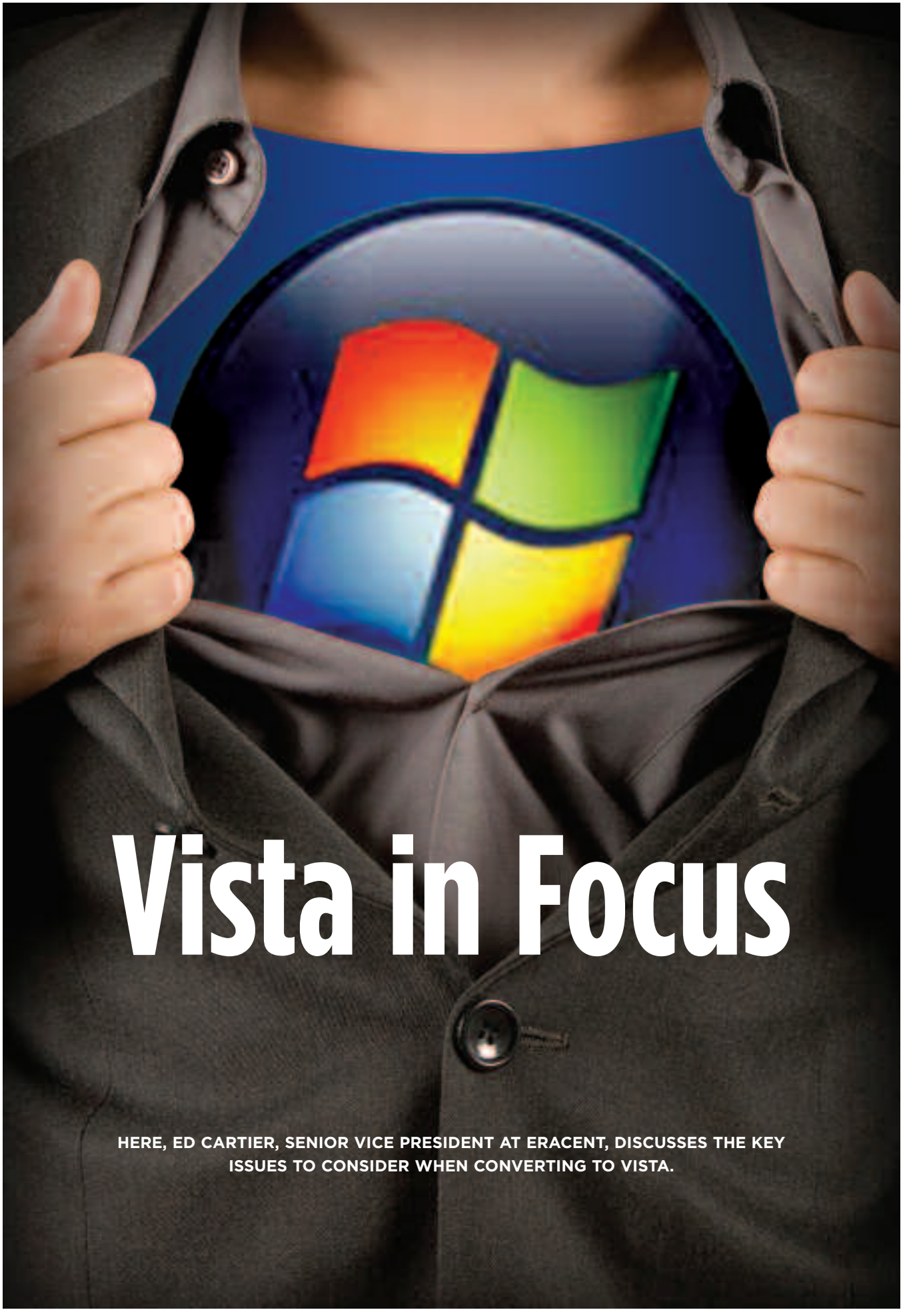
Peter Kay	*FAST Limited*
Karen Jewitt	*FAST Limited*
Anne Mead	*The Federation Against Software Theft (The Federation)*
Julian Heathcote-Hobbins	*The Federation Against Software Theft (The Federation)*
Phil Heap	*FAST Consultancy Services*

Gerry Brown *Bloor Research* | Matt Fisher *Centennial Software*
Ed Cartier *Eracent Inc* | Richard Dickinson *Essant* | *Experian*
Richard Hales *F-Secure* | Dominic Saunders *NETconsent Ltd*
Graeme Pitts-Drake *PrefixIT* | *Seaward Electronic Ltd*
Alan Lycett *Ultima Risk Management* | Ian Kilpatrick *Wick Hill Group*

Federation Member Opportunities

Federation Members have the opportunity to submit articles for inclusion in FAST*talk*. We are always on the look out for opinion pieces, FAQs and case studies that will be of interest to FAST Members. Please forward any relevant articles to us for consideration. There are also advertising opportunities in each issue of FAST*talk*. For more information, please contact:
Tel: +44 (0)118 900 1133 Email: marketing@fast.org

This magazine was produced using fonts supplied by Monotype Imaging Ltd
For more information please visit www.monotypefonts.co.uk



Vista in Focus

HERE, ED CARTIER, SENIOR VICE PRESIDENT AT ERACENT, DISCUSSES THE KEY ISSUES TO CONSIDER WHEN CONVERTING TO VISTA.

With Vista's requirements for faster processors, more memory and upgraded graphics cards, IT executives are looking at a tidal wave of 'legacy systems' that are only a few years old. Vista presents IT professionals with a series of critical decisions including: what systems to replace or upgrade, what training to offer end-users, and how to dispose of potentially thousands of serviceable, but technically obsolete, systems.

One recent study of over 400 companies of various sizes encompassing over 100,000 computers revealed that half of the systems inventories were unable to meet the minimum system requirements for Windows Vista, and over 90 per cent would not meet the optimum configurations system requirements[1]. A conversion to Vista requires a complete exposure of the configuration of all IT assets that should be upgraded.

Locating the hardware

The plan for hardware begins by creating and maintaining an accurate inventory of each desktop or laptop system in use. Organisations with IT Asset Management (ITAM) discovery systems already in place can benefit again from the investment. Discovery identifies each system's exact configuration and provides reporting to facilitate analysis. Processes supported by ITAM discovery include lifecycle management so that the location of the asset is known as well as the maintenance records. Without these processes, organisations face a steep uphill battle to just gather the baseline data. An organisation's ability to determine exactly what systems are Vista-ready, which can be efficiently upgraded and which need to be replaced, will save thousands of pounds and staff hours when the conversion begins.

Leased equipment poses another set of considerations. Unless the leases are all co-terminus, systems will be replaced in batches. It is critical that systems be replaced on schedule to avoid penalties associated with late or premature returns. "Organisations that lease, typically manage the entire lifecycle of their assets, so they are a step ahead of their peers in purchase-only shops," stated Terry Divelbliss, Director of IT Lifecycle Management for Eracent. "The problem arises when your lease schedules are dictating the upgrade rather than a plan that better suits the testing cycles required for applications. It may be well worth your time to consider re-negotiating leases or relocating leased machines so that the upgrade can follow a more natural path throughout the organisation."

Software considerations

Hardware configurations are only one set of assets to be catalogued. The software on all impacted end-user systems and servers must also be identified and inventoried. Although Microsoft Office 2003 will run on Vista, other key applications may not, especially applications developed in-house. It is likely that an application-refresh or upgrade will also be a component of the conversion to Vista, and will need to be included in the budget. Older software may need to be replaced with a comparable, more current, application.

The conversion process also provides an excellent opportunity to identify excess and unused software, or obsolete software that should have been retired years ago. "Excess software is a common finding when an organisation begins to manage its software licence entitlements with our Enterprise Entitlements Management product," stated Jenny Schuchert, Vice President of Marketing for Eracent. "Eliminating excess and obsolete software not only reduces your risk of problems during your upgrade, but potentially could pay for the entire effort. Managing your software assets reduces the need to have a buffer zone 'just in case'."

Training issues

As has been documented in the press, Vista uses a new Graphical User Interface (GUI) and it is likely that training will be needed on both Vista and Microsoft Office™ 2007. A Wall Street Journal article comments on how

vendors are planning to offer not only conversion services, but also fee-based staff training to assist customers[2]. Training issues to consider include budget, scheduling time for training immediately prior to the roll-out, and planning for an increase in help desk activity. If help desk staff have on-line access to individual end-user hardware and software inventory data, their ability to solve problems and answer questions will be greatly improved. Similarly, software inventory data can be used to determine which employees are 'power users' requiring little training and which members of the staff will require a more extensive orientation.

Knowledge is power

Dealing with a mass conversion and handling potentially immense numbers of newly created legacy systems will tax even the best IT department. Having the right ITAM processes and tools in place will be a decided advantage, keeping the project on schedule and within budget. If knowledge is power, then the knowledge provided by a comprehensive ITAM toolset will give IT professionals the power to successfully convert to Vista.

Microsoft's system requirements for Windows Vista:

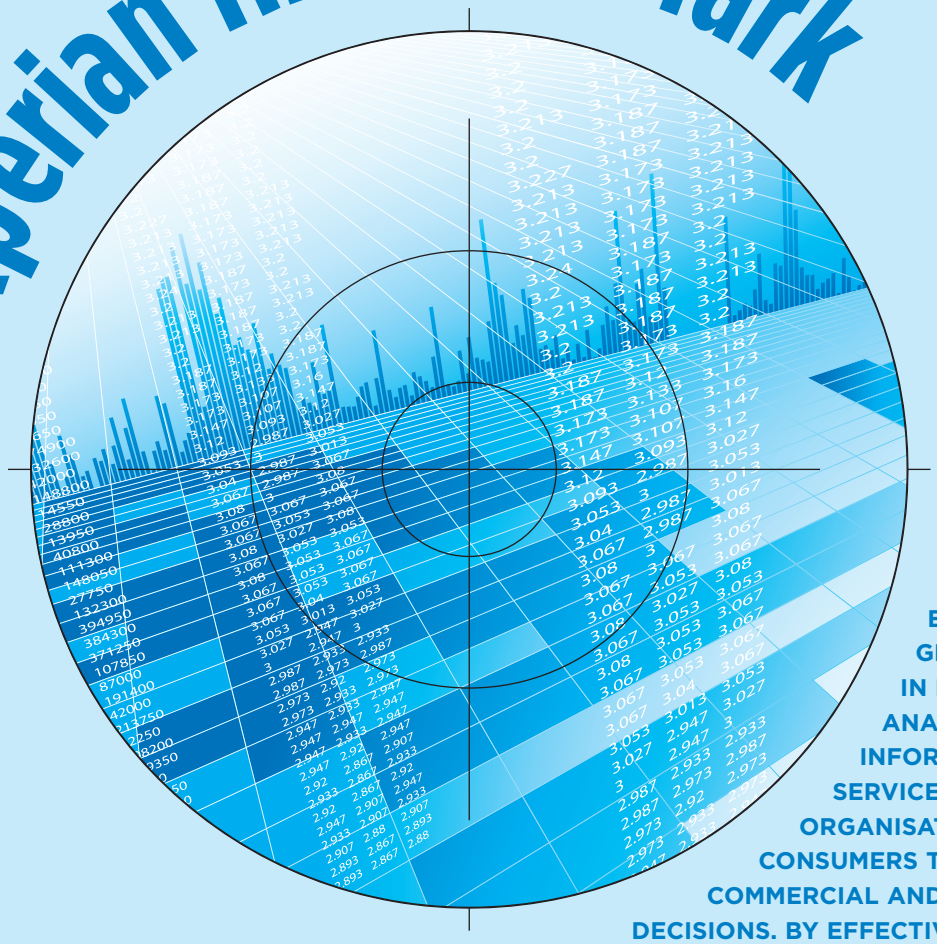
Vista Capable	Vista Premium Ready
Processor 800 MHz	1.0 GHz
Memory 512 MB RAM	1 GB RAM
Graphics Card DirectX 9 capable	DirectX 9 capable GPU with Hardware Pixel Shader v2.0 and WDDM Driver support
Graphics Memory 32 MB RAM	128 MB RAM up to 2,304,000 total pixels (e.g. 1920 x1200) or 256 MB+ for greater resolutions
HDD capacity 20 GB	40 GB
HDD free space 15 GB	15 GB
HDD type Normal	Normal, but Hybrid flash memory/hard disk recommended.
Other drives DVD-ROM	DVD-ROM

[1] *Lack of Vista Readiness Pushes PC Lifecycle Readiness to the Forefront* by Dean Williams, Corporate Services Consultant, Softchoice Corporation, December, 2006.

