Information Systems Audit and Control Association

ISSN 1356-0735

DATAWATCH

In this issue:

Issue 49, Jun-Sep £3.00

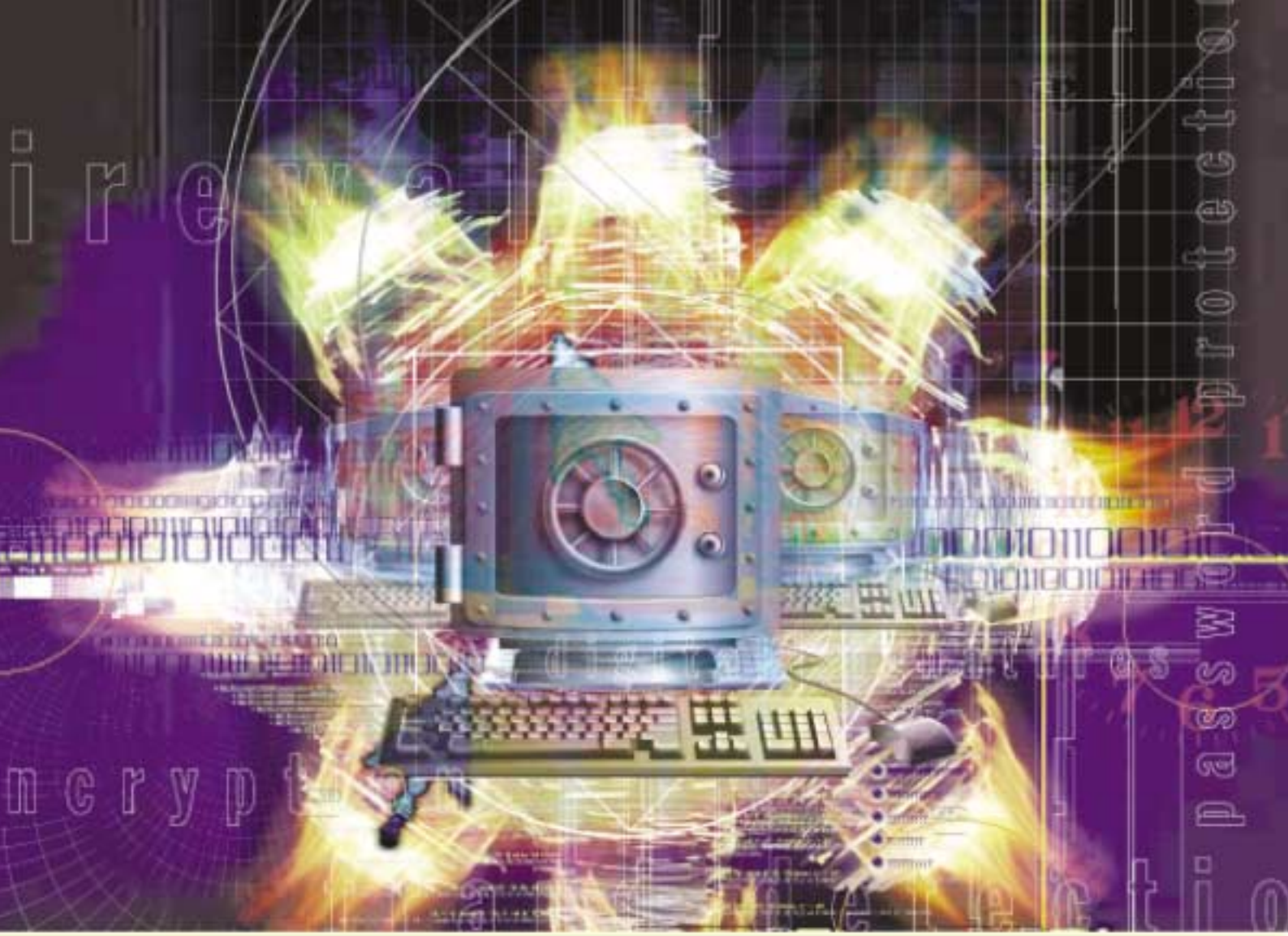
- Implications of Regulation of Investigatory Powers Act
- Windows NT 4/2000
- Back to Basics
- E-Procurement

2001 London Chapter's 20th Anniversary

www.isaca.org.uk

When the Grim RIPA calls

The Quarterly Magazine of ISACA London Chapter



NETWORK SECURITY CONFERENCE

Network Security Conference
Amsterdam Hilton
Amsterdam, Netherlands
11-14 November 2001

Register Now and Save!
Early Registration Deadline:
20 August 2001

Each session is a half-day technical presentation.

World-renowned and respected presenters.

Now in its third successful year!
First time in Europe!

Topics include:
- Using SSL—It's Easier Than You Think
- Understanding and Implementing Firewalls
- Securing the Mainframe TCP/IP Network
- Intrusion Detection
- Anatomy of Internet Attacks
- Whither PKI: What It Is, Why You Need It, What It Takes to Get Ready for It
- Computer Incident Response
- Building an Enterprise Security Architecture
- Computer Forensics for the IS Auditor
- VPN Concepts and Solutions

Optional Full-day Workshops:
- Network Security Fundamentals
- Network Penetration

Earn up to 25 CPE Hours

For Information:
Web site:
www.isaca.org/nsc2001am.htm
E-mail: conference@isaca.org
Call: +1.847.253.1545 ext. 485

Information Systems Audit and Control Association

,49, Jun-Sep 2001

DATAWATCH

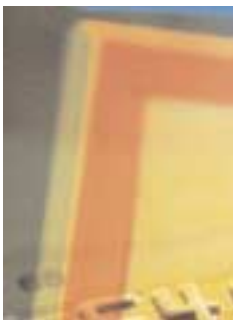
Information Systems Audit and Control Association

DATAWATCH is published by the ISACA London Chapter. Membership of the chapter entitles one to receive an annual subscription to DATAWATCH.

Opinions expressed in DATAWATCH represent the views of the authors. They may differ from policies and official statements of the ISACA London Chapter and its board, and from opinions endorsed by authors' employers, or the editorial team of this magazine. ISACA London Chapter does not attest to the originality of the authors' content.

10 Drayhorse Road
Ramsey, Huntingdon
Cambs PE26 1SD
www.isaca.org.uk
nancy@isaca.org.uk

In this issue:



regulars

ISACA London Chapter Committee 2001/2002

PRESIDENT
Karen Sharpe
Deloitte & Touche
0207 303 7478
karen.sharpe@deloitte.co.uk

VICE PRESIDENT
Charles Mansour
The Woolwich
0208 298 5646
Charles.Mansour@woolwich.co.uk

TREASURER
Archie Watt
BDO Stoy Hayward
0207 893 2671
Archie.Watt@bdo.co.uk

SECRETARY
Joseph Wright
0207 260 +6843
joe-wright@supanet.com

MEMBERSHIP/RESEARCH
Kamal Khan
Rabobank International
020 7809 3935
khank@rabo-bank.com

PUBLICATIONS
Annabel Lane
Nestle UK Ltd
0208 667 6530
Annabel.Lane@uk.nestle.com

PUBLICATIONS/SIGS
John Hunter
HLB Development Consulting
01635 248944
jhunter@hlbdc.com

PUBLICATIONS/SIGS
Bill Hawkins
Corporation of London
0207 332 1296
Bill.Hawkins@corpoflondon.gov.uk

EXTERNAL RELATIONS
Derek Oliver
Ravenswood Consultants
01268 794556
consultants@ravenswood.co.uk

PAST PRESIDENT
John Mitchell
LHS Business Control
01707 851454
Lhs@lhscontrol.co.uk

CISA CO-ORDINATOR
Michael Christodoulides
District Audit
01438 351570
m-christodoulides@district-audit.gov.uk

WEBMASTER
Allan Boardman
Internet Working 4U
01732 462 133
allan@internetworking4u.co.uk

INTERNATIONAL
Steve Bailey
Steve Bailey Associates
01480 432602
Spart@compuserve.com

EVENTS
Gideon Pretorius
KPMG
Gideon.Pretorius@kpmg.co.uk

EVENTS
Nick Fellows
The Woolwich
0208 298 5646
Nick.Fellows @barclays.co.uk

GENERAL ASSISTANCE
David Spaven
KPMG
0207 311 5620
David.Spaven@kpmg.co.uk

ISACA Northern UK Committee (officers only)

PRESIDENT
Ray Butler
HM Customs & Excise
0161 827 0875
ray.butler@hmce.gov.uk

VICE PRESIDENT
Robert Newbould
Corus plc
Bob.Newbould@corusgroup.com

TREASURER
Ian Simpson
Halifax plc
IanDSimpson@halifax.co.uk

SECRETARY
Peter Thompson
peter.thompson@deloitte.co.uk

MEMBERSHIP
Alan Rainford
Axa Insurance
01253 662782
alan.rainford@axa-insurance.co.uk

CISA CO-ORDINATOR
Gan Subramaniam
Skipton Building Society
gsubramaniam@skipton.co.uk

ACADEMIC RELATIONS
Mike O'Hara
University of Salford
0161 295 5665
m.j.ohara@salford.ac.uk

WEBSITE:
www.isaca.org.uk/northern

ISACA Central UK Committee (officers only)

PRESIDENT
Mike Hughes
KPMG
0121 232 3207

VICE PRESIDENT/CISA
Simon Parker
Capital One
0115 843 6456

SECRETARY
Chris Chandler
Arthur Andersen
0121 233 2101

TREASURER
Geoff Adey
KPMG
0121 232 3202

PAST PRESIDENT
James Whittaker
BT
0121 230 2214

WEBSITE:
www.isaca.org.uk/central

All change! We have just passed through that time of the year when the London Chapter Committee members stand down, change roles, or stand for re-election. Those members who were able to attend the AGM in May will know the results of the voting for the elected officers.