[2] *Vista Phobia Treatments Are Available* by Christopher Lawton, Wall Street Journal, January 25, page D1.

Ed Cartier | *Senior Vice President*
Eracent Inc | www.eracent.com
Tel: +44 (0)1702 340565 | sales.emea@eracent.com

Experian Hits The Mark



EXPERIAN IS A GLOBAL LEADER IN PROVIDING ANALYTICAL AND INFORMATION SERVICES TO ORGANISATIONS AND CONSUMERS TO MANAGE COMMERCIAL AND FINANCIAL DECISIONS. BY EFFECTIVELY REDUCING BUSINESS RISK AND PROVING COMPLIANCE, LAST YEAR EXPERIAN ATTAINED THE GOLD AWARD OF THE FAST STANDARD FOR SOFTWARE COMPLIANCE, BECOMING ONE OF THE FIRST BUSINESSES OF ITS SIZE TO ACHIEVE THIS IN A MULTI-PLATFORM ENVIRONMENT.

"Experian is a large organisation with thousands of users across a number of locations. Gaining the FAST Standard for Software Compliance is therefore a major achievement..."

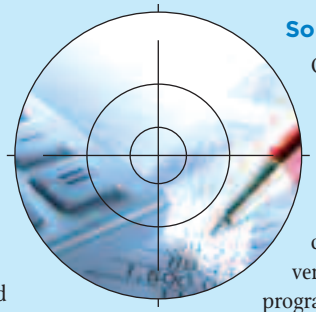
Experian delivers critical information enabling individuals to make financial and purchasing decisions with greater control and confidence. The company is a household name, most commonly known for its 'credit search' capabilities. Listed on the London Stock Exchange (EXPN) and a FTSE 100 company, Experian's operational headquarters are in Nottingham, UK, and Costa Mesa, California. It has more than 12,500 employees spanning 34 countries, supporting clients in over 60 countries.

A key goal for the company since 1999 was to achieve software compliance for its 600,000 software licences and, at the same time, to put in place a best practice framework and set of procedures to maintain and manage ongoing purchases of software and licences. In June 2006, Experian attained the FAST Standard, becoming one of the first businesses of its size to achieve this in a multi-platform environment. Over this eight-year timeframe, Experian enlisted the help of Business Continuity Services and its Software Organiser tool to successfully achieve FAST Gold status.

"...The award demonstrates that the people, policies and procedures in place for managing software licensing across Experian's large multi-platform IT environment are of the highest calibre."

Software Organiser helped Experian to:

- gain a clear view of its software assets
- reduce the risk of non-compliance and any associated costs/fines
- realise savings which equate to 30 man-hours a month
- become compliant and achieve the FAST Standard
- provide regular reconciliation reports to maintain software compliance moving forward
- progress to the next stage and start software harvesting so that the company can actually start to reap the benefits.



Achieving senior-level buy-in

Experian UK's IT department is vast, managing users across 10 sites around the country with a total of 5,000 PCs, 1,100 Wintel Servers, 100 Unix Servers and two mainframe units. Back in 1999, the company initiated a campaign to raise awareness of software licensing regulations and, as a result, it became a FAST Corporate Member in November 1999.

Richard Brown, Head of Business Improvement, Experian takes up the story:

"Maintaining compliance of all our assets is an enormous challenge, as we purchase hundreds of licences every month. Back in 1999, the company simply didn't have a clear view of its software estate and this needed to change. The first step was actually recognising this, obtaining senior level buy-in and subsequently starting a programme to achieve compliance. The first step in this process involved becoming a FAST Member."

Once the decision was taken, the journey towards the Gold award commenced. The programme was initiated with Proof-of-Purchase collation and the Commercial Services Purchasing Operations team registering all licence information into Software Organiser. Software Organiser is a licence management tool which enables companies to qualify, assess, address and reduce the risk of non-compliance through the effective management and tracking of company software licences. In early 2000, Experian changed from using an Excel spreadsheet to complete this task, to Software Organiser, which was infinitely more manageable. At the same time, the relevant processes were implemented to ensure that all purchases of software from Experian's software suppliers were recorded.

Richard Brown continues:

"In the early stages, it was really important that if an auditor came into our business we could demonstrate how our software was purchased, how it was logged and distributed. In addition, this process needed to be clearly documented, so that we could point a new starter to our policy and procedures from day one."

So near yet so far

Over the next few years the task of obtaining this licence information, raising awareness, building processes and collecting audit data continued – no easy task in a company which was seeing double-digit growth year-on-year. Nevertheless, Experian was awarded FAST Bronze in 2003 and then Silver in 2004.

At this time, Experian's risk committee identified that the consequences of non-compliance for a company of its size could be very serious, and so a project team was set up to assist in the programme. The company invested in a software deployment tool, Marimba, which also gave important audit data on all of Experian's mid-range technology. This tool detected over 2,000 different applications installed across the user environment. The Experian Board signed off a Software Policy in April 2005 and a six-week software amnesty helped reduce the amount of 'unwanted' software on machines.

And the rest is history

In June 2006 Experian achieved registration to the FAST Standard for Software Compliance (FSSC-1:2004) by FAST Corporate Services. At the time, Experian was only the third company, with more than 4,000 UK-based employees, to achieve the FAST Gold Award.

The award follows a full audit of Experian software compliance processes and policies by FAST. The review confirmed that Experian has up-to-date licences for all software installed on desktop clients, servers and the mainframes throughout the organisation, and that the policies and procedures for managing software licensing have been considered and approved at Board level.

Tiku Patel, Managing Director of Experian UK and Ireland comments:

"Experian is a large organisation with thousands of users across a number of locations. Gaining a Gold standard for software compliance is therefore a major achievement. The award demonstrates that the people, policies and procedures in place for managing software licensing across Experian's large multi-platform IT environment are of the highest calibre."

Now that Experian is compliant it can start to reap the benefits. The next stage for the company is to start a software harvesting programme. This allows licences to be passed between staff and departments where needed, rather than buying additional licences.

Richard Brown concludes:

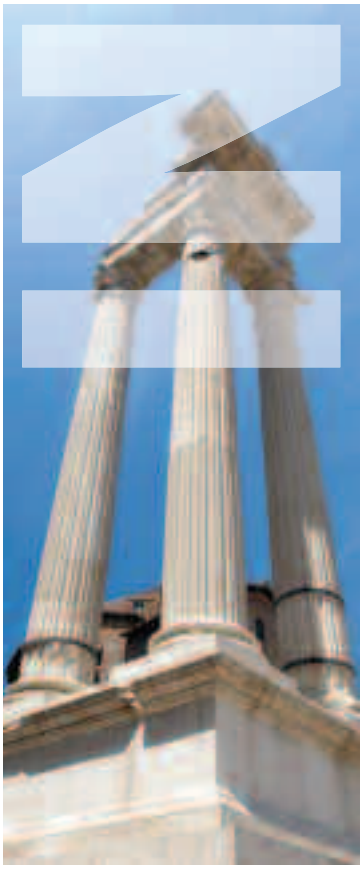
"Throughout this process, Software Organiser has been a pivotal tool enabling us to achieve compliance. We have saved 30-man hours a month, as we now log, store and manage all our licence reconciliation using this tool. It has effectively enabled us to accurately reconcile over 600,000 licences from 5,700 Proof-of-Purchase entries for over 6,000 computers."

For more information about Software Organiser please visit www.right2use.co.uk

One of the world's leading IT analyst and consultancy organisations, Bloor Research's mission is to increase business success by guiding organisations on the effective development and utilisation of information technology, through independent, expert research, analysis and tailor-made advice. Here, Gerry Brown discusses the impact of Founder-driven technology companies.

Founder-driven software vendors

— are they good for enterprise software buyers?



I met with Gerry Cohen last week, the Founder CEO of BI vendor Information Builders (IB). After 30 years in the business he still has an infectious enthusiasm for software. As has Jim Goodnight, the Founder CEO of SAS, and Michael Saylor, the Founder CEO of MicroStrategy, who founded his company in 1989. Between them, this triumvirate of Founder CEOs account for $2.3Bn of world-wide annual BI industry sales: about one third of the whole BI market.

Venture Capitalists are conspicuously absent from the ownership of their companies. These Founder CEOs represent a previous generation of entrepreneur. They used their own hard-earned cash to set up their businesses and they borrowed nothing. They are all highly intelligent, driven, and intent on continuing to do it 'their way'.

They are all technologists first and foremost. They have all engineered break-through products based on technical innovation (MicroStrategy pioneered Relational OLAP, SAS pioneered scientific/technical analytics, and IB pioneered mass reporting). They believe in the superiority of their technology with almost religious fervour. They are dismissive of the technology of their competitors. Acquisitions are for others; these Founder-driven companies believe in organic growth (although SAS did acquire data quality vendor, Dataflux).

If you have little knowledge of these companies you are not alone. A look at Google Trends confirms they are hardly on the radar. Founder-driven technology companies are often little-known outside their customers. They treat marketing with mistrust. This is based on bitter experience. MicroStrategy reputedly once spent $1m on a television advert during the SuperBowl. Information Builders similarly once spent heavily on corporate marketing. Advertisements from either are rare indeed these days.

In recent years SAS has been more aggressive, but as Hyperion CEO Godfrey Sullivan said in December 2006: "We never see them". The triumvirate are the antithesis of Business Objects and Cognos in this respect. However, this may not be all bad. If you can set a premium price, and spend very little on marketing, margins can be good. MicroStrategy posts an extremely healthy 32 per cent operating margin – around three times the industry average. If profit, rather than market share, is your goal this is a good strategy.

The triumvirate looks after their customers. As Jim Goodnight says: "when we get a customer, we virtually never lose them". SAS, in particular, is famed for its excellent customer services. As part of their SAS Poll initiative customers are encouraged to put forward their requests for software enhancements. 85 per cent of these suggestions are incorporated into SAS products. Pretty impressive.

The take-away for customers: on the upside, Founder-driven companies deliver robust and proven technology and excellent customer service and user group communities. They are immune from hostile take-over so their technology strategies can be played out. To some extent they are 'a safe bet'.

However, they are now more risk-averse than in earlier days, and are less likely to deliver ground-breaking innovation. Without substantial new investment in marketing they may be relegated to niche players over time – you can't acquire new customers if they don't know you are there. Also none have articulated a clear succession plan, so there may be continuity risk (remember what happened to Digital Equipment after Founder CEO Ken Olsen left?).

Jim Goodnight delivered the joke of 2006: "PowerPoint is used by people who have no power, and have no point". He doesn't much like PowerPoint, nor do Michael and Gerry. Like Jonny Wilkinson of the English rugby team, it is certainly too early to write them off – their companies may yet stage an amazing finale.

Gerry Brown | *Senior Analyst* | Bloor Research | www.bloor-research.com

Founded in 1989, Bloor Research distributes research and analysis to IT user and vendor organisations throughout the world via online subscriptions, tailored research services and consultancy projects. For more information, visit: www.bloor-research.com or email: info@bloor-research.com

THE BENEFITS OF IMPLEMENTING AN IT ASSET MANAGEMENT (ITAM) STRATEGY ARE WELL DOCUMENTED, YET THE VAST MAJORITY OF ORGANISATIONS ARE BEHIND IN ACHIEVING THIS ESSENTIAL MANAGEMENT GOAL. HERE, GRAEME PITTS-DRAKE FROM PrefixIT, DISCUSSES WHY REAL-TIME ASSET MANAGEMENT SHOULD BE ON EVERY IT MANAGER'S 'TO DO' LIST.

A week might be a long time in politics – but in IT it's an eternity. Everything can change and what was safe, secure and accounted for on Monday can be threatened, compromised or even gone by Friday. The world is not always a good place – we know this! People make mistakes and lose things or steal them, they download unlicensed software from the Web or their kids install it at the weekend and generally 'company property' is unguarded and out of control. Yet most IT managers are still not taking the most basic of precautions to guard their IT inventory and get automated asset management in place.

When networks were small, simple and PCs were a novelty, things were easy as pie. Asset management was a quarterly stroll amongst users with a clipboard. However, the complexity of most networks now means that IT managers have to keep tabs on a growing number of items which are increasingly widespread. IT has grown legs and is walking out the door with mobile workers, it's going home on USB hubs with employees wanting to catch up on work in the evenings, or it's being 'borrowed' by students or staff on the sly!

There is only one solution to managing today's organic network assets; and that is automated, real-time asset management. Yet despite this, in the past five years the percentage of companies that employ automated asset management has hardly changed at all, and still lurks around the 40 per cent mark. The requirements for effective asset management become indisputable as networks become more complex and the compliance environment more rigorous. Yes, as Corinne Bailey Rae recently reminded us, the more things change, the more they stay the same.

For some reason an unsavoury air has hung around asset management as if it were a dull housekeeping task, whereas in fact it could be the one single thing to most improve the quality of life for IT managers. It's a guaranteed way to realise substantial time savings and financial paybacks – that's why it's more than just a 'good idea' to get round to at some point.

For several years, Gartner and other independent analyst firms, have confirmed that organisations implementing effective asset management strategies will realise savings of between 5 and 35 per cent of their IT budgets. Software Asset Management (SAM) alone can deliver disproportionate benefits almost overnight, with many businesses seeing a budget saving of 25 per cent. According to Compass for instance, 9 per cent of software costs for UK companies are tied up in over-licensing alone.

Of course, SAM involves more than asset discovery, but a well-structured approach should also identify changing usage trends and improve operational efficiency. According to Compass, the ROI is £5 to £10 for every £1 invested in SAM processes.

Software licence compliance is a whole new ballgame; software piracy is a serious issue and although most companies fall into non-compliance by mistake or ignorance, the fault is still dangerous and often expensive to rectify.

In summary, there are five key reasons to implement real-time ITAM:

- time savings
- operational efficiencies
- cost benefits
- compliance management
- fraud prevention.

On the other hand, there's not one reason to stall the decision, so whilst the 'To do' lists for 2007 are still wet, surely real-time asset management should be added to the list, if not at the top.

Graeme Pitts-Drake	
PrefixIT PC Network Management	
Tel: 0845 222 0420 | www.prefixit.com	
graeme.pitts-drake@prefixit.com	

Ask FAST ???

Q Are UK companies allowed to act as a system builder, even if system building is not their normal business? For example, if a company's IT department prefers to build its own PCs rather than buy off-the-shelf... if they buy OEM XP home licence (with the appropriate hardware part) to use with the PC, is this okay? If so, are there any licensing considerations that should be taken into account?

A The company would need to be registered as a Microsoft System Builder. The following links may be of assistance:

- *www.microsoft.com/oem/default.mspx*
- *www.microsoft.com/oem/english/default.mspx*

With regard to home licensing, the following link may be of assistance:

- *Microsoft Work at Home (WAH) Licenses.*

Following the introduction of the WEEE Directive any computer equipment will have to be correctly disposed of...

EVERY MONTH FAST RECEIVES QUESTIONS FROM ITS MEMBERS BY PHONE AND VIA ITS WEBSITE. HERE, WE PROVIDE ANSWERS TO A SELECTION OF THOSE POSED OVER THE LAST QUARTER.

'If you connect a personal device to the network it will be audited whilst it is connected'

Q We have talked about purchasing software (mainly Microsoft) through our US subsidiary for use by UK and US employees. Our IT infrastructure is based in the UK and we are a Microsoft Gold Partner. Can we legitimately purchase software this way or does this fall under 'grey import'?

A The answer to this depends very much upon what the licence agreement(s) actually says. If it restricts use to the US or excludes Europe, then any purchases would fall under the category of 'grey imports' and would not be legitimate purchases.

With regard to your Microsoft Gold Partner status, our understanding is this can mean different things to different organisations, so again it would depend on the terms and conditions of your agreement.

Q Where do we stand with auditing employees' personal equipment as there is no specific legislation referencing this area?

A If a user refuses to let you audit their personal equipment, there is little you can do to insist. So, we recommend that you do not allow them to connect to your network.

However, if you are going to allow personal devices to connect to your network, you could consider protecting the organisation and the user by expressly covering it within your policies and procedures, stating something to the extent of: 'If you connect a personal device to the network it will be audited whilst it is connected'. If the user takes exception to this they then have the choice of not connecting to the network.

Q Do you know of any resources on the Web that will help me identify software packages from their filenames – in other words filenames which PC audit software has detected?

A Some of the following will be of assistance:

- *www.quickerwit.com*
- *www.driversearch.com*
- *www.filext.com*.

Q Can MSI files be used instead of .exe files for registration to the FAST Standard for Software Compliance (FSSC-1:2004)?

A MSI files are installers and packaging that are used to install and configure application executables. Many applications don't use them at all; .exe files are used because they are the application. The logic extends to only looking at the install/uninstall list in Microsoft Windows. Many applications simply don't appear there at all.

Q What can we do to protect ourselves from the Data Protection issues associated with disposal of computers?

A Make sure that all company data is removed and the hard drive is destroyed. Through the introduction of the WEEE Directive any computer equipment will have to be correctly disposed of, however, disposal companies should supply a certificate of disposal.

Q When donating old equipment to charities, schools, staff etc., how should we handle this with regards to disposal?

A Make sure that a signed agreement is in place clearly stating what has been passed to whom. In some cases software publishers may need to be informed of the change of ownership.

Q How can we track the movements of hardware and software effectively?

A Have an agreement with facilities so that you can track what equipment is where. Also, you need to have links with Human Resources for starters and leavers – so that you can issue and revoke passwords to manage equipment effectively.

For more information and answers to other questions, please visit the FAQ database by logging into the FAST MemberZone
www.fastcorporateservices.com

UTMS

In The Spotlight

IAN KILPATRICK, CHAIRMAN OF WICK HILL GROUP, TAKES A LOOK AT HOW UNIFIED THREAT MANAGEMENT SYSTEMS (UTMS) CAN HELP WITH SECURITY SYSTEMS MANAGEMENT, AND OFFERS ADVICE ON CHOOSING A UTM APPLIANCE.

UTMS have been growing in popularity for the last few years. This is largely because they provide an excellent means of reducing security costs and simplifying the whole process of security systems management and installation. UTMS growth is predicted by many analysts to significantly exceed that of firewalls and individual point security solutions over the next few years.

The minimum requirement for a UTMS, according to IDC, is a firewall, VPN, anti-virus and intrusion detection/prevention. UTMS have, however, evolved from this to incorporate additional capabilities, which can include URL filtering, spam blocking and spyware protection, as well as centralised management, monitoring, and logging capabilities.

While the widest deployment of UTMS has been in SMEs, larger organisations are also using them, as they increasingly appreciate the benefits of less expenditure and easier centralised administration. Large organisations are typically using UTMS to centrally secure branch and remote offices; or alongside their existing gateway firewall, for the additional UTMS functionality.

The benefits of UTMS

Cost is a key factor behind the growth of UTMS, with some appliances costing less than a quarter of the price of equivalent point solutions. Significant cost savings come from simplified and reduced installation, as well as fewer ongoing management costs such as training, maintenance and upgrades. And of course, UTMS have only one dedicated platform to support.

UTMS also provide some major benefits in relation to software and hardware management. A single dedicated appliance is a significant reduction in asset inventory, and of course removes the licence tracking and reporting issues of point solutions installed on servers.

Larger organisations using point solutions are often unable to scale the solutions to the number of sites they have, because of cost, installation, management and ongoing support issues. This can lead to organisations deploying reduced security and inferior policies at remote locations. UTMS can enable them to overcome these problems.

A stated disadvantage of UTMS is that they have a single point of failure with all security systems potentially down at the same time. This is typically dealt with by using high availability.

There is no legal definition of a UTMS and there are significant variations between UTMS appliances. The variations are on price, functionality, performance, scalability and most importantly security.

Issues to consider

Key factors to consider when buying a UTMS are future proofing and performance issues. With some UTMS, you can start off with just the security solutions you need and add extra functionality as required, which is a good option. You should also look for a solution which allows you to easily upgrade performance.

Beware of vendor performance statistics. Many UTMS aren't designed for all the functions to work together, so performance can fall off rapidly when all functions are switched on. This is often not apparent in the statistics, which may give performance details with most of the functions switched off!

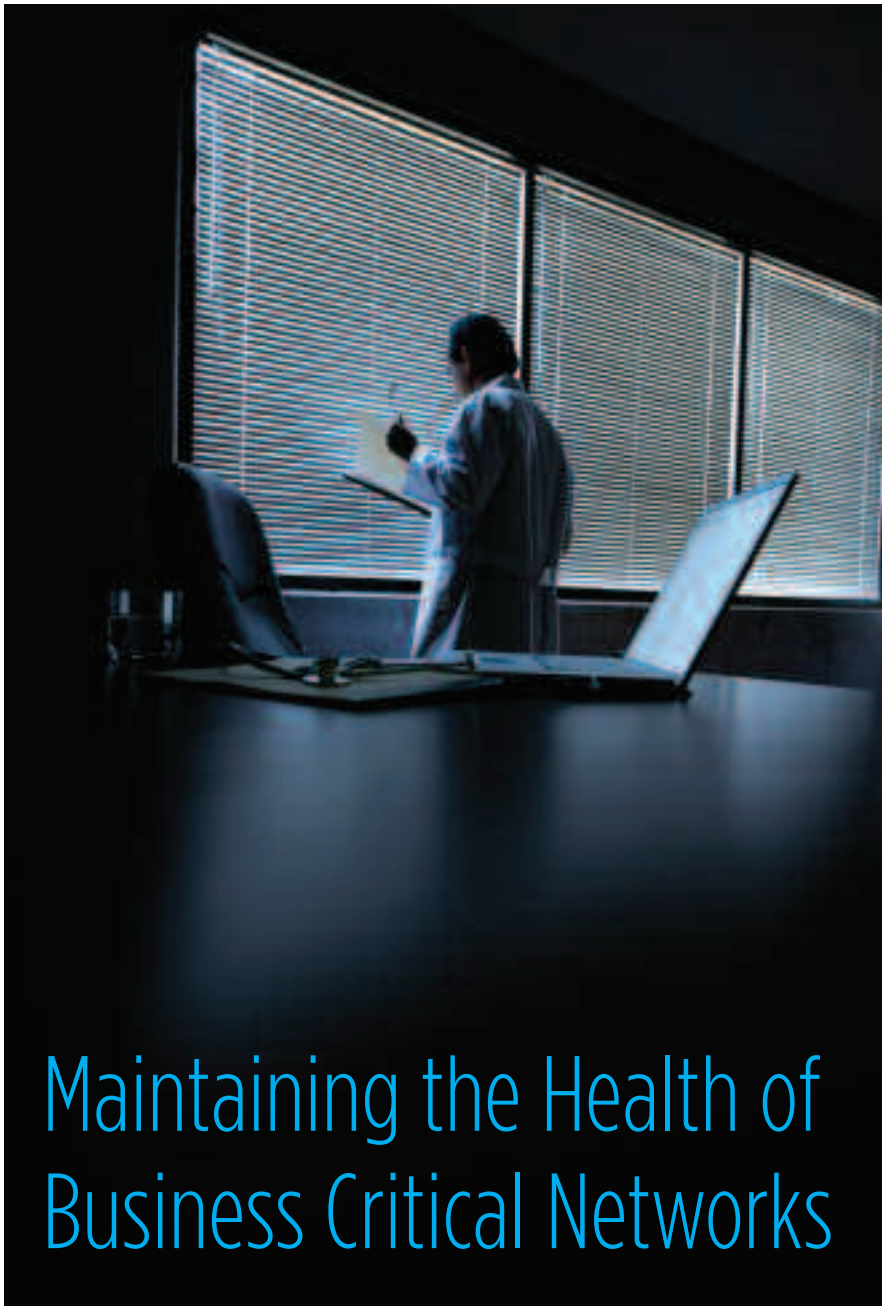
Finally, make sure you choose a UTMS which has deep packet inspection firewall, as a minimum, not just stateful inspection, which doesn't provide adequate security.