So there have been some changes. You'll see that the President's column is now written by Karen Sharpe, who has just taken on this role. Charles who was secretary takes on the mantle of Vice President while his post is filled by Joe Wright. Our former president John Mitchell takes the Robin Cook option of becoming the committee's resident Past President. We call it the voice of sanity role and his experience will continue to be at the disposal of the committee as a whole.

Some things, however, don't change. There are many of us on the committee who don't require direct election under our constitution and the Publications team members fall into that category. We also found ourselves inexplicably saying "yes" when John asked us at a previous meeting whether we were prepared to continue in our roles. So here we all are again, committed to maintaining Datawatch to its current standards and improving it where possible. Once again we have scooped the Best Newsletter award for large ISACA chapters in the Europe/Africa region, an achievement we hope to continue. Just because I get to tell you this doesn't mean I do all the work though. Far from it. Putting together a magazine like this one is a team effort and in particular we would be unable to do it without the expertise of our Chapter Administrator, Nancy Watt, who, as long term readers will know, continually strives to improve the magazine's layout and appearance.

On to this quarter's contents. I think we have some great articles as usual. Security policies are a theme with a Back to Basics article by Brian Shorten on the creation of a policy - yes, even now, not everyone has one - and this theme is picked up by Karen Nelson's article on endorsement of security policies. Our new president provides a discussion of the risks that can be associated with e-procurement - still a popular area for IS projects despite the condition of the dot com market. And Andy Farrington guides us through the Regulation of Investigatory Powers Act (RIPA); something which has generated a great deal of comment. It also gives an opportunity for a spectacularly dreadful pun - Who says computer audit can't raise a smile?!

Correction

In Vol 48 of Datawatch, article: "The E-Corporation and the Law".

This article refers to Robin Chater's 1999 report to the Office of the Data Protection Commissioner (now Information Commissioner). Unfortunately we indicated that Mr Chater represented an organisation called Privacy International. This is not the case. Mr Chater is the Director of The Personnel Policy Research Unit and has no connection with Privacy International. We would like to apologise for any confusion this may have caused.

MIND GAMES
by Puzz

How many words of three letters or more can you find from the word

INTERNET

30 words: good
40 words: very good
50 words or more : excellent
Answers on page 32

As I recall, the conversation went something like:
"Will you be the next President, Karen?"
"No John, I won't, I don't have enough time."
"Go on, be the next President."
"No!"
"Pleeeaase! We'll all be there to support you"
"Oh, go on then, I'll do it!"

So here I am, late at night on the eve of the copy deadline for DataWatch looking at my computer screen and thinking to myself, "What on earth have I done and what am I going to write about?"

It's been an interesting few weeks since I was elected to look after the London Chapter on 17th May. I have been an ISACA member for 8 years now, so I thought I knew a bit about the organisation. Admittedly, I have been organising events for the last two years but that hasn't really required me to deal with anyone in ISACA (apart from the other Board members!). However, I have been involved in many discussions on a myriad of topics in that time, so there can't be that much to it. Or can there?

The biggest change that I have noticed to my life (apart from having to write articles for DataWatch and the Mailshot) is the huge number of e-mails I now receive from International on a vast range of subjects. I have received (and read) ISACA publications for years and was aware of most of the issues that have recently been brought to my attention. The only difference now is that I am taking much more notice. Did you know that there are 22,453 members from 195 Chapters around the World, and London, with 639 members at the last count, is the biggest?

All this information set me thinking, why are we all members of this organisation? There have been numerous efforts to collect this information from members in London over the years with, it has to be said, little success. The best I can do, then, is think back to why I joined 8 years ago.

My employer at that time, the National Audit Office (NAO), encouraged me to join ISACA and sit the CISA exam. The NAO, along with many other employers, had recognised the value of employing people with a professional computer audit qualification. I looked at the paperwork, discovered that CISA was recognised all over the world, and agreed with them. Once I had been a member for a few months, I started to receive high quality, informative publications and to attend the local Chapter events and training days and realised that ISACA was also a means of maintaining my professional knowledge.

For me then, there are 2 key benefits of ISACA membership:

- recognition of CISA by employers as the premier IT audit and security qualification; and
- professional training opportunities.

So what is ISACA doing to promote and maintain these key benefits? Promotion of ISACA as the best international institute for IT audit and security professionals can be demonstrated by ensuring that we are seen to be at the forefront of research. This is the function of the Information Systems Audit and Control Foundation (ISACF). Now that we have achieved financial stability in London, the Board will be looking closely at opportunities to involve the London Chapter in appropriate research projects to help promote the value of our qualification and generally add value to our members.

We can also promote CISA as a qualification and IT audit and security as a profession by working to raise awareness of ISACA within academic institutions. This latter area is something that we intend to work hard on in London over the next year, hence our appointment of John Mitchell to be responsible for Academic Relations.

The London Chapter has a good track record of providing high quality training opportunities to members, through the monthly meetings and training weeks. We are committed to continuing with this effort during the next year. In addition, the DataWatch editorial team is very skilled at cajoling people into providing high quality technical articles to keep us all up to date! On an international level, I have joined the organising committee to plan EUROCACS 2002, which will take place in March 2002 in Budapest and which, as usual, promises to provide a very valuable training forum for our members.

That takes me nicely to Paris, the venue of EURCACS 2001. This event will be preceded by an International Presidents' meeting, to which I will travel tomorrow evening. I am sure to learn a great deal from that event and will let you know all about it in my next President's column.

Until then, happy auditing!

When the Grim RIPA calls

The Implications for Business of the Regulation of Investigatory Powers Act

By
Andy Farrington, CISA

There can have been few items of legislation in recent years which have generated as much controversy as The Regulation of Investigatory Powers Act (RIPA). As the Bill progressed through the legislative process it was intensely debated in the media and received a particularly savage mauling in the House of Lords. Since the first parts of the Act came into force in October 2000, much of the hyperbole has ebbed but it remains an object of concern to on-line privacy groups, civil libertarians and business. It is an Act with which we, as computer audit and security professionals, should be familiar not least because the provisions relating to the interception of communications and the disclosure of decryption keys have profound implications for e-commerce activity.

This is part one of a two-part article for Datawatch in which I will provide an overview of the Act and examine some of the implications for business. In this first part, I will cover the background to the Act and deal with Section 1, which addresses the interception of communications. This will enable me, among other things, to summarise the impact of the interception provisions on business and examine the issue of employer monitoring of employee communications. In the second part of the article (which will be published in the next edition of Datawatch) I will move on to Section III of the Act which deals with the contentious issue of encryption key disclosure. Before concluding, I will move on to look at the extent to which the Act is likely to meet its objectives and the many ways in which it may be circumvented.

Background to RIPA

RIPA was introduced to establish a regulatory framework for the interception of communications and by doing so to protect citizens from unregulated interception. This was needed before enshrining the principles of the European Convention on Human Rights (ECHR) into UK law in the form of the Human Rights Act (HRA). The deficiencies in UK legislation in this area were highlighted when the European Court found against the Government for breaching section 8 of the ECHR in the Alison Halford case, (see my previous article 'The E-Corporation and the Law'). There was also a need for the UK to comply with the requirements of section 14 (1) of the EU Telecoms Data Protection Directive, which required changes to the UK legislative framework in this area. There can be no doubt however that the need for change has served as convenient 'hook' upon which the Government has hung sweeping powers to tap and intercept personal and commercial communications. The Government itself admits in guidance notes to the Act that it goes far further than what is strictly required to comply with the UK HRA. Given that RIPA proclaims to protect civil liberties, but in reality appears to sweep much of them away, it is inevitable that the Act would generate dissent. Interestingly enough this dissent has not been restricted to the 'usual suspects'. Concerns have been expressed by the CBI, the Institute of Directors and the British Chambers of Commerce among others.

As result of intense lobbying, during the first few readings of the Bill, the Act is far better than the original draft but attempting to summarise RIPA is a difficult task. It is a complex piece of legislation which has suffered more than most by the speed of its passage through the legislature (it was termed 'Hurricane RIPA' by a parliamentary wag at one point). RIPA is a substantial document which is supported by 10 statutory instruments designed to

provide interpretive guidance and fill gaps in the legislation. The main body of the Act is structured into 5 parts which will be implemented in a phased approach according to the timetable set out in statutory instrument 2000 No 2543 (C.71). Part II of the Act, covering surveillance and covert human intelligence, was implemented in full on 25th September 2000. Shortly afterwards on 2nd October Part 1 Chapter 1 was implemented which deals with the Interception of Communications. This was accompanied by various sections of Part IV and V dealing with the scrutiny of investigatory powers and the functions of the Intelligence Services. Section 1(13) was implemented in late October together with a number of transitional provisions and Parts 1(II) and Part III of the Act will come into force during 2001.

The Main Provisions of RIPA

Section 1: the Interception of Communications and Access to Communications Data

This establishes a new criminal offence of: *'interception of a communication in the course of its transmission via a public telecommunications system, a private telecommunications system or the postal service, without a warrant or other lawful authority'.*

The Act provides powers to the Secretary of State to serve warrants for the interception of communications following the receipt of applications from specified high-ranking officials. The list includes the Director General of the Security Services, the Chief of the Secret Intelligence Service, the Director of GCHQ, The Director General of the National Criminal Intelligence Service, the Commissioner of Customs and Excise the Chief of Defence Intelligence together with the Commissioner of the Metropolitan Police and the Chief Constables of any police force in the UK. The Secretary of State must personally authorise the application unless it is so urgent that it cannot wait, in which case a 'senior official' in the Home Office will do. Warrants can only be issued for one or more of the following reasons:

- national security
- the detection or prevention of serious crime
- the economic interests of the UK
- compliance with international obligations.

These reasons are singularly vague and open to interpretation. They are not clarified in either the Act nor the associated codes of practice and it is difficult to conceive of any circumstances which fail to fit within one or more of the categories. The Home Office has devised the codes of practice in an attempt to address many of the criticisms of the Act by industry and civil liberties groups.

The draft code of practice on Interception obliges the Secretary of State to evaluate whether the conduct specified in the warrant application is proportionate to what it seeks to achieve. In particular, he must consider whether the information could reasonably be obtained by other means. The code of practice also obliges him to consider whether the warrant could affect communications which the target of the warrant could reasonably expect would be subject to a high degree of privacy. This covers religious, medical, legal or journalistic matters. Consideration must also be given to the possible infringement of the privacy of third parties who are not the subject of the warrant. It should be noted that there is nothing within the Act or the draft codes of practice to prevent interceptions under these circumstances but applications must be more rigorous in explaining precisely why such an interception is required. These safeguards have been the subject of considerable criticism from media and civil liberties groups as they depend exclusively upon the judgement of the Secretary of State and it is believed that leaving such matters in the hands of a politician is insufficient to provide protection for such things as journalistic freedom and the privacy of sources. There could be a significant conflict of interest here in the context of any reporting which is critical of Government policy. Warrants will be valid for three months but the Secretary of State may grant renewal for additional three-month periods as required. Warrants issued on the grounds of 'national security'or 'economic well-being' are valid for six months.

The warrants apply to all Public telecommunications services including ISPs (together with public news services, WAP gateways and web site hosting companies). Fulfillment may require the recipient of the warrant to install software and hardware technologies to provide the requestor with an interception capability at source. This 'black box' proposal has provoked significant protest from the UK ISP community in particular, which is concerned at both the cost and the practicality of the proposal. In order to counter these arguments, it is proposed that the issuing of warrants will be overseen by a Technical Advisory Board, (TAB), which will advise the Secretary of State on the technical feasibility of any interception requests received and decide upon a 'fair contribution' towards any costs incurred by the recipient in complying with the warrant. There is an undertaking to ensure that the TAB is composed of industry representatives and representatives from the Interception Agencies in equal measure. The results of the consultation process on the composition of the TAB were published by the Home Office in March this year with the undertaking to set up the TAB as soon as parliamentary time permits. It is likely that this will now be delayed until after the

General Election.

This part of the Act also gives powers to officials working for public authorities (such as the police, intelligence services and revenue commissioners) to authorise the obtaining or disclosure of "communications data". This is defined as everything apart from the content of voice or data messages. The new provisions introduced by the Act make this data available without the requirement for a warrant or order to a broader class of person and for much wider purposes than the provisions regulating interception of content.

The purposes for which the communication data may be accessed include the prevention or detection of crime (as opposed to serious crime) protecting public health/safety and the assessment and collection of taxes.

Issues for Business arising from Section 1

- Part 1 applies to a 'public telecommunications systems' or a 'service provider' but these terms are not clearly defined within the Act and as such are open to interpretation by the courts. There has been considerable debate on this issue among industry groups. It could, for example, be argued that the term could include the telephone switchboard of a public company. Additionally, telecommunications services, where public access is granted to telecommunication devices such as Automated Teller Machines, could be included. If so, the Secretary of State is empowered to require the installation of an interception capability. This argument may also apply in circumstances where companies make extended transactional offerings on web sites such as branded ISP services, host bulletin boards or e-mail services. However, in reality this distinction may be academic as Section 8(1) of the Act provides the capability for warrants to be issued in respect of private telecommunication networks.

- The responsibilities of service providers in maintaining an interception capability were defined in more detail in a consultation document published on the Home Office Web Site in mid December 2000. This specifies what information an organisation issued with an interception warrant will be expected to supply. It is less informative on the technology to be deployed in order to provide the information. This could extend from the provision of an approved 'black box' supplied by a third party to the re-configuration of e-mail addresses to ensure that the relevant authorities receive blind copies as soon as they are available within an interceptee's infrastructure. The TAB will advise the Secretary of State of the technical implications of any proposal for interception and the likely costs prior to the issue of any warrant to a service provider requiring it to maintain an interception capability. It is rumored that the Government has set aside approximately £20m to fund such costs. The Act permits the Secretary of State to make a 'contribution' to the costs of any technical solution but the extent of the contribution is undefined. At this point it may be appropriate to dispel one of the more persistent myths concerning RIPA. The Act does not make it compulsory for all ISPs and telecommunication service companies to install interception capabilities. Interception capabilities can only be installed following the issue of an interception warrant. The Home Office has emphasised that such warrants will only be issued to specified ISPs subject to the specific circumstances which are defined within the Act.

- The Act makes it a criminal offences to disclose either the issue or contents of an interception warrant to anyone who is not authorised to know punishable by up to five years imprisonment and a fine or both. The draft Bill which included this provision was subject to considerable debate as, under the wording of the original Bill, a subordinate within a company who is issued with a warrant would commit a criminal offence if they communicated the receipt of the warrant to anyone else in the company including the MD. This has been modified within the code of practice which now requires that the interception warrant should specify the degree of confidentiality required. There is also a requirement for the authorities to take reasonable steps to identify in advance who may be told about the warrant in order to ensure compliance. This pre-supposes that organisations will have considered this issue and will have established an appropriate point of contact for the receipt and actioning of such warrants.

- Agencies defined within the Act as having the power to request interception warrants are required to keep records for scrutiny by an Interception Commissioner appointed by the Government.

- The dissemination of intercepted material must be limited to the minimum necessary for the authorised purpose. This will be enforced by prohibiting disclosure to those who do not hold the appropriate security clearance. Copies of the material may be made and summaries constructed but they will be covered by the arrangements governing dissemination of the original.

- There is a requirement for the 'secure storage' of intercepted material although what is deemed to constitute 'an adequate degree of security' is not defined. There is also a requirement to destroy information when it no longer needed and, if a decision has been made to retain the material, to conduct a review at 'appropriate intervals' to determine whether retention remains valid. Theoretically material could be stored indefinitely.

- Neither the possibility of interception nor the intercepted material itself may play any part in legal proceedings. However, limited disclosure is permitted to a prosecutor or a judge in order to assess what is required in the preparation of a case to secure fairness of prosecution and to assess whether there may be any exceptional legal circumstances where disclosure is necessary in the interests of justice. Both prosecutor and judge are expressly prohibited from revealing the fact of interception to third parties. At the moment, there is no requirement to disclose the information to defence lawyers.

- There are some technical concerns arising from this section of the Act which are not properly addressed either in the Act itself or the codes of practice. The capabilities of 'big brother' to 'snoop' on the general public is a highly topical matter for debate in the Internet community. One can anticipate that any hardware device installed to comply with the interception requirements of the Intelligence community will act as a 'hacker magnet' A well established hacking technique is to compromise network devices such that they act in promiscuous mode in order to sniff packets of data. Any publicity surrounding a successful 'hack' of a 'black box' could be commercially and reputationaly devastating to the business concerned. Public authorities could attempt to 'gag' the perpetrators under the disclosure provisions of the Act but Government attempts in the past to prevent the dissemination of controlled information once it has reached the public domain have scarcely been edifying. The Government has provided more details of its interception requirements in a consultation document for the section 12 of the Act. This indicates that the Government will adopt a risk management approach in judging the security of the interception system. It can only be hoped that this approach will take into account the risk of hacking and the impact upon the organisation concerned should news leak into the public domain.

- The · The provisions of Section 1 of the Act also regulate the monitoring of communications initiated and received by employees while at work. This matter raised considerable concern in the business community as the Act in its original state would have prevented the routine monitoring of employee communications unless via warrant authorised by the Secretary of State. This could have created significant problems for some organisations, particularly those in the financial services sector who record details of conversations and communications conducted by staff responsible for executing sensitive high value commercial transactions. In order to overcome these problems the Act includes provision for employees to conducted interception without a warrant for 'lawful business purposes'. These have been defined as:

- for establishing the existence of facts
- for ascertaining compliance with regulatory or self-regulatory practices or procedures
- for ascertaining or demonstrating standards which are to be achieved or ought to be achieved by persons using the system
- for preventing or detecting a crime
- for investigating or detecting unauthorised use of the businesses telecoms system
- for ensuring the effective operation of a system
- for checking whether or not communications are relevant to business
- for monitoring calls to confidential counseling helplines run free of charge.

This is a comprehensive list and would appear to clarify matters but in reality, the situation is far from clear. This issue is worth examining in more detail.

Monitoring Employee Email Usage and the Law

As stated above, RIPA enables employers to intercept and monitor employee emails (with or without their consent) for 'lawful business purposes' as defined under the Act. This power has been in place since 24th October 2000. Unfortunately, RIPA is not the only piece of legislation that has a bearing on this issue. Employers must also take account of the Data Protection Act. The Information Commissioner (previously called the Data Protection Commissioner) has issued a Draft Code of Practice on the use of personal data in employer/employee relationships. This was prepared in advance of the publication of the 'lawful business purpose' exceptions. The code is a substantial 80 page document. It does not confine itself to employee email and Internet usage but covers the use of all forms of employee related information by employers.

The draft code places restrictions on the workplace monitoring of communications thereby constraining the powers conferred under RIPA. Despite coming under pressure from the Government and the CBI, the Information Commissioner has refused to back down and is standing by the code.