Ian Kilpatrick | *Chairman*

Wick Hill Group

Tel: +44 (0)1483 227600

iank@wickhill.com | www.wickhill.com



Maintaining the Health of Business Critical Networks

HIGH AVAILABILITY ENVIRONMENTS NEED RELIABLE AND SECURE NETWORKS. HERE, RICHARD DICKINSON, DIRECTOR OF ESSANT, DISCUSSES THE ADVANTAGES OF TAKING A PROACTIVE APPROACH TO ASSESSING THE HEALTH OF YOUR BUSINESS CRITICAL NETWORK.

A high availability environment requires a network that is fully secure and compliant, resilient to failure, easily manageable and with sufficient capacity to meet future organisational objectives.

As corporate networks evolve in line with strategically-led deployments of new services and systems, they are continually exposed to different risks and pressures. Cumulative changes, such as device upgrades and security practice amendments, are commonplace. Meanwhile, protocols, technologies and their means of implementation are constantly improved. Add to this factors such as personnel changes, mergers and acquisitions, and keeping track of networked assets, and their configurations and associated software becomes a sizeable undertaking.

In this environment, taking a proactive approach to assessing the health of your network can help improve knowledge, reduce costs and mitigate risks, whilst also ensuring conformance to best practice, whether for internal purposes or to meet with external regulatory compliance.

In cases where an organisation is looking to capitalise on offering new networked services, or is planning network upgrades in the near future, a structured, independent audit of the appropriateness and effectiveness of its systems and controls is highly recommended. In certain sectors, when an organisation relies on its IP network for the successful delivery of mission critical services, a regular audit is enforced by industry regulators.

For any mission critical network, the recommended frequency for such audits is once every 12 months. To maximise the usefulness of the audit itself, it is recommended that the operational and technical objectives of the organisation are taken into consideration, prior to the audit commencing. In order to gain buy-in from all relevant stakeholders, the audit should be carried out by a team who have direct reporting lines into senior management and are independent of the day-to-day activities of the organisation. In this way, a clear and impartial view of the findings can be ensured.

Once organisational objectives have been agreed and documented, it is recommended that the audit should begin as soon as possible. Of fundamental importance to the audit's success, is that all data gathered is then reviewed against best practice and that an assessment of compliance is made. It may be useful to categorise areas into compliant, partially compliant and non-compliant. This means that priorities can be easily identified and any non- or partially-compliant areas can be brought in-line with best practice, quickly and effectively. Once the audit is completed, all major stakeholders should reconvene so that buy-in to recommendations can be achieved.

The benefits of a regular audit are numerous. Through gaining an appreciation of the network's vulnerabilities, potential problems can be highlighted prior to outages, and the risk of network downtime and associated costs can be minimised. The insight gained from the process and documents created will enhance the capability and knowledge of key staff, and simplify the ongoing management of the network and its assets. Finally, ongoing costs relating to maintenance contracts and software licences can be saved and asset lifecycle and performance management can be undertaken far more effectively.

Richard Dickinson | *Director*	
Essant | www.essant.co.uk	
richard.dickinson@essant.co.uk	
Tel: +44 (0)8456 740047	

STARTING OUT ON A SOFTWARE ASSET MANAGEMENT PROJECT CAN FEEL LIKE A JOURNEY INTO THE UNKNOWN ... BUT IT DOESN'T HAVE TO BE A HIGH RISK VENTURE. A LITTLE STRATEGIC FORWARD PLANNING CAN GO A LONG WAY, AS PHIL HEAP, MANAGING CONSULTANT, AT FAST CONSULTANCY SERVICES EXPLAINS.

Sustainability matters

So, you've made the commitment to creating a legal software environment and managing your software assets to optimum financial benefit. You've achieved Board-level approval for your initial plans, signed up to the FAST Standard for Software Compliance, and started to think about the first steps you need to take in order to embark on your Software Asset Management (SAM) project. All good stuff! The key question that now remains is how are you going to sustain your focus and enthusiasm for the project over the long-term?

You're probably already aware that establishing a legally compliant software environment will take time*, energy, and laser-like concentration – especially if you want to be as prudent as possible with the financial and people resources that have been allocated to the project. But are you also aware of the extent to which a best practice approach to SAM project planning can significantly reduce the effort involved in reaching your project goals on time and within budget?

In my experience, even the most conscientious IT managers sometimes gloss over this critical project planning stage. The most commonly cited reason is that it can be tricky to know where (and how) to begin. As a result, many new FAST Members considerably under-estimate the full scope of the software compliance challenge – and that's when it can start to get both expensive and frustrating. The good news is it doesn't have to be that way.

Expedition unknown!

Coping with a company-wide SAM programme is a bit like preparing for a long-haul expedition into unknown territory – and one which may well throw up a few wild beasts and some complicated team challenges along the way! To be successful, you need to do ample preparation up front and then put in place a carefully constructed journey plan with clear milestones. That way, you'll be minimising the potential risks involved, making sure you keep your business aims and project objectives in mind every step of the way, and giving yourself the best chance of sidestepping any problems that do arise before they have a chance to make a negative impact.

In essence, the key steps in shrewd SAM project planning are simply good business sense. As the Cheshire Cat in Lewis Carroll's 'Alice in Wonderland' tale so elegantly explains – if you don't much care where you want to get to, it doesn't matter which way you go. So, conversely, if you want to be sure of reaching your SAM destination, you first need to be clear about where you want to get to – and then build a detailed project plan that considers the disciplines involved at every stage, as well as the potential pitfalls and obstacles that may occur.

A SAM Gap Analysis is the ideal tool for making sure that your SAM project stays on track. If it also benchmarks your progress against FSSC-1:2004 (the FAST Standard for Software Compliance), so much the better. Properly conducted it should pinpoint your essential steps to success by:

- carrying out a high-level review of your existing IT infrastructure
- identifying the critical vulnerability points and areas of unmanaged risk in your business
- assessing the potential gaps in your resourcing, budget, or management information armoury.

Some FAST Members take up to a year to reach Bronze level and a further six to 12 months to get to Silver because they lose focus along the way. A Gap Analysis can help to refocus and therefore reduce the time taken.

A SAM Gap Analysis is the ideal tool for making sure that your SAM project stays on track...

Bridging the gap

Ideally, any SAM Gap Analysis worth its salt will examine the following key areas from a risk perspective and provide detailed metrics to enable you to benchmark your compliance progress:

- IT policies and procedures
- IT procurement (hardware and software)
- software delivery to business and end-users
- software licence and media storage and control
- software movements / additions / changes
- software and media disposal
- hardware disposal
- current audit strategy
- current reconciliation strategy
- company communication, training and culture.

By providing you with a perfect understanding of your organisation's software compliance start-point and then mapping this analysis across into a bespoke project plan (which can be reviewed at regular intervals against your business goals), a risk-based SAM Gap Analysis will ensure that your company stays on target to meet the assessment criteria identified by the FAST Standard for Software Compliance, FSSC-1:2004.

In addition, by highlighting all the information and resources you need to gather along the way, identifying and mitigating any potential risks at an early stage, and offering a best practice approach to seeing the project through to completion, your SAM Gap Analysis will help to maintain the crucial buy-in of your Board.

Minimising the threat of vendor audits

With the growing threat of fines and imprisonment for Company Directors who fail to prove that their IT environment is beyond legal reproach (a fact that is being driven by accountability legislation such as Sarbanes-Oxley, 2002 and The Companies Act, 2006), establishing a firm compliance position as quickly as possible has never been more important. Your SAM Gap Analysis can help here too.

A Compliance Readiness Review, which gathers information on your company's installed software base and compares this with the licence entitlement that your company holds, will typically be the first stage in any effective SAM Gap Analysis. Not only will this provide a good indication of your likely software compliance position, but it will also help improve your negotiating position in the event of annual true ups or even vendor-driven audits.

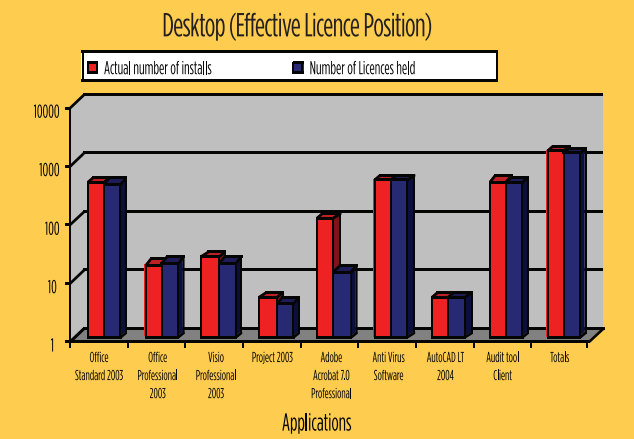
Just imagine if you are asked to demonstrate your entitlement to use a particular vendor's software and you have no idea what entitlement you have, even for the most common desktop applications. You could end up paying larger fees than needed purely because you haven't collected some basic information about your software estate. An example of the kind of graphical information that your Compliance Readiness Review should be able to provide is illustrated by the bar chart below.

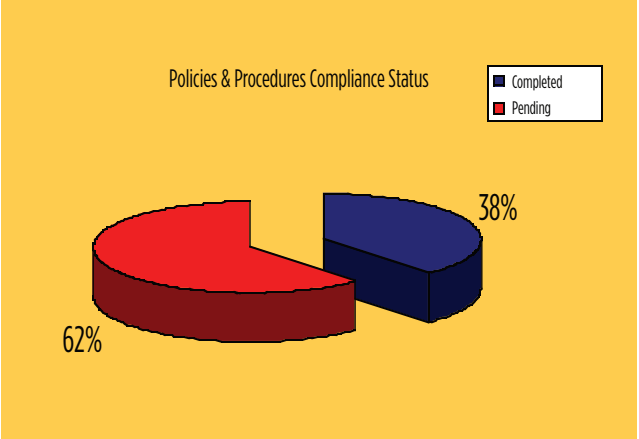
Springboard to success

A SAM Gap Analysis is a great start-point from which to launch your software compliance project. It will help to protect your organisation in the early stages by identifying your likely current compliance position and pinpointing the probable extent of the project ahead. It will also help to guide, measure and control your company's progress through the numerous tasks that need to be properly completed in order to reach each level of the FAST Standard for Software Compliance (see the pie chart below, which illustrates policies and procedures readiness – one of the requirements of FSSC-1:2004).

By producing an in-depth project plan which identifies the resources and skills that your SAM project requires, estimating the costs and areas of high risk involved, and producing a business case that resonates with your senior management team, a comprehensive Gap Analysis will transform your SAM project. If reducing project stress and increasing the odds of success is high on your agenda, you would be well advised to find out more.

For more information on how to create a SAM Gap Analysis or a Compliance Readiness Review that meets the criteria of your FAST Standard for Software Compliance registration, please contact: phil.heap@fastconsultancy.com.