According to the Commissioner, employers will face a 'two hurdle test' in monitoring staff communications. They must first ensure that such monitoring conforms to 'lawful business practice' as defined under RIPA but in addition they must take steps to ensure that they conduct such monitoring in accordance with the Data Protection Code of Practice. This requires employers:

- not to monitor the content of e-mail messages unless it is clear that the business purpose for which the monitoring is undertaken cannot be achieved by the use of a record of e-mail traffic. If the traffic record alone is not sufficient to achieve the business purpose, any further monitoring must be strictly limited and targeted (Principles 1 & 3).
- To only consider the monitoring of content if neither a record of traffic nor a record of both traffic and the subject of e-mails achieves the business purpose. In assessing whether monitoring of content is justified, employers must take account of the privacy of those sending e-mails as well as the privacy and autonomy of those receiving them. Wherever possible employers should restrict the monitoring of e-mails sent to specific employees to messages which the employee has received and chosen to retain rather than delete. Employers must not open e-mails that are clearly personal (Principles 1 & 3).
- To consider the reasons for monitoring. If monitoring the content of incoming e-mails is justified on the basis of detecting computer viruses employers must use an automated monitoring and detection process. Employers must only use information obtained for the purpose of virus detection. A need for virus detection does not warrant the reading of the content of incoming e-mails (Principles 1 & 2).
- To inform employees beforehand if it is necessary to check the mailboxes of employees in their absence. The purpose of such monitoring is to ensure the business responds properly to its customers and other contacts. Employers must only use the information for this purpose unless it reveals criminal offences or gross misconduct. (Principles 1 & 2).
- Provide a means by which employees can effectively expunge from the system e-mails they receive or send (see section 3.4) (Principles 5 & 7).

This approach means that employers could face additional costs in having to modify e-mail systems so that, unlike now, deleted messages cannot be retrieved from hard disks. The draft code generated a huge response from the consultation process and some governmental 'angst' in how to square RIPA with data protection principles. The result of this is that the final version of the code, scheduled to be published by Easter 2001, is likely to be delayed until the end of the year leaving employers and employees alike in a legal vacuum.

This is not the end of the matter as the situation for employers is confused further by the HRA which passed into law on 2 October 2000. Article 8 of the Act provides individuals with a right to respect for private and family life, home and correspondence. This right could certainly be extended to personal email use at work. It is conceivable that monitoring by employers of staff emails could be subject to legal challenge under article 8 of the HRA irrespective of the rights conveyed by RIPA or the extent of compliance with the Information Commissioner's draft code. The HRA has been termed the 'nearest thing that UK has to a written constitution' which is a reasonable description for an Act which could have far reaching implications in many areas of legislation in the UK. It is ironic that RIPA could be challenged by the very Act that contributed to its birth. The HRA has yet to be tested in the courts in connection with privacy at work and until case law is established the best advice for any employer is to tread prudently and carefully through, what shows every sign at present, of being a legal minefield.

Part II - Regulation of Surveillance and covert human intelligence sources

This section is designed to regulate the activities of the Police and the Security Services in conducting intrusive or covert surveillance operations. It has limited applicability to business and is therefore outside the scope of this article.

This concludes part one of the article. In part two I will deal with encryption key disclosures and the issues that business needs to consider in complying with this section of the Act. I will also explore some of the deficiencies in RIPA by examining the broader issue of enciphement and the opportunities presented for circumvention.

Profile of the Author

Andy has sixteen years of experience in computing, twelve of which have been spent in computer audit. His experience spans Local Government, the Health Service and an international conglomerate. For the past seven years, Andy has worked in the financial services sector and is currently an IT Audit Manager specialising in e-commerce for a major international bank.

It's July and summer has arrived, hopefully, the AGM has signified the passing of another year and I enter my third term as President of the Central Chapter. It is at this time of year that we reflect on the year that has just past, and look forward to the year ahead.

We have had another successful year, membership now stands at 141, 74 of which are CISA qualified. 21 sat the 2001 exam and are now patiently awaiting their results, so hopefully the number of CISA's will increase further. As usual we will be awarding a prize for the highest scoring Central Chapter member

This is also the time of year to thank all those who put so much effort in over the year to make the Chapter such a success. First of all I would like to publicly thank my committee for all their hard work. Particular thanks go to Lawrence Devlin, who was our founding President. Unfortunately, Lawrence has moved away from the Central area so has reluctantly resigned from the committee. So I take this opportunity to thank Lawrence for all his work and support since we formed the Chapter back in 1993 and wish him well for the future. I am also sorry to announce the resignation of Anne Robson from the committee, due to increase work demands and again my thanks go to Anne for her contribution over the past couple of years.

I also need to give my thanks for those who work so hard behind the scenes and make my job much easier. Firstly many thanks to Pat McMullen who does so much work in helping to administer the Chapter. And finally, thank you to Oli Ralph, who has done a fantastic job with the Chapter's web site.

Having reflected on the past, now let's look forward to the future. The Committee is presently discussing the strategic direction for the Chapter, particularly looking at the events schedule for the next 12 months. Whilst membership numbers are healthy, it would be good to see a few more faces at Chapter meetings. With this in mind, we would be interested to hear the type of events you, the membership would support. Therefore, I would be grateful if you would drop me an email at the following address: Mike.Hughes@kpmg.co.uk with any thoughts you may have. These could be on topics for evening meetings, names of good speakers you have heard at other events, topics for day events, would you be interested in the Chapter organising training courses on specific subjects or workshops covering specific technical areas. Please take this opportunity to influence the events that the Chapter organises on your behalf. I am also interested in hearing any ideas for the future development of our web site. If you haven't visited the site yet, then you can find it at www.isaca.org.uk/central.

One interesting development I am looking into is a possible link up with the Business School of The Nottingham Trent University. They are looking to promote a new degree course focussing on Accounting and Information Systems and are looking to the Central chapter to help with the information systems governance aspects of the course. Watch this space for further developments.

Well I hope you all enjoy your summer holidays, and return to work nicely refreshed and ready for the challenges a-head. I am looking forward to being inundated with emails with all your views for future events and I will publish the results in the next edition of Datawatch in the Autumn.

Mike Hughes, Central Chapter President, presenting Pat McMullen with a small token of appreciation for all her hard work on behalf of the Chapter.

ARE YOUR ORGANISATION'S SECURITY POLICIES BEING ENFORCED?

Karen Nelson

Windows 2000 takes a giant leap forward in providing security controls through policy. "Group policies are the primary method for enabling centralised administration of users and computers within Windows 2000," according to Information Security Forum (ISF)[1]. More than 1,500 options can be set using Windows 2000 Group Policy. In Windows NT 4.0 Administrators use User Profiles and System Policies to centralise control over user preferences and computer configuration in order to reduce the number of support staff ' trips to the desktop.' In security-aware shops these controls also provide enhanced security, largely by restricting user access to specific applications and system tools.

NT 4 used separate utilities for managing audit policies, user rights, password and account lockout policies. Windows 2000 consolidates these tools in its Group Policy management console[2]. The extensions available through a Windows 2000 domain make implementing security policy much easier (after an initial learning curve). Other security tools can be loaded into the same management console as the Group Policy Snap-In editor, making it easier to centralise control and delegate limited responsibilities.

In addition to centralising and extending the availability of security configuration options, Windows 2000 revises the ways policy information is stored in the registry. NT 4.0 policies are considered insecure because the registry keys that contain the policy information by default can be viewed and edited by Everyone. Also, Policies although revised at the server, may persist in the registry. In brief, the Windows NT 4.0 entries are hard to clean. Windows 2000 consolidates the registry keys that contain policy information and by default restricts modification to Administrators. The Windows 2000 registry entries change when Group Policy changes, making it easier to "clean" the registry.

Organisations replacing current desktop and laptops with Windows 2000 Professional can run Windows NT 4.0 PDC's, and still implement NT 4.0 System Policies for domain access and Windows 2000 local computer policies, for local use. A more detailed explanation of Profile settings is included as Appendix A.

Considering the importance of Policy in securing Windows 2000 and NT systems, as a professional auditor it is more important than ever to become familiar with the options available for securing end user computers through policies. This article discusses Profiles and Policies available in NT 4.0 and Windows 2000.

Audit procedures for reviewing the use of Profiles and Policies should address the following items:

1. Policy administration and management
   - Authorisations to create and modify policy and profile entries in files and in the registry,
   - Ability to assign policy to appropriate users and groups,
   - Ability to apply and utilise policy,
   - Ability to read policy,
   - Ability to replicate and distribute policy in accordance with requirements
2. Policy content
   - Does it provide access and permissions according to the principle of least privilege?
   - Does it enforce management's intended security policy based on business requirements, regulatory and contractual obligations, and assessed risks?

Windows 2000 includes a Security Configuration Toolkit utility that is loaded through a Microsoft Management Console (MMC). This utility can be used to configure a security template that includes many of the Group Policy settings. The toolkit contains an analysis tool that can be used to prepare a baseline security configuration that can be used to compare the present and future security configuration settings against a baseline setting. This can be a useful tool for auditors when examining current settings as well as changes to policies.

PROFILES

Both Windows NT 4.0 and 2000 use three types of profiles: local, roaming and mandatory. The profile location is specified in User Manager for Domains, Profile path entry in NT 4.0 and in the Local Users and Group Snap-in or Active Directory Users and Group account properties for Windows 2000. The profile path should be separate from the Home Directory path to avoid copying user private files across the network at logon.

The Administrator may create a mandatory user profile that cannot be modified, a network or local default profile that applies to all new users on Windows NT 4.0 computers and which can be modified by the user.

Key Definitions[3]:

Local Profile

A local profile is specific to a computer. A user who has a local profile on a particular computer can gain access to that profile only while logged on to that computer. Changes are saved to the local ached profile.

Mandatory Profile

A mandatory profile is a pre-configured roaming profile that the user cannot change. In most cases, these are assigned to a person or a group of people for whom a common interface and standard configuration is required.

Roaming Profile

A roaming profile is stored on a network share and can be accessed from any computer. A user who has a roaming

profile can log on to any computer for which that profile is valid and access the profile. (Note that a profile is only valid on the platform for which it was created-for example, a Windows NT 4.0 profile cannot be used on a Windows 95 computer.) User changes are saved to the server profile.

Roaming User

A roaming user is a user who logs on to the network from different computers at different times. This type of user may use a kiosk or may share a bank of computers with other users. A roaming user stores his or her user profile on a network share, and can log on to any networked computer and access that profile.