Security in a Web 2.0 World

HAVING AN EMPLOYEE INTERNET USAGE POLICY ISN'T ENOUGH ON ITS OWN; YOU ALSO NEED TO EDUCATE YOUR EMPLOYEES, SAYS DOMINIC SAUNDERS, OPERATIONS DIRECTOR AT NETCONSENT.

Web 2.0 is here to stay

If there's a buzzword that defines the Noughties in new media circles it has to be 'Web 2.0'. The phrase inevitably means different things to different people, but essentially describes next-generation Internet applications. From a technical perspective, Web 2.0 services are enabled by new, dynamic technologies – such as AJAX – that underpin the latest generation of websites. From a social perspective, Web 2.0 defines the new wave of user-generated content and social networking sites that have shot to fame over the last 12 to 18 months and encourage two-way participation.

Indeed, sites such as YouTube, Bebo, Facebook and MySpace have become the most popular meeting places online. A National Cyber Security Alliance (NCSA) study in 2006 found that nearly half of all adult Internet users spend an average of two hours per week on social networking sites. Likewise, blogging has become a mainstream activity, with more than eighty million people aged 16 to 44 contributing their opinions online, according to a study of 16,000 frequent Internet users from global advertising agency, Universal McCann.

For consumers, Web 2.0 sites provide an opportunity to interact with like-minded individuals and find out the 'real' views of products and services from the man on the street, rather than the corporate marketer. Likewise, social media sites offer businesses a new way to reach out to customers. However, there are risks. In order to adequately protect corporate assets and their staff, organisations need to find ways to ensure that their policies cover the ever-changing Internet and have been read and understood by all concerned. Effective policies mean staff understand the risks, why they are in place and their responsibilities when carrying out their day-to-day work activities.

The growing security threat

As criminals become ever more ingenious, they provide an increasingly lucrative way for cyber criminals and organised gangs to commit fraud, steal people's identities and infect computers. According to the NCSA study, 83 per cent of adults who use social networking sites have exposed themselves to hackers and thieves by downloading unknown files. 74 per cent have revealed some sort of personal information, which could give criminals enough ammunition to hack into financial records and compromise people's personal information.

The 2006 McAfee Virtual Criminology Report highlighted two Web 2.0 scams last year. The first concerned a banner ad posted on MySpace last summer, which attempted to download spyware when users clicked on the ad and compromised almost 1.1 million computers. Another attack involved the German site of Wikipedia, the online encyclopedia that allows users to add or edit content. This same openness makes it an attractive target for virus authors to plant malicious code, which happened in October, when content about Blaster was re-written to include a link that took visitors to a site for malware, designed to infect Windows PCs.

With more than 40 per cent of employees revealing in the NCSA study that they visit websites while at their desk, it's not just an individual's own identity or IT systems that are under threat. There's also a security risk for organisations, whose employees might be inadvertently opening a backdoor to hackers and criminals. At the same time, employees could be unwittingly releasing corporate information through blogs, forums or bulletin boards. Many people approach blogs and online forums with a far more relaxed attitude than they would adopt if talking to a stranger in the street. What's more, almost all information released online is fully searchable by anyone with access to a search engine.

As criminals become ever more ingenious, they provide an increasingly lucrative way for cyber criminals and organised gangs to commit fraud, steal

Taking action

Although there are warnings and safety tips posted on sites such as MySpace reminding people that what they post publicly could embarrass or expose them – and their company – to danger, the onus is on the individual to exercise caution. But when an organisation employs perhaps several thousand individuals, controlling the use of social media has to be formalised in an Internet policy if the company is to protect its corporate assets from unintentional – or intentional – harm.

In a research report last year, John Pescatore, lead analyst at Gartner, presented organisations with a chilling warning: "Ignoring security during the Web 1.0 deployment led to website defacement, identity theft and business losses. Building security into Web 2.0 applications should be done before applications are deployed to avoid a negative business impact."

Taking a proactive approach to the Web 2.0 security threat is, therefore, vital. Many forward-thinking companies already have a policy for email and Internet usage, which states what employees can and cannot email, visit and download. However, in a 2005 poll only 16 per cent of the FAST Members that responded were confident that their organisation had an IT policy to cover the issue of blogging. The 2006 Information Security Breaches Survey from PricewaterhouseCoopers found that more companies have an acceptable usage policy for the Internet than have an overall information security policy. What organisations really need to do is update and extend these policies to cover social networking sites and blogs – outlining exactly what employees are allowed to write, send and access – if they are to protect their corporate assets and brand reputation online.

Educating the workforce

That said, it is no use if the policy becomes the company's best-kept secret and is hidden away in someone's top drawer. All Internet and email usage policies need to be communicated clearly and thoroughly to staff, otherwise measures developed to protect an organisation's corporate assets will be rendered ineffective if employees fail to observe some basic security rules.

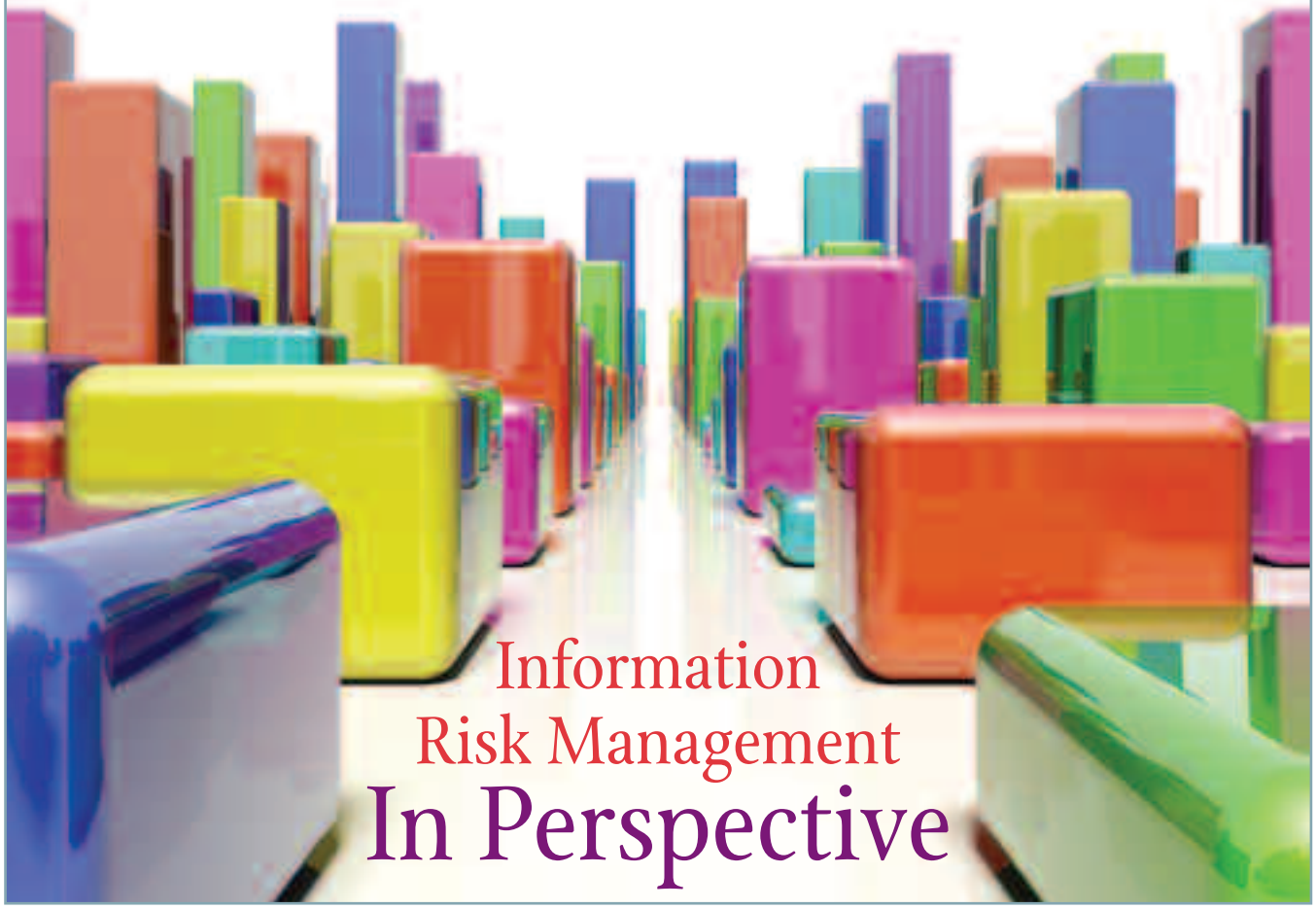
Ultimately, it comes down to educating the workforce about social responsibility when accessing Web 2.0 sites. Perhaps surprisingly, outright bans on practices such as blogging aren't always the answer. Technically it can be difficult to protect an organisation from blogging; even if well-known sites are banned in the workplace an employee could easily post entries from home or make their views heard elsewhere. And, unfortunately, some employees will always find a way to circumvent the corporate Internet policy.

So once again it comes back to educating the workforce about using Web 2.0 sites in a sensible and secure way. Moreover, the increasing Corporate Governance demands placed upon businesses today make it absolutely necessary for them to ensure policies are comprehensively deployed with a full audit trail. The traditional paper-based distribution models no longer suffice for this task and electronic solutions such as NETconsent can really help to deliver a very cost-effective alternative. It might not be as exciting as Web 2.0, but if an organisation can establish best practices now for protecting its organisation from Internet misuse, it will be far easier to update and amend employee Internet policies when Web 3.0 Internet applications arrive.

Dominic Saunders | *Operations Director*	
NETconsent Ltd | www.netconsent.com	
Tel: +44 (0)870 013 1600	
dom@netconsent.com	

people's identities and infect computers...

PUTTING IN PLACE A COHERENT RISK STRATEGY IS ESSENTIAL IF YOU WANT TO DEVELOP A SECURITY-AWARE BUSINESS CULTURE. HERE, IN THE FIRST OF A SPECIAL TWO-PART SERIES, ALAN LYCETT OF ULTIMA RISK MANAGEMENT DESCRIBES THE KEY COMPONENTS AND CHARACTERISTICS OF THIS MISSION CRITICAL BUSINESS PROCESS.



Information Risk Management In Perspective

The main Information Security Breaches Survey to be conducted in the UK is carried out by the Department of Trade and Industry every two years. The 2006 survey revealed that many UK businesses are a long way from having a security-aware culture, and that expenditure on security is either low or not targeted at key risks. Of course, the reason for low or poorly focussed investment in security controls is often quite easy to explain. The roots of this malaise lie in the fact that too few organisations have adopted a coherent risk strategy that is supported by a consistent, explainable and easy-to-use approach to risk management. Why this is so is harder to explain; after all, it is not as though the risk management process is not well defined. Detailed below is the first step... stage two will follow in the July edition of FAST*talk*.

Stage One: Assess Your Risks

ISO 27001 defines risk management as "coordinated activities to direct and control an organisation with regard to risk". Before risks can, therefore, be subject to management influence they have to be identified. This process is called risk assessment. Risk assessment comprises two processes – **risk analysis** and **risk evaluation.** The former involves the "systematic use of information to identify sources and to estimate the risk" and the latter entails a "process of comparing the estimated risk against given risk criteria to determine the significance of the risk".

Implementing risk management must be a strategic decision. It will require an organisation's senior management team (the actual risk takers in any organisation) to make certain decisions ahead of any implementation. For example, the components that comprise risk from an organisational perspective should be defined. Reference to the ISO 27001 will show that business impact, vulnerability to threats and the likelihood of a security breach occurring need to be factored in. However, some organisations only consider impact and threat probability as this two dimensional model is easier to depict in, say, a graphic. The former three dimensional model, however, provides management with a more detailed and accurate picture of the make-up of any risk scenario, thus leading to a better understanding of what can be done to reduce unacceptable risk.

What is your organisation's appetite for risk?