Profiles are stored on a shared directory of the network server or cached locally. At logon the system loads a set of registry entries in the HKEY_CURRENT_USER (HKCU) portion of the hive from the NTUSER.dat[4] file. The registry portion of the profile stores settings that maintain network connections, Control Panel configurations unique to the user (such as the desktop color and mouse), and application-specific settings. The directory portion of the profile stores shortcut links, desktop icons, start-up applications, and so forth.

Users can be denied access at logon if permissions on the Profile directory are incorrect. For Mandatory profiles, the user must have READ and for Roaming profiles the user should have Change, but with Delete permission removed. In addition an administrator can force the use of server-based mandatory profiles.

POLICY ADMINISTRATION

The NT 4.0 Server System Policy controls the user work environment and actions and enforces system configuration settings. NT 4.0 System policies, stored in the file Ntconfig.Pol, overwrite registry entries in HKEY_CURRENT_MACHINE (HKCM) and HKCU after the user has logged in and profiles have been loaded and before the user gains control of the desktop. It is critically important that replication of the NTConfig.pol file to the NETLOGON directory of the authenticating Domain Controller takes place. When local profiles are being used, the directory containing the NTConfig.pol file must be secured and the user must have Read.

The policies can be applied at the user or group level of the domain. User specific settings are applied first, and group settings discarded. If no user specific settings exist, user defaults will be applied; if user defaults do not exist, group settings will be applied.

The Windows 2000 Group Policy is not the same as the Windows NT®4.0 System Policy and the administrative policies are stored in separate registry keys. Additional functionality available in the Windows 2000 Group Policy includes policy settings for scripts, software installation, security settings, Internet Explorer maintenance, folder redirection, and Remote Installation Services. Windows NT®4.0 policy is only associated with the domain where the computer and user are registered. The Windows 2000 Group Policy can be associated to a local computer, site, domains, and organisational units, however in order to utilise all features, both workstations and DC should run Windows 2000. Within organisational units various settings can be filtered by security groups for improved discretionary access control. By default Windows 2000 automatically creates three policies, applied as outlined in Table 1.

Table 1 Default application of Group Policies (Windows 2000)[5]

Computer Type	Domain Group Policies	Domain Controller Group Policies	Domain Local Group Policies
Domain Controller	Yes	Yes	Yes
Server within domain, not a DC	Yes	No	Yes
Stand-alone Server	No	No	Yes
Any workstation	No	No	Yes

Once installed the policies have to be configured to meet organisation requirements. High-level Group Policies can overwrite low level policies. In addition Windows 2000 offers the ability to block, allow or force inheritance of policies from a parent object to child objects. Administration of Group policies at each level can be delegated to security administrators or specific users.

If implementing Windows Professional desktops in NT 4.0 domains, while anticipating migration to Windows 2000 Domain Controllers, the additional Group Policy options can be applied at the desktop only as Local Computer Policy. If either the user and/or computer account are in a Windows NT 4.0 domain, the Windows 2000 Professional client will process the NT 4.0 System policy. Later, Group policies managed from the Windows 2000 domain controller can overwrite the local policy. Because of the persistent nature of NT.40 based registry changes in some cases the Professional desktop may have to be reinstalled.

Permissions Required to Administer Windows 2000 Group Policy

To make use of all of its features, Windows 2000 Group Policy requires Active Directory and Windows 2000 clients. "To set Group Policy for a selected Active Directory container, you must have a Windows 2000 domain controller installed, and you must have Read and Write permission to access the system volume of domain controllers (Sysvol folder) and modify rights to the currently selected directory container."[6] Group policy expands to include not only critical registry settings, but also, options for security settings, software installation, scripts, folder redirection, Remote Installation Services, and Internet Explorer maintenance. By default a Group Policy object (GPO) applies to all users contained in the linked site, domain or organizational unit. However, the Access Control Entries (ACE) on the GPO can be changed to exclude or include any members of a Windows 2000 security group.

The root node of the Group Policy identifies its

namespace in the following format: *GPO Name [DomainName.com] Policy.*

The GPO policy settings are stored in two locations: the Group Policy Container of the Active Directory and the Group Policy Template folder of SYSVOL, containing the various policy files. The template folder contains three *.adm files, System.adm, Inetres.adm, and Conf.adm, which enumerate all the settings initially displayed in the Administrative Templates node, as well as Winnt.adm and Common.adm for use with the NT 4.0 System Policy. GPO's are identified by a globally unique identifier (GUID) stored at the domain level.

In Windows 2000, the preferred registry keys and values for policies are set in either the \Software\Policies (the preferred location for all new policies) or \Software\Microsoft\Windows\CurrentVersion\Policies trees, in either HKCU or HKLM. Policies set outside these locations, such as those set with NT 4.0, are known as preferences, and may require manual editing of the registry

POLICY CONTENT

The Appendixes B and C in the article include detailed lists of security configuration options available through the NT 4.0 system policy and through Windows 2000 Domain Controller Group Policies. Figure 1 displays the Windows 2000 Domain Controller Group Policy nodes that can be configured.

In NT 4.0 System Policy includes items such as preventing access to the Run Start menu to prevent users from running their own applications in the NT command line shell, removing key utilities that could be used to gain information for exploiting the system, such as find, cmd, nbtstat, netstat, ping and others. Windows 2000 policy can be used to enforce password policies, account lockout, Kerberos policy when strong authentication is required in a native environment, and audit policies. If the encrypted file system (EFS) is to be used, ensure that a Encrypted Data Recovery agent policy has been set in the Public Key Policy. The EFS cannot be used in conjunction with offline, synchronised, or shared folders. User configuration settings can be used to relocate user data in Application Data, Desktop, My Documents and Start Menu folders to server-based directories. This will ensure that end-user data is backed up. Disk quotas should be utilised to restrict the space available on the server to each user.

The Windows 2000 Policy allows the configuration of Restricted Groups policy, which limit who can be a member of a group. For example, Ted and Alice maybe defined as the only accounts permitted to be members of Enterprise Administrators group. Any attempts to add another user account would be prevented.

The Registry policy maybe used to configure access control, audit, and ownership permissions on specific Registry keys and the File System policy maybe used to configure access control, audit, and ownership on specific files. The Administrator adds the Registry keys and files and assigns permissions.

When moving to Windows 2000 the implementation of the Domain architecture and Group Policies requires tedious planning. The Policy structure should be simple enough to maintain and robust enough to provide for various levels of security required throughout the organization.

footnotes:

1. Windows 2000 Security Checklist, Version 2, Information Security Forum (ISF).
2. The management console can be customised to meet requirements. Management of security and Group policy can be delegated to security staff or end-user administrative managers
3. Windows NT 4.0 Profiles and Policies, Microsoft. P3-4'.
4. For Mandatory Profiles, the file extension change to Ntuser.man.
5. Windows 2000 Security Checklist, Version2, Information Security Forum.
6. Microsoft Windows 2000 Group Policy White Paper, Microsoft, p.6.

Appendix A. Summary of Profile Settings

Configuration Preferences Stored in the Registry Hive

The NTuser.dat file contains the following configuration settings.

- *Windows NT Explorer settings.* All user-definable settings for Windows NT Explorer as well as persistent network connections.
- *Taskbar*. All personal program groups and their properties, all program items and their properties and all taskbar settings.
- *Printer settings.* All network printer connections.
- *Control Panel*. All user-defined settings made in the Control Panel.
- *Accessories*. All user-specific applicaiton settings affecting the Windows NT environment, including: Calculator, Clock, Notepad, Paint and HyperTerminal, among others.
- *Help bookmarks*. Any bookmarks placed in the Windows NT Help system.

Configuration Preferences Stored in Profile Directories

The profile directories are designed to contain the following configuration settings.

- *Application data.* Application-specific data, such as a custom dictionary for a word processing program. Application vendors decide what data to store in this directory.
- *Desktop.* Desktop items, including files and shortcuts.
- *Favorites*. Shortcuts to program items and favorite locations.
- *NetHood**. Short cuts to Network Neighbourhood items.
- *Personal*. Shortcuts to program items. Also a central store for any documents that the user creates. Applications should be written to save files here by default.
- *PrintHood*.* Shortcuts to printer folder items.
- *SendTo*. Shortcuts to document storage locations and applications.
- Start Menu. Shortcuts to program items.
- Templates.* Shortcuts to template items.

* These directories are hidden by default. To see these directories, change the View Options

Table E.2 Windows 2000 Profile Settings*

Folder Name	Description	Roams with Profile	Redirectable with Group Policy
Application Data	per-user roaming application data	Yes	Yes
Cookies	User's Internet Explorer cookies	Yes	Yes
Desktop		Yes	Yes
Favorites	User's Internet Explorer Favorites	Yes	No
Local Settings	Temporary files and per-user non-roaming application data	No	No
My Documents	User's Documents	Yes	Yes
NetHood		Yes	No
PrintHood		Yes	No
Recent	Shortcuts to recently used documents	Yes	No
Send To		Yes	No
Start menu	User's personal start menu	Yes	Yes
Templates	Per-user customised templates	Yes	No

*'Step by Step Guide to User Data & Settings,' Microsoft

Appendix B - NT 4.0 Policy Editor

Two nodes make up the NT 4.0 System Policy Editor: Computer and User. The table below lists the major branches and options available under each of these two nodes, starting with "Default Computer". To select desired objects, enter a check mark in the checkbox; to deselect remove the check mark.