Another consideration follows naturally from the above. For example, what is an acceptable level of risk (often referred to as 'risk appetite') for any particular organisation and how should this be determined? This is often one of the more elusive criterion to be defined. Indeed, it is my view that, without some experience of risk assessment and implementation within an organisation, it is extremely challenging to establish a meaningful risk strategy which incorporates an appropriate risk appetite. This is where the selection of an appropriate tool or method to facilitate risk assessment can be vital. The right selection will enable an organisation to play some "what ifs", which will enable different views to be obtained until, eventually, an appropriate level of risk appetite can be defined.

The need for consistent classification

Of course, it is also important to define how risk will be calculated and decide what you want risk values to depict. For most organisations it would be a major step forward if they could calculate risk in a meaningful way so that results from different risk assessments could be compared. This qualitative approach to risk assessment is one that is broadly accepted and enables organisations to classify risk in such terms as 'high', 'medium' and 'low'. The low boundary of course would be representative of an organisation's risk appetite. The upper boundaries ('high' and 'medium') would form the basis of a strategy for risk reduction. For example, an organisation could adopt a risk reduction strategy based on simple parameters such as reduce high risks to medium risks within a six-month period and reduce medium risks to acceptable risk levels within a 12 month time frame.

Measuring impact, vulnerability and likelihood, and calculating risk

It is important to bear in mind that even this qualitative approach requires impact, vulnerability and likelihood to be measured against agreed and defined scales. The actual scales used by an organisation will vary. However, if other types of operational risks are already being assessed, then it is important that the system for measuring the components of risk and the way that risk is calculated are consistent. This will result in the organisation being able to obtain a common view of all risks and be displayed in a meaningful way in a corporate risk register. The cliché that comes to mind is you need to compare "apples with apples".

A simple example of the type of scales that could be used for measuring vulnerability and likelihood would be the traditional 'high', 'medium' and 'low'. Of course, a method would need to be adopted for determining how such a scale would be used. The guidelines, and examples, need to be published so everyone engaged in risk assessment work is assessing vulnerability and likelihood in a consistent manner.

With business impact, the scoring mechanism may need to be varied. Often organisations will adopt, say, a four or five layer model. A four layer model may result in impacts being assessed as minimal impact at the lower end, to catastrophic at the higher; with the intervening layers being described, for example, as significant and major. Accompanying guidance can be provided in order to ensure that impact, like vulnerability and likelihood, is assessed in a consistent manner so that credibility of the process is maintained.

The 'Red Amber Green' (RAG) diagram below (Figure 1) shows how risk can be depicted, taking account of impact, vulnerability and likelihood.

Threat Name	Vulnerability	Likelihood	Impact	Risk Score %
Malicious code such as viruses, worms, and trojan horses	1.95	4	2.1	31
Unauthorised information access by outsiders or external hacking	1.55	3	2.8	27
User error	1.8	3	2	23
Air conditioning failure	1.47	3	2	18
Unauthorised information access by insiders including internal hacking	1.54	2	2.7	17
Water damage	1.16	3	2	14
Operations error	1.69	2	2	14
Power failure	1.37	2	2	11

Figure 1

'RAG' diagram for a risk-averse organisation

The RAG diagram provides information on specific threats, for example:

- malicious code
- the impact that the threat may cause
- vulnerability based on the presence of appropriate controls to manage the threat
- and the likelihood of the threat occurring taking into consideration local factors such as environment and history of events.

The risk score is represented as a percentage of the worst possible risk score – that is the factorisation of the highest level of impact, vulnerability and likelihood. 'High', 'medium' and 'low' levels of risk are shown in traditional traffic light (red, amber, green) colours. In this particular illustration the RAG boundaries have been set at 25 per cent and 15 per cent, the latter being representative of the risk appetite of the organisation. Using this particular approach to risk assessment, these particular boundaries would be typical for an organisation which would want to adopt a fairly risk-averse strategy.

An organisation wishing to adopt a less risk-averse strategy could amend the boundaries upwards to say 30 per cent and 20 per cent. This would result in fewer high risks with the consequence that less priority would be associated to risk reduction measures. This is illustrated in Figure 2 which contains the same information as in Figure 1 but with the revised boundaries being adopted for the RAG display.

Threat Name	Vulnerability	Likelihood	Impact	Risk Score %
Malicious code such as viruses, worms, and trojan horses	1.95	4	2.1	31
Unauthorised information access by outsiders or external hacking	1.55	3	2.8	27
User error	1.8	3	2	23
Air conditioning failure	1.47	3	2	18
Unauthorised information access by insiders including internal hacking	1.54	2	2.7	17
Water damage	1.16	3	2	14
Operations error	1.69	2	2	14
Power failure	1.37	2	2	11

Figure 2

'RAG' diagram for a less risk-averse organisation

So that's stage one. Stage two is all about where you go from here and how you manage the security risks you have identified. Don't miss out on the second part of this article in the July edition of FAST*talk*!

References:

ISO 17799-1: 2005 Security Techniques – Code of Practice for Information Security Management (ISO 17799)

ISO 27001: 2005 Security Techniques – Information Security Management Systems – Requirements (ISO 27001)

BS 7799-3: 2006 Information Security Management Systems – Guidelines For Information Risk Management.

Alan Lycett | *Principal Security Consultant*

Ultima Risk Management

www.ultimariskmanagement.com

alycett@ultimariskmanagement.com

Mobility is high on nearly every company's agenda. Here, Richard Hales, F-Secure's Country Manager, UK and Ireland, offers guidelines for keeping your workforce secure on the move.

Richard Hales	
Country Manager, UK & Ireland	
F-Secure | www.f-secure.co.uk	
Tel: +44 (0)845 890 3300	
richard.hales@f-secure.com	

Securing the mobile enterprise

Today's working environment is becoming increasingly mobile. The global economy has set new standards for communications, productivity and customer expectations in working life.

What's more, flexible working legislation, increasing business travel and the wider availability of broadband mean that employees seldom work from the office on one machine. It's more likely that workers will log on to corporate networks remotely and keep in contact via their mobile phone.

There's also the technology issue. Device proliferation has left many a road warrior armed with a whole host of gadgets ranging from PDAs to smartphones.

Adopt a device-centric approach

As new devices increase in popularity, so do the associated threats and viruses that seek to infect them. Whilst most of us have anti-virus software installed on our PC, the chances are that not all of our devices will be protected in the same way.

Take mobile phones for example. Until a few years ago the very notion of a mobile phone virus just wouldn't have crossed people's minds. Yet, in 2004, Cabir became the first mobile phone virus to hit users' phones and transmit via Bluetooth.

There are now 340 mobile phone viruses, which, while they don't wreak havoc, compromise the security of information on the user's phone.

Security vendors have responded with anti-virus solutions that can be installed on smart phones to protect these devices in the same way as a PC.

Beware of friendly-fire

But security solutions alone cannot solve the problem. Users must adopt best practice to ensure that they do not bring about their own problems.

Laptops left in taxis, infections brought in to the company via USB sticks, or security features switched off on anti-virus protection are just some of the examples of how mobile users can be the mobile enterprise's own worst enemy. Although not a malicious attack on the company, 'friendly fire' can be just as damaging.

Developing a mobile security policy sets out a framework and simple set of reminders to employees on the move.

Protect against zero-day attacks

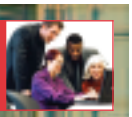
In recent years, hackers have become quicker to exploit vulnerabilities once they have become generally known.

The industry is now bracing itself for 'zero-day' attacks. In these instances the hackers themselves will identify the flaw and launch an attack before any fix can be issued.

There are now solutions capable of protecting users against unknown exploits by quarantining suspicious software. So, even if a piece of malicious code is detected on a remote worker's laptop while connected at a customer's site, the threat will be neutralised – and remain in quarantine when they connect to the corporate network, rather than rampaging undetected.

As well as being a tremendous business enabler, mobile working can also open up the corporate network to the danger of an attack. It's a technology issue as much as a cultural one. Future-proofing your enterprise to securely accommodate an increasingly mobile workplace will keep you one step ahead of the competition – and the virus writers.

The IT Security Group is sent to the Tower!



Delegates gathered on the morning of 24 November 2006 to meet with and hear presentations by experts from the Federation's IT Security Group (ITSG) at the latest in its series of free seminars (*"Looking at Defence in Depth – An Approach to Layered Security"*) which was held, appropriately, at the Tower of London.

The event was designed to help organisations develop and implement policies to combat the increasing number and complexity of threats, not only in the work environment, but also at home and through mobile phones.

The first presentation, given by Richard Hales of F-Secure, initially focused on explaining the threats that everyone needed to be aware of before a security policy could be devised – after all if you don't know what the threats are, how can you combat them? Richard then went on to give examples and concluded with some general business policy guidelines.

Neil Larkins of Pointsec then highlighted to the audience the internal threats that companies face from employees deliberately or accidentally transferring data outside the company by the use of smartphones, iPods and USB memory sticks. Amazingly, 55 per cent of firms recently surveyed have taken no action to protect themselves against the threat posed by removable media.

The final presentation, by Frank Coggrave of Websense, outlined the external threats that companies need to be aware of, citing phishing, malicious websites, spyware, crimeware and keylogger installs amongst others. Frank illustrated the harm that these can do and explained how organisations can protect themselves against them.

The morning was completed by the presenters taking part in a lively question and answer session, after which delegates were able to speak to ITSG Members participating in the event, on a one-to-one basis. Feedback from delegates was exceptional – 98 per cent said that they would recommend ITSG events to other FAST Members – and comments included: "very beneficial with a lot of up-to-date information on current and future threats..." and "more of the same please!"

If you missed this interesting and thought-provoking event, why not take a look at the slides? You can download them from The Federation's website at: http://www.fast.org.uk/itsgroup.asp.

The next ITSG event – *"Re-drawing the Battle Lines"* – takes place on the morning of 15 May at Bletchley Park, Milton Keynes, home of the Enigma code breakers! For more information, please turn to the article on page 30.

Or, to book your place, please contact Karen Jewitt by email at: events@fast.org.

About The Federation's IT Security Group

The IT Security Group, established by The Federation, aims to educate and provide organisations with secure and efficient IT systems. The members of the Group are: 3M UK plc, Aladdin Knowledge Systems, BigFix Europe Ltd, Brookcourt Solutions Ltd, Centennial Software Ltd, Computer Forensic Alliance, Elcom ITG, F-Secure (UK) Ltd, Nexus Technology Ltd, Pointsec Mobile Technologies Ltd (formerly Reflex Magnetics Ltd), Secure Ltd, Secure Computing International Ltd, SecureWave Ltd, SurfControl plc, Ultima Risk Management Ltd, Websense UK Ltd and Wick Hill Ltd.

Contact details for all these companies may be found on the Corporate Members' website under: FAST Programme Resources/Federation Groups or FAST Programme Resources/Supplier Directory.

The Group holds regular free seminars for Corporate Members – keep an eye on the Events Circular for the next event.

Any provider of security products or services that would like more information about the Group should contact Anne Mead, Federation Membership Manager, at: anne.mead@fast.org.

ON BEHALF OF THE FEDERATION'S ASSET MANAGEMENT GROUP, MATT FISHER, VP OF MARKETING AT CENTENNIAL, DISCUSSES HOW IT AUDITING IS ESSENTIAL TO GOOD RISK MANAGEMENT AND IT GOVERNANCE PRACTICES.

IT Audit

– it's not all about software compliance

It's often tempting, especially when you're in the middle of a FAST programme, to view the importance of your IT audit data as limited to software compliance. While it's true that you can't achieve compliance without an accurate view of what's on the network, it's also important to understand the wider benefits that full asset discovery can bring.

In this article, we're going to look at the impact that having complete visibility of the network has on risk management and the wider issue of IT governance.