Default Computer	Options
Network Node - System Polices - Remote Update	Update mode: Automatic (use default path) Display error messages, Load balancing
System	Items to run at start-up (select from list)
Default Computer - Windows NT Network -Sharing	Create hidden drive shares (Workstation or Server)
Default Computer - Windows NT Printer	Disable browser thread on this computer. Scheduler priority. Beep for error enabled
Windows NT - Remote Access	Maximum number of unsuccessful logon attempts Max time limit for authentication Wait interval for call-back AutoDisconnect
Windows NT Shell Custom Shared folders (Program, desktop, Start menu, Start-up)	
Windows NT System Logon	Logon Logon Banner Enable shutdown from authenticated logon Do not display last logged on user name Run logon scripts synchronously
Windows NT System File System	File System Do not create 8.3 file names Allow extended characters in 8.3 filename Do not update last time access
Windows NT - User Profile	Delete cached copies of roaming profiles Slow network connection timeout Slow network default profile Choose profile default operations Timeout for dialog boxes
Default User	
Control Panel - Display	Restrict display
Desktop	Wallpaper - specify location & name Colour Scheme - name
Shell - Restrictions	Remove Run command from Start menu Remove folders from Settings on Start Menu Remove taskbar from Settings on Start Menu

Appendix B Continued on page 16

...Appendix B continued from page 15

	Remove Find command from Start Menu Hide Drives in My Computer Hide Network Neighbourhood No Entire Network in Network Neighbourhood No workgroup contents in Network Neighborhood Hide all items on desktop Remove Shut Down command from Start Menu Don't save settings at exit
System - Restrictions	Disable Registry editing tools. Run only allowed Windows applications
Windows NT Shell	Custom user interface - Custom shell - Name
Windows NT Shell	Custom Folders Custom programs folders Custom desktop icons Hide Start menu subfolders Custom Start-up folder Custom Network Neighbourhood Custom Start menu
Windows NT Shell	Restrictions Only use approved shell extensions Remove Views - Options menu from Explorer Remove Tools - Go To menu from Explorer Remove File menu from Explorer Remove common program groups from Start up Menu Disable context menus for the task bar Disable Explorer's default context menu Remove the "Map Network Drive" and "Disconnect Network Drive" options Disable link file tracing Remove NT Security item from Start menu Remove Disconnect item from Start Menu Prevent user from changing file type associations
Windows NT System	Parse autoexec.bat Run logon scripts synchronously Disable logoff Disable Task Manager Disable Lock Workstation Disable Change Password Show Welcome tips at logon
Windows NT User Profiles	Limit profile size Exclude directories in roaming profile.

We are aware that some members might have missed out on our monthly Chapter presentations as the Mailshot did not reach them on time. In future we will be sending you an email with a link so you can find an electronic version of the Mailshot. Unfortunately, not all our members have provided accurate or up-to-date contact details. There are a surprising number of missing or incorrect email addresses, phone numbers and employers names. You can easily change contact details by logging in to the ISACA.ORG membership area - you should have received a password from the States. Don't forget to check out K-NET in the members only area formerly Global Information Repository (GIR) "that satisfies the need for professional IS audit, control, security and governance information."

On the subject of monthly Chapter presentations, some of you might have noticed that there is an on-line poll at the isaca-london.org website to help determine whether the current start-time of 16:30 is acceptable to all our members. So far, only 33 of you have responded, and the majority (27%) have shown a preference for sticking to the current start-time. I don't think 33 responses out of a potential nearly 700 are statistically significant, so if you have a preference either way, please respond to the poll at *http://vote.pollit.com/webpoll2?ID=380932*.

With regard to Research, there are a number of projects underway. These are just some the projects underway and you can look forward to their publication in due time with availability at the ISACA Bookstore.:

- **E-commerce-Public Key Infrastructure (Good Practices for Secure Communications)**
- **Virtual Private Network-New Issues for Network Security**
- **Electronic/Digital Signature Legislation Project**
- **Wireless Communication Project**
- **Enterprise Information Integrity Project**

Please contact KAMAL KHAN, for further information.

Appendix C - Windows 2000 Group Policy for Domain Controllers

These security settings are typically domain-wide. Domain controllers ignore password, lockout or Kereberos policies defined at an OU or LGPO level.

Policy	Default Value	Comment
Password Policy		
Enforce password policy	1 password remembered	
Maximum password age	42 days	
Minimum password age	0 days	
Passwords must meet complexity requirements	Disabled	
Store password using reversible encryption for	Disabled	
All users in the domain		
Account Lockout Policy		
Account Lockout Threshold	0	
Kerebros Policy		
Since Kereberos support was not available in previous versions of Windows NT, the following Kerebros policies are always defined for the first domain controller of a Windows 2000 domain, regardless of whether it was upgraded or not.		
Enforce user logon restrictions	Enabled	
Maximum lifetime that a user ticket can be	7 days	
renewed.		
Maximum user ticket lifetime	10 hours	
Maximum service ticket lifetime	60 minutes	
Maximum tolerance for synchronization of computer clocks	5 minutes	
Security Options		
Automatically logoff users when logon time expires	Disabled	This is a domain-wide setting even though it appears under the Security Options area.

Appendix C - Computer - Default Domain Policy: Digital Signatures, Audit Policy, User Rights

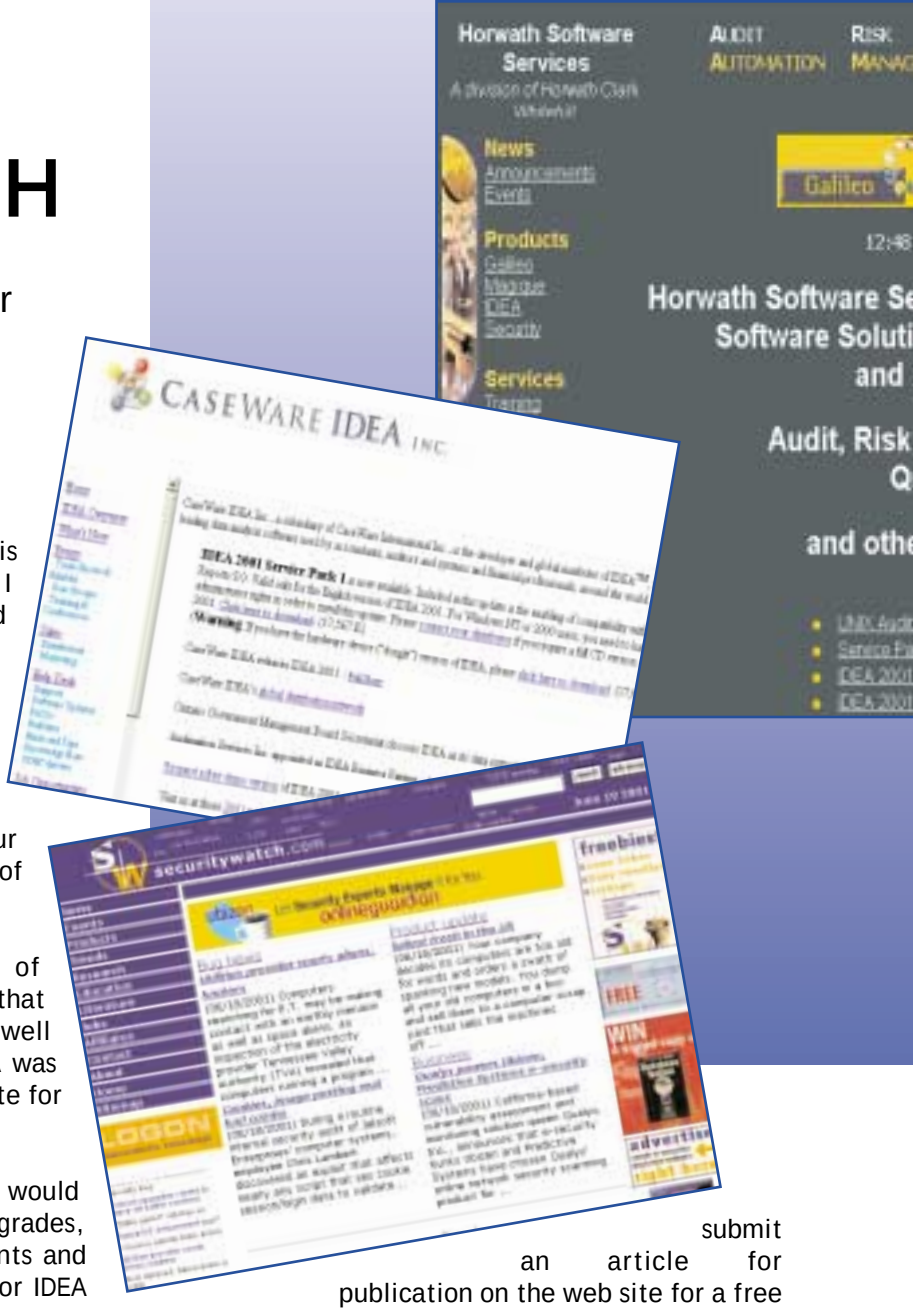
Policy	Default Value	Comment
Security Options		
Digitally sign server-side communications when possible	Enabled	
Audit Policy		
Audit Account Logon events	No Auditing	
Audit Account Management	No Auditing	
Audit Directory Service Access	No Auditing	
Audit Log on Events	No Auditing	
Audit Object Access	No Auditing	
Audit Policy Change	No Auditing	
Audit Privilege Use	No Auditing	
Audit Process Tracking	No Auditing	
Audit System Events	No Auditing	
User Rights Policy		
Access this computer from the network	Administrators Authenticated Users, Everyone	If the following groups were given this right prior to running DC Promo then they are removed: Backup Operators, Guests and Users If a Windows NT 4.0 domain controller is upgraded as the first Windows 2000 domain controller using a slipstreamed setup of Windows 2000 + Service Pack 1, then the Authenticated Users group is automatically given this right.
Act as part of the operating system		
Add workstations to the domain	Authenticated Users	This User Right is for the support of legacy APIs. You can also allow users to create computer accounts by using this User Right. Authenticated Users can only create 10 computer accounts using this User Right.
Back up files and directories	Administrators, Backup Operators, Server Operators.	
Bypass traverse checking	Administrators, Authenticated Users, Everyone.	If the following groups were given this right prior to running DCPromo, then they are removed: Backup Operators, Users.
Change the system time	Administrators,	
	Server Operators	
Create a pagefile	Administrators	
Create a token object		
Create a permanent shared object		
Debug programs	Administrators	
Force shutdown from a remote system	Administrators, Server Operators	
Generate Security Audits		
Increase quotas	Administrators	
Increase scheduling priority	Administrators	
Load and unload device drivers	Administrators	
Lock pages in memory		
Log on as a batch job		
Log on as a service		
Log on locally	Account Operators, Administrators, Backup Operators Server Operators Print Operators	If the following groups were given this right prior to running DCPromo, then they are removed: Authenticated Users, Guests, Guest, Users and Everyone.
Manage auditng and security log	Administrators	
Modify firmware environment variables	Administrators	
Profile single process	Administrators	
Profile system performance	Administrators	
Replace a process-level token		
Restore files and directories	Administrators, Backup Operators, Server Operators	
Shut down the system	Account Operators Administrators, Backup Operators, Server Operators Print Operators	If the following groups were given this right prior to running DCPromo, then they are removed: Authenticated Users, Guests, Guest, Users and Everyone
Take ownership of files or other	Administrators	
objects		
Deny Logon locally		
Deny logon as a service		
Deny access to this computer from network		
Remove computer from docking station	Administrators	If the following groups were given this right prior to running DCPromo, then they are removed: Users
Synchronize directory service data		
Enable computer and user accounts to be trusted for delegation.	Administrators	If the following groups were given this right prior to running DCPromo, then they are removed: Users

Appendix C - Computer - Local Policies Security Options for Domain Controllers

Additional restrictions for anonymous connections	Do not allow enumeration of SAM accounts and shares
Amount of idle time required before disconnecting the session	120 minutes
Audit the access of global system objects	Enabled
Audit use of Backup and Restore Procedures	Enabled
Automatically logoff users when logon time expires	Enabled
Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign client communications (when possible)	Disabled
Disable CTRL+ALT+DEL requirement for logon	Disabled
Do not display last user name in logon screen	Enabled
LAN Manager Authentication Level	Send NTLM v2 response only/refuse LM & NTLM
Message text for users attempting to logon	
Message title for users attempting to logon	
Number of previous logons to cache (in case domain controller not available	
Prevent system maintenance of computer account password	Enabled
Prompt user to change password before expiration	Begin prompting this many days before password expires: 14 days
Recovery Console: Allow automatic administrative logon	Define this policy setting in the template: Enabled
Recovery Console: Allow floppy copy and access to all drives and folders	Define this policy setting in the template: Disabled
Rename administrator account	
Rename guest account	
Restrict CD-ROM access to locally logged on user only	Enabled
Restrict floppy access to locally logged on user only	Enabled
Secure channel: Digitally encrypt secure channel (when possible)	Enabled
Secure channel: Require strong (Windows 2000 or better) session key	Enabled
Send unencrypted password to connect to idle third party SMS server	Disabled
Shutdown system immediately if unable to log security audits	Disabled
Smart card removal behaviour	Force logoff: lock workstation
Strengthen default permissions of global system objects (e.g.) symbolic links	Enabled
Unsigned driver installation	Do not allow: Warn but allow installation: Silently Succeed.

NETWATCH

ANNABEL LANE takes us on another trawl through cyberspace.
The Internet Resource List is on page 32



When I started writing this column, I must confess that I wondered how long I would be able to continue to find sites to write about, especially as a lot of very relevant sites had already been reported on by my predecessor. However I reckoned without the vast resources of the net, the ever expanding areas most of us cover in our day to day jobs, and also the feedback of members.

I am indebted to Trevor Williams of Howarth Software Services for pointing out that the url the resource list gives for IDEA (that well known audit software) has changed as IDEA was taken over by Caseware last year. The new site for all you IDEA enthusiasts is now at caseware: **www.caseware-idea.com**.

This has all the sort of information you would expect: shows and events, notices of new upgrades, and a Help Desk section containing some hints and tips, FAQs and bulletins. A useful resource for IDEA users and I know there are quite a few out there.

www.horwathsoftware.co.uk

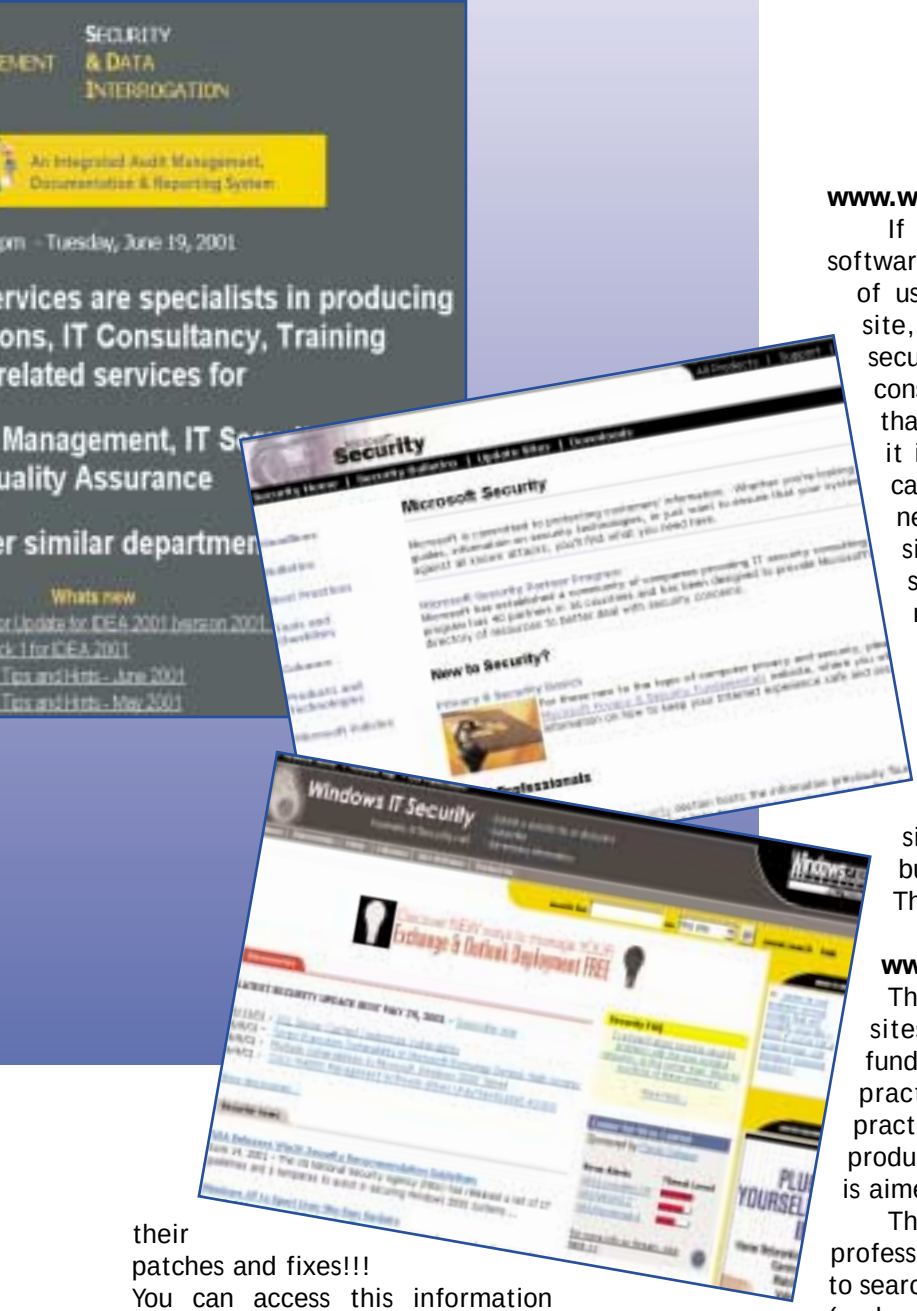
Horwath software have their own site. The emphasis is on their commercial activities but there is also some information on auditing NT and other information such as more IDEA tips and hints.

And now let's turn our attention to something we haven't addressed specifically in this column for some time - security from the point of view of hackers. It's always interesting and keeping up with what the hacking fraternity are up to is a constant and unequal struggle. But those of us responsible for the security side of things or conducting reviews of specific systems for which we want to know the latest exploits could do worse than visit: www.freshmeat.net

There is a great deal of information on here which is quite technical and probably at a lower level than most of us will generally need to know about. (Well, I didn't understand it anyway, I'll confess!). But there are also some interesting articles in the Editorial section - you too could submit an article for publication on the web site for a free T shirt and 15 minutes of fame! When I last visited there was an interesting one on "Egoless Admin" for support staff, an article reviewing the way software development projects are undertaken, and some one's opinion on how the use of open source software should be restricted. But the main thrust of the site is the new scripts and viruses that are being created and released for hackers to use. There's an archive which lists new additions each day - check it out and feel sobered at the amount of malicious activity we and our company networks are up against!

www.securitywatch.com

In a similar vein though less technical is this site which draws together quite a range of information on exploits and security breaches. For example, you can scan down the latest news to an item regarding a system you are running - such as Microsoft SQL server 7.0. Clicking on the text will take you to a description of the problem and what can be done about it, and there's also a link through to the Microsoft site where you can obtain the necessary patch. There's no excuse now for your network administrators not to be up to date with



their
patches and fixes!!!
You can access this information through the news section or a lightning search called, interestingly "Headlinivore". I also particularly like the education system which starts with a list of the basic security problems, at the level of authentication, availability, etc and goes on after telling you what percentage of companies don't take adequate action on these to a list of FAQs. Some examples I thought were useful are:

· What is SSL? Is SSL good enough?
· What is a PKI?
· Do I need application layer security?