Setting the scene

The role of IT continues to evolve as more companies realise the impact that IT can have on the organisation's bottom line. Fundamentally, the objective of IT should be to help the organisation establish a complete and dynamic understanding of their corporate IT infrastructure and its usage in order to maximise IT efficiencies, mitigate security and compliance risks, enforce policies and reduce the cost of IT operations.

However, with software and hardware continually being added, moved, re-configured and retired, with new devices coming on and off the network daily, and with the rapid growth of user-installed software and personal hardware connecting to the network, today's IT estate is more challenging to track and manage than ever before.

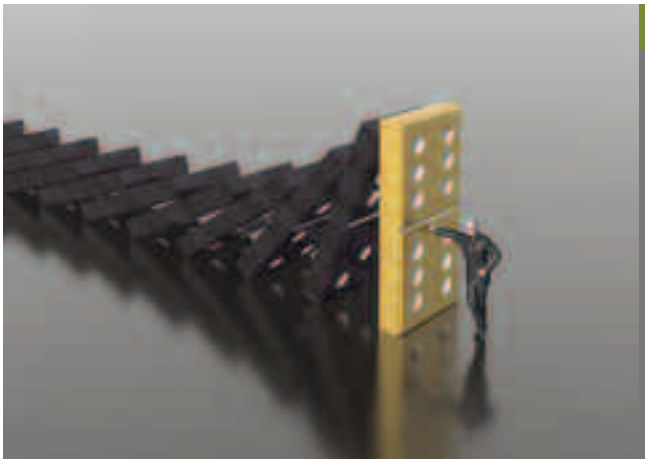
To effectively meet this challenge, organisations must ensure that they have complete visibility of what they have, how it is used and what impact its presence or loss may have on the organisation.

Managing risk

Risks to the organisation and its network come in many different forms. Whether it is the all-too-familiar risk of non-compliance, the threat of security breaches or legal and productivity issues surrounding employee use of IT systems.

Let's assume that the risks around software licensing are well understood and don't need further elaboration. But, what about the wider issues of compliance? Depending on your industry sector and corporate parentage, your organisation may be subject to all manner of national and industrial regulations which require full visibility of the network – whether it's financial reporting for Sarbanes Oxley or tracking computer and data usage for HIPAA.

IT security – i.e. the protection of the network against security breaches – is often viewed as a distinct requirement which is addressed through substantial investments in perimeter defence technologies such as firewalls, email filtering and anti-virus solutions. But not all IT security risks originate outside the enterprise.



HOW TO GET MORE FROM YOUR AUDIT

- don't rely on a historic snapshot. Audit regularly to keep abreast of changes to the IT environment
- use audit data – version numbers, patch levels etc. – to monitor the network for possible security risks
- share audit data and management reports with multiple stakeholders across the organisation
- don't start any major IT project or initiative without a full understanding of the present state of the IT estate
- think outside the box. Audits usually contain a wealth of untapped data – check you're not missing out on valuable network intelligence.

From security flaws in commonly-used business applications, to the presence on the network of unwanted Peer-to-Peer (P2P) and hacking tools, any company that doesn't know exactly what is on the network is potentially leaving the front door wide open.

And it's not just operating systems and applications that are at risk. Increasingly, hackers are targeting vulnerabilities in the firmware found on hardware such as managed switches, routers and other network devices.

Even the presence of large quantities of unwanted files such as MP3s, JPGs and other non-business documents can point to wider security and productivity issues.

With security flaws in software and hardware being exposed every week, it's near impossible to understand how vulnerabilities 'in the wild' translate onto the organisation's network. In order to effectively understand and combat the risks facing each individual IT estate, it is vital that managers and administrators have a clear and complete understanding of the current make-up of IT assets.

Optimising ongoing IT management

In a dynamic IT environment, it's all too easy to lose sight of the impact that the state and condition of the IT estate can have on an organisation and its bottom line. Decisions are made locally without understanding their impact to the broader organisation. Policies are made but without consideration to how they will be enforced. And network lines are often blurred and defences bypassed as hardware and software are moved to and from the network.

Many parts of the organisation, from network administrators to chief financial officers, need access to information about the IT estate. For some, like help desk agents, this data in a raw form, integrated directly into a service management application, provides the perfect level of information. For others, the transformation of that raw data into actionable business intelligence is required.

Yet many users of ITAM (IT Asset Management), ERP (Enterprise Resource Planning) and project planning applications are frequently both disappointed and hampered by the lack of totality of information they require or the inability to turn raw data into effective business intelligence.

This lack of visibility and information-sharing will invariably lead to over-spending, increased risk and a generally less productive IT environment.

Beyond software compliance

As this article highlights, it's important to remember that an IT audit isn't just for software compliance. The benefits of making the right tools choice and implementing the right asset management processes can pay dividends way beyond the completion of a FAST or vendor audit.

Asset discovery – the ability to have complete visibility of the hardware and software on the network – should be central to any organisation's IT management strategy, ensuring that assets are utilised to the full and that liabilities are kept to a minimum.

The Asset Management Group

This article has been written on behalf of The Federation's Asset Management Group, a group of audit and asset management tool publishers who have come together to collectively provide expert advice and guidance to FAST Corporate Services Members.

The Group was formed in December 2003 and the current members are; ASAP Software, BigFix Europe Ltd, BMC Software, Centennial Software Ltd, Computer Associates UK Ltd, Deskforce Europe, Enteo UK, Eracent Inc., Hitachi Europe Ltd, Hornbill Systems Ltd, HP, Liken Ltd, Novell UK, Phoenix Software Ltd, Richmond Systems Ltd, RMS Services Ltd, ScanTrack (PTY) Ltd and Touchpaper Software plc. Contact details for all these companies may be found on the Corporate Members' website under: FAST Programme Resources/Federation Groups or FAST Programme Resources/Supplier Directory.

The Group will be holding free, product neutral seminars and workshops during 2007. Dates and venues will be announced in FAST*talk*, the monthly events circular and FAST*forward*.

Any asset management tool publisher that would like more information about the Group, should contact Anne Mead, Federation Membership Manager, at: anne.mead@fast.org.

Introducing FAST Forums

FAST Forums bring together representatives from different businesses and industries and provide a chance for Members to discuss issues surrounding the FAST Standard for Software Compliance (FSSC-1:2004) and any hurdles they are facing, as well as other matters surrounding IT compliance.

FAST facilitates Forum meetings across the UK and they are included as part of your FAST Membership, so they are free for you to attend, and you are welcome to bring a colleague along too. Here, we provide a little more background information to whet your appetite!

Content and logistics

Chaired by FAST Corporate Advisors, Forum sessions tend to last three hours and most provide a choice of a morning session starting at 09.30 or an afternoon session starting at 13.00. The content of every meeting is tailored according to Member input and suggestions, and group discussion steers the direction of each session. Topics covered at previous Forums include:

- policies and procedures
- discovery tool selection and capabilities
- entitlement collection and cataloguing
- data analysis
- data management
- software/hardware asset management
- ISO standards
- ITIL best practices
- legislation surrounding email and Internet use
- and many other issues you may have faced or will be faced with in the future!

In response to Member requests we have also had many guest speakers at past meetings including: BCS, FAST Consultancy Services, and Creative Publishing Solutions (Fontworks).

In between the Forum meetings, MemberZone Discussion Forums are available if you want to exchange ideas with other FAST Members from your meeting.

All Members will receive an invitation for their local forum from their Corporate Advisor.

In the meantime, if you would like more information please contact your Membership or Corporate Advisor using the details opposite.

General regional Forum dates

11/04/2007	East Mids	AM
17/04/2007	Bracknell	AM
17/04/2007	Bracknell	PM
17/04/2007	Stafford	AM
17/04/2007	Lancashire	PM
23/04/2007	Glasgow	AM
23/04/2007	Glasgow	PM
25/04/2007	Manchester	AM
25/04/2007	Manchester	PM
26/04/2007	Reading	AM
26/04/2007	Reading	PM
26/04/2007	York	PM
17/05/2007	Aberdeen	AM
17/05/2007	Aberdeen	PM
22/05/2007	Edinburgh	AM
22/05/2007	Edinburgh	PM
13/06/2007	Belfast	AM
13/06/2007	Belfast	PM

Forthcoming INDUSTRY-SPECIFIC FORUMS

We are currently gauging interest in Forums for the Education, Charity, and Finance sectors. If you would like to attend any of these industry-specific Forums, or if you would like FAST to run a Forum for your industry sector or in your area, please contact your FAST Membership Advisor on: +44 (0)1628 760357 or email: membership@fastcorporateservices.com

- **Northern Local Authority Forum**
  Tuesday 24 April, 11.00 – 15.00: Kirklees Council, Huddersfield
- **Central England Local Authority Forum**
  Tuesday 12 June, 10.30 – 14.30: Staffordshire County Council Offices
- **Scottish Local Authority Forum**
  Thursday 14 June, 11.00 – 15.00: West Dunbartonshire Council, Dumbarton

More dates for our industry-specific Forums will be listed in the 'Events' section of the FAST MemberZone as soon as they are available.

FAST Membership Team AREAS

Alan Cousins
Corporate Advisor
+44 (0)7866 422424

Raza Khan
Membership Advisor
+44 (0)1628 760339

Amanda Driver
Corporate Advisor
+44 (0)7811 965379

Michael Man
Membership Advisor
+44 (0)1628 760342

Rebecca Warton
Corporate Advisor
+44 (0)7971 461887

Liana Cook
Membership Advisor
+44 (0)1628 760341

Matt Parsons
Corporate Advisor
+44 (0)7970 935929

Paul Clements
Team Supervisor
+44 (0)1628 760344

Pete Thomas
Corporate Advisor
+44 (0)7816 826396

Georgina Godsell
Membership Advisor
+44 (0)1628 760340

Andy Lennon
Corporate Advisor
+44 (0)7730 620042

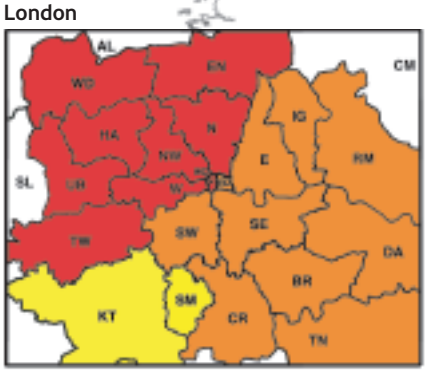
Membership Advisor
By Company Name:

A-CL	Liana Cook
Co-J	Michael Man
K-S	Georgina Godsell
T-Z	Phil Herd

Nick Sparks
Corporate Advisor
+44 (0)7855 419260

Phil Herd
Membership Advisor
+44 (0)1628 760343

London



Channel Islands

E-mail the Membership Team: firstname.lastname@fastcorporateservices.com

LEGAL UPDATE

THE FEDERATION'S LEGAL COUNSEL JULIAN HEATHCOTE-HOBBINS TELLS US MORE ABOUT THE GOVERNMENT'S APPROACH TO PROTECTING INTELLECTUAL PROPERTY IN THE UK.

Protecting Intellectual Property

Gowers

In this issue of FAST*talk*, I would like to provide you with an update on the Gowers Review of Intellectual Property (IP) that was published on 6 December 2006. A copy of the Review can be downloaded from: **www.hm-treasury.gov.uk/independent_reviews/gowers_review_intellectual_property/gowersreview_index.cfm.**

The Review has caused much deliberation, as it was commissioned by the all-powerful Treasury Department, providing a good indication that the matter is being taken seriously by Government.

Originally announced by the Chancellor of the Exchequer in December 2005, the Gowers Review examined the UK's IP framework, reporting into the Chancellor and the Secretary of State for Trade and Industry and the Secretary of State for Culture, Media and Sport.

The Review is in line with the Labour Party Manifesto for the 2005 General Election which clearly stated:

"We will modernise copyright and other forms of protection of Intellectual Property Rights so that they are appropriate for the digital age. We will use our presidency of the EU to look at how to ensure content creators can protect their innovations in a digital age. Piracy is a growing threat and we will work with industry to protect against it."

In responding to the Review, the Federation worked in conjunction with other Members of the Alliance Against Intellectual Property Theft (see www.allianceagainstiptheft.co.uk) to urge the Gowers panel to recommend vital changes to the way that IP rights are enforced in the UK.

Certain changes are required to improve the Intellectual Property regime to ensure the health of the software industry now and in the future. The Federation is concerned that respect for copyright is dwindling in corporate UK and believes that this issue should be addressed as one of importance as jobs are threatened.

The Federation called for a demonstrative display of Government support to protect one of the most important industries in the UK today, and that means the Gowers Review must address the deficiencies in the IP regime including enforcement. It is about addressing some key problems and making sure our system is fit-for-purpose. This is a clear necessity when you realise the creative industries as a whole employ over 2 million people and contribute over £11.4 billion to our balance of trade.

GIT

So, the Gowers team have reported – what's next? In short, *"GIT"*, or *"Gowers Implementation Team"*. The Government is serious about making sure the Gowers recommendations are implemented and, as a result, the GIT team have sprung into action and are openly sharing a helpful status table at: **www.patent.gov.uk/policy/policy-issues/policy-issues-gowers.htm**.

Julian Heathcote-Hobbins	
Senior Legal Counsel	
Federation Against Software Theft	
julian.hobbins@fast.org	

In conclusion, I ought to sign-off by summarising the increased risks to business' software users which GIT will have to see through into law:

1. The implementation of section 107A Copyright, Designs and Patents Act 1988. If your business is suspected of misusing software, Trading Standards will have a duty to investigate, and can visit your premises to inspect the software being used. No warrants or prior notice are needed. A conviction for copyright offences may carry a prison sentence of up to 10 years and an unlimited fine for serious copyright offences.

2. The penalties for infringement of copyright via the Internet become comparable with those for infringements by other means. This means theoretically that illegal file-sharing (in the office) is punishable by 10 years imprisonment, five times more than the current two years.

3. If your company is successfully sued for misusing software, it is envisaged that the damages payable may be multiplied. In practice, this means that your company may well have to pay more than just the licence fee that it should have paid in the first place.

4. IP crime has been recommended as an area for 'police action'. This implies that IP crime could be placed on the National Policing Plan. IP crime would then be an area which Chief Police Officers were measured against. Consequently, police forces around the country would make IP crime an area to crack down on. Police have powers under section 109 Copyright, Designs and Patents Act 1988.

WE WANT TO HIGHLIGHT THE SUCCESS THAT FAST'S FEDERATION MEMBERS ARE HAVING IN THEIR FIGHT AGAINST LICENSING AND COPYRIGHT INFRINGEMENTS. HERE, IN THE FIRST OF A REGULAR LEGAL NEWS SERIES WE HEAR FROM SEAWARD ELECTRONIC...

SEAWARD STRIKES BACK AGAINST ILLEGAL SOFTWARE SALES

Successful legal action is helping electrical safety testing specialist Seaward Electronic Ltd to step-up the fight against illegal online sales of its specialist software products.

In November, Seaward successfully obtained a judgment against Mr Michael Mellors from Nottinghamshire for the sale of PatGuard programs on eBay which infringed Seaward's Intellectual Property Rights.

PatGuard is a proprietary portable appliance testing data management software system and is a well established market leading brand.

Seaward was alerted to the sale of the product on the Internet, and in a judgment issued on 13 November 2006 at Nottingham County Court, Judge Reeson ordered that Mr Mellors pay Seaward a sum representing an account of the profits he made as a result of the act of infringement of Seaward's copyright in the PATGuard program and Seaward's costs, disbursements and interest.

Mr Mellors sold over 20 infringing copies of the software over several months resulting in lost potential revenue of over £10,000.

In addition to this case, Seaward is also actively pursuing other parties which are illegally selling copies of Seaward's software and Seaward recently made an out-of-court settlement with another individual selling the software on eBay.

Mark Marsh, Seaward Group Finance Director, said: "The company is very happy with the outcome of the legal action and we intend pursuing the individuals who have purchased the software from Mr Mellors.

As part of a zero-tolerance policy on software theft, we actively monitor the Internet for illegal sales that infringe our rights, and this example should act as a serious warning to all those involved in supplying and purchasing unauthorised Seaward products online."

Seaward is also in talks with The Federation Against Software Theft (The Federation) to identify additional ways in which genuine software can be protected.

Seaward Electronic Ltd
www.seaward.co.uk
Tel: +44 (0)191 586 3511
karenm@seaward.co.uk

RE-DRAWING THE BATTLE LINES

15 MAY, BLETCHLEY PARK, MILTON KEYNES

Free half-day ITSG event

ON TUESDAY 15 MAY, the Federation's IT Security Group (ITSG) will be running a special half-day seminar at Bletchley Park – the historic site of secret British code breaking activities during World War Two and the birthplace of the modern computer.

The event will give delegates the opportunity to find out about the latest techniques for protecting their organisations both before, and after, a security incident, keeping casualties to a minimum.

Entitled 'Re-drawing the Battle Lines', the half-day ITSG event will cover three key topic areas:

- **Understanding the Rules of Engagement: Policy Management**
  How can organisations do more to make their staff aware of their rights and responsibilities in helping to mitigate risk?
- **Let the Battle Commence: Removable Media and Mobile Working**
  What are the dos and don'ts of managing security without creating an administrative nightmare for IT staff?
- **The Aftermath: Incident Investigation**
  What should you do and what can you do when all lines of defence fail? This session will provide an introduction to the role of computer forensics, explaining its requirement and value in the context of a real case study.

After lunch, delegates will have free access to Bletchley Park's fascinating National Codes Centre where they can check out the tales of spies and strategic deception and view the Enigma, Bombe, Lorenz and Colossus machines.

TO BOOK YOUR FREE PLACE ON THIS SEMINAR

please contact Karen Jewitt

by email at: **events@fast.org**

or call: **+44 (0)1628 760354**

Photos courtesy of Bletchley Park | www.bletchleypart.ord.uk

FAST consultancyservices

Advances in technology are rapidly changing the landscape for Software Asset Management.

Licensing models are more complex than ever before.

50 per cent of IT directors now spend much more time on licence management than they did 12 months ago.

The complexity involved in managing multiple licensing deals is making it tricky for companies to maintain compliance.

FAST Consultancy Services provide expert advice and support to help UK organisations manage their software environments legally and cost-effectively.

Our portfolio of services includes:

- Benchmark assessment
- Policies and procedures
- Business case development
- Asset management tool selection
- Audit, data management and reconciliation
- FileCruncher data analysis services
- FileCruncher file identification services
- Managed Services.

To find out more about
FAST Consultancy Services
please visit our website at:
www.fastconsultancy.com
call us on: **+44 (0)1628 760359**
or email: **info@fastconsultancy.com**

FAST Consultancy Services, York House
18 York Road, Maidenhead, Berkshire SL6 1SF

CONSULTANCY

Our courses fill up quickly, so do book early to avoid disappointment!

FAST Events Calendar | April – December 2007

FAST CORPORATE SERVICES COURSES

FAST Software Management Day – 1 day course

CONTENT: This course will help you achieve the FAST Bronze Award. Successful completion of the end-of-day exam will qualify you as a 'FAST Approved Software Manager'. The day is available to FAST Corporate Members only and covers:

- the FAST Standard
- legislation
- licensing basics
- licence collection & cataloging
- policies and procedures.

COST: This course is available for Corporate Members only at the special rate of £395 + VAT. As part of your Membership you may be entitled to a free place*. Please contact your Membership Co-ordinator on +44 (0)1628 760357 to check your entitlement.

April	18	Leeds
	18	London
May	17	Swindon
	17	Midlands
	23	London
June	7	London
	20	Warrington
	27	Glasgow
July	11	Leeds
	12	Swindon
	12	London
	19	Midlands
August	8	London
September	6	London
	13	Midlands
	26	Warrington
	27	Edinburgh
October	17	London
	31	Leeds
November	8	London
	14	Bristol
	21	Midlands
December	6	London
	12	Warrington
	13	Glasgow

The FAST Software Audit Day – 1 day course

CONTENT: This course will help you achieve the FAST Silver Award. Successful completion of the end-of-day exam will qualify you as a FAST Approved Software Auditor. The day is available to FAST Corporate Members only and covers:

- why audit and the planning stages
- licensing and contractual collection
- electronic audit tools
- case study
- reconciliation.

COST: This course is available for Corporate Members only at the special rate of £395 + VAT. As part of your Membership you may be entitled to a free place*. Please contact your Membership Co-ordinator on +44 (0)1628 760357 to check your entitlement.

April	19	Edinburgh
	26	London
May	10	Leeds
	22	Midlands
	23	Swindon
June	12	London
July	11	Glasgow
	18	Leeds
August	9	Midlands
	15	Swindon
September	20	London
October	18	Leeds
	24	Midlands
November	15	Edinburgh
	22	London
	29	Warrington
December	13	Midlands

FREE

Free event places

Some FAST seminars are offered free to help you on your path to compliance. Places on these courses are always in great demand. So, although we appreciate that meetings can crop up from time to time, we hope you will understand our policy of levying a £50 cancellation charge for non-attendance on a free course without three days' notice. Full details of this cancellation policy can be found on the Events page in the FAST MemberZone.

Microsoft Licensing – 1/2 day seminar

CONTENT: FAST is running a series of half-day licensing seminars aimed at helping you deal with the complexities of MS Licensing. Each seminar will look at the following areas:

- proof of purchase
- MS licensing programs explained
- disaster recovery
- working at home
- licensing and downgrading licences
- server and CAL
- OEM
- transferring and cataloging licences.

May	22	Leeds	pm
June	14	Birmingham	pm
September	12	London	am
October	2	Leeds	am
November	6	Birmingham	pm

COST: This course is available for Corporate Members only at the special rate of £99 + VAT.

BOOKING: Look out for dates and locations on the FAST website and in the FAST Events Bulletin email. To register for your place, please email Karen Jewitt at karen.jewitt@fast-ltd.co.uk with your PO number/method of payment.

Data Protection Act – 1/2 day seminar

FREE

CONTENT: FAST Corporate Services, in association with Ultima Risk Management, is running a series of free half-day Data Protection Act (DPA) seminars covering:

- introduction to the DPA: objectives and main principles
- roles and responsibilities within the organisation for DPA compliance
- the main principles which impact on the IT department
- impact of DPA on outsourcing
- impact of DPA on email/internet monitoring
- the need for staff education.

April	19	Birmingham	pm
June	11	Leeds	pm

BOOKING: Look out for dates and locations on the FAST website and in the FAST Events Bulletin email. To register for your free place, please email Karen Jewitt at karen.jewitt@fast-ltd.co.uk.

ISEB Certificate in Software Asset Management Essentials – 3 day course in conjunction with Ultima Risk Management

CONTENT: This 3 day course will provide delegates with a qualification which covers the Software Asset Management (SAM) processes as described in the SAM module within the IT Infrastructure Library (ITIL) and closely follows the ISO 19770-1:2006 Standard. The course will enable delegates to confidently sit the multiple choice BCS/ISEB Certificate in Software Asset Management Essentials exam which is taken on the final afternoon of the course.

April	23 — 25	Birmingham
May	8 — 10	Maidenhead

Upon completion of the course delegates will be able to:

- describe the objectives and major activities required to implement SAM
- explain and use SAM techniques and processes
- be aware of the support tools and techniques available and be able to indicate how possible improvements can be made
- manage software assets through stages of their lifecycle
- prepare and distribute SAM reports and plans throughout the organisation.

COST: The cost of this course is £750 + VAT per person for FAST Members, £950 + VAT for non-Members.

BOOKING: There are only a limited number of places on these courses, so to book please contact: events@fast.org or call: +44 (0)1628 760354, providing a PO number or credit card details for payment.

**Dependent on Membership level*

Please note that the content of this Events page is subject to change.