The answers are short, and punchy. Could be useful for converting the recalcitrant auditee. And we all meet a few of those.
There's also a section on products like firewalls and VPNs. Following this link takes you to a brief review of what different companies have to offer and what their products do. Again, useful stuff. I would recommend this site as having a wide range of information, pitched at a level that suits those who are less technical but need to grasp more than a basic understanding.

www.windowsitsecurity.com

If Bill Gates's monopolistic domination of the software market is true, then there are a great many of us out there using Microsoft products. This site, as its name suggests, specialises in Windows security. On the front page the first category consists of the latest vulnerabilities and exploits that have been found in Microsoft products and it is possible to subscribe to these so that you can be alerted to them. There's also security news and columns from writers. As this is the site of Windows 2000 Magazine, you can search back issues of this too and there's a method of searching on topics for back articles. There are also discussion groups to join in on subjects such as Windows 2000 security, Security "how to" and Ecommerce security. There are other security resources too, such as a link through to the System Administrator site which is very similar in appearance and layout to this one but slanted towards System Administration. The Microsoft security site is also linked.

www.microsoft.com/security

This site basically links you to other Microsoft sites, such as the Microsoft security and fundamentals website. This includes a best practices security checklist which advises practices such as using strong passwords, antivirus products, and backing up early and often. This one is aimed more at the personal user.

The Microsoft Technet site is aimed at IT professionals and is more technical with the facility to search security bulletins; hot topics and headlines (such as "New Boot Patches now available!"). A useful resource for finding information on Microsoft products is the "How it works" section. You can use this to check out the implications of new products, or ascertain their suitability to resolve audit issues. For example there are articles on how PKI and cryptography work in Windows, Windows 2000 security features, and how Kerberos, the user authentication within Windows 2000 works. There are also articles which are released monthly and each time take up a different topic - the archive for those is on this site too.

There's also a link for developers, but that is probably not of as much interest to us.

This edition's trawl through cyberspace seems to have ended up at destination Microsoft, so I apologise to those of you who aren't Microsoft users. Never mind, here's some late breaking news on the foot and mouth outbreak - it seems to have spread to Japan: some nibbled beds were found in Tokyo and they think it is a case of futon mouse….!

Back to Basics

Security Policy

We spend so much time on e-Business these days that it is easy to forget that other things are also important in the world of security. BRIAN SHORTEN tells us why a security policy is the first step in a co-ordinated security process.

This article is a personal view, from someone who has written policies, on why you should have a policy and what it should cover. The last section covers how you start to write a policy.

Why have a policy?

The security policy is the foundation to all your security. A formal security policy, signed by the CEO, defines how the company intends to handle security and says the company is not only concerned about security, but takes it seriously.

You will note I say 'signed by the CEO' - this is an important part of the overall process. It is vital that staff can see that there is Management buy-in right from the top.

While signoff from the Security Manager or Director is good, it just doesn't convey the same message. After all, as some staff see it, the Security Manager/Director is expected, and paid, to care about security

So, what meaning does the policy put into words? The policy tells staff what they CAN do, what they CANNOT do, what they MUST do, and what their RESPONSIBILITIES are towards IT security.

What should it cover?

Many books state that the policy should be short, with some authors saying the policy should only cover one side of an A4 sheet. Some even give examples, which you can modify for your own company. While I agree that a short document has more chance of being read by its intended audience, most of these samples are basically mission statements, which must still be supported by a policy.

I would suggest that the mission statement be used as a personal foreword, signed by the CEO, to the policy.

The policy says WHY things must be done. The next layer down is the processes/procedures and standards, which say HOW things are to be done.

For example:

Policy Says	Procedure Says
All applications must have a password	Create a procedure for each application Each procedure should detail exactly how the password, for that application, is to be created and maintained
All new applications, purchased or developed, must be approved by security prior to purchase.	A document must be available to show what levels of security new applications must reach. This must be written to cover all the platforms on which applications may run.
All servers must be configured to the company standard	A guideline should exist to give full details of how NT and Unix servers must be configured. Because of the detail to which these documents must be written, they must not be freely available, but only issued as required.

The bulk of the security policy should include high-level sections on:

Suggested Heading	Sample Contents
Access Control Standards	A discretionary access policy will be implemented to provide users with access to all information, which is needed to perform their job functions and no more
Accountability	Users will be held accountable for all actions carried out under their user login.
Audit Trails	The systems will record a minimum of 30 days user sign-on and sign-off details for use by systems security whenever deemed necessary.
Backups	All software and user data will be backed up to an alternative media on a regular basis and kept in a secure area. The frequency of the back-ups shall be appropriate to the importance of the system and the data, which would need to be recovered in the event of a failure.
Business Continuity	All appropriate computer serves should have a contingency plan designed implemented and tested.
Disposal of Hardware and Media	Hardware, such as disc drives, floppy discs, CDs and other storage facilities must be destroyed in a business manner. The manner of such destruction must be agreed to by Systems Security.
Disposal of printed matter	Each department should have provision for the destruction of printed confidential matter.
Downloading from the Internet	The rules under which members of staff are given access to the internet: ◆ Business use only ◆ Unsuitable downloads (with definitions)
Information Ownership	All prime groups of information shall have a designated 'owner' who will decide to whom, and under what circumstances, the information is available.
Management Responsibilities	It is the responsibility of all levels of management to ensure: ◆ All employees under their direct supervision (permanent, temporary and contractors) are aware of the company's security policies. ◆ All visitors that are permitted to use company MIS facilities are aware of the company's Information Security Policy. Each person holding a management or supervisory position is responsible for noting and reporting any deviations from this policy.
Modems and Analogue Lines	The installation of analogue lines for **any** is prohibited unless prior authorisation is given after the requestor has provided full justification. Active modems must not be connected to network machines.
Off-site Repairs to Equpiment	Should it become necessary for faulty equipment to be sent off-site for repairs, Systems Security must be contacted on each occasion for advice on security of the equpment/data whilst off site.
Physical Security	Physical access security measures are required to protect against the threats of loss and damage to the computing based equipment and information: ◆ All assets and materials are required to be protected from unauthorised use or removal, or damage whether accidental or deliberate. ◆ The Physical Security Policy of the company is to ensrue that the Management Informaton Systems, their peripherals, removable storage media, electrical services and communications services are protected from unauthorised access and from damage as far as possible, consistent with a cost-efficient operation.
Portable Devices	◆ Laptop computers and other portable devices are the responsibility of the person to whom the equpment is allocated (permanently or temporarily). The security of any information downloaded to such devices is also the responsibility of the person to whom the equipment is allocated (permanently or temporarily). ◆ Users must be aware that laptop computers and Personal Digital Assistants (electronic diaries such as PalmPilots, Psion organisers etc), are extremely vulnerable to theft as they have a high value and are easily portable. ◆ Care must be taken when travelling that they are not left unattended in public areas, and when left in cars, houses or hotel rooms etc, all possible measure to ensure their security have been taken.
Staff Responsibilities	The protection of the company's information assets is a fundamental employee responsibility. Each member of staff is required to: ◆ understand and comply with the security policies; know and follow instructions for controlling the access to, and use of, company computer equipment; know and follow instructions governing the secre handling of our invformation assets; ensure their password is kept secret. It must never be given to anyone; be aware that it is expressly forbidden to: install, execute, download, upload or in any other way introduce third party software onto computer equipment; abuse any special account privileges that may have been granted. Each employee is responsible for noting and reporting any deviations from this policy.
Use of Email	The rules under which members of staff are given access to email. ◆ Business user only. ◆ Use for employees only. ◆ Unsuitable attachments (with definitions)
Viruses	◆ Any data files which come into the company must be virus checked before being loaded to the data network. ◆ Any questions regarding virus checking should be directed to Help Desk. ◆ If a virus is detected it should be reported immediately to the Help Desk.
Workstation Security	A workstation, which has not received any input or generated any CPU activity for a period of time, ie 60 minutes, will be automatically logged off from the network.

Other sections to be included in the policy should be:

Privacy:

Whilst most companies do not have the resources, or reason, to monitor emails on a regular basis, there will be occasions when it will be necessary to check the email of a member of staff. To prepare for that occasion the policy should spell out the companies stance on privacy. For example:

> *No employee or user of the company mail system(s) should have any expectation of privacy with respect to any electronic mail sent or received. The company may, at any time without prior notification, monitor, review, audit or control any aspect of the mail systems, including individual accounts. This process has internal control processes and is subject to audit.*

Staff will then be aware that the facility to monitor email exists, but that checks and balances bind it.

Non-compliance:

Having covered what you expect of staff, you should also include the consequences of non-compliance. A note similar to *non-compliance may result in disciplinary action* should suffice. Note I say 'may' which allows leeway; 'Will' doesn't say the same thing.

Legislation:

As more and more companies operate on a global basis, it is important to make reference to all relevant legislation. This should not be restricted to UK legislation, but should also include the relevant legislation for every location where the company has staff who are expected to comply with the policy. If your company has offices across the world make this a separate appendix.

Other issues:

As an aid to users, you could also include separate appendices of advice on choosing secure passwords, and the usual Do's and Don'ts of good security practice.

Do remember that your security policy is an umbrella document that forms the basis of separate security standards and baselines, which can be application specific. You should therefore beware of trying to make the policy too specific. Specifying 'must have a password which meets current standards' is better than stating the exact size, format and make-up of the password. After all, you will have several applications requiring a password, and Mr Murphy guarantees that different rules will apply in each case. In addition, your process should include others within the company.

Legal	To ensure your wording is correct - particularly taking into account Human Rights Legislation.
Human Resources	To ensure that the company disciplinary process is adequate for the task.
Data Protection	To ensure the policy complies with the DP legislation in all relevant countries.

How do you start?

Before you start, remember you don't have to do this on your own. The international standard I7799 is a good starting point. There are also books on policies which allow you to "pick'n'mix"; and colleagues in the industry can help. Why not use **ISACA**, after all that's what it is there for.

There are a number of things to consider before you start drafting your policy:

- What is the culture and environment of the company?
- Are you reviewing an existing policy, or is this the first?

If the latter you may find that you need to modify your zeal.

You may have read all the books and taken advice, and based on that you have plans for the policy to end all policies, which will cover everything. This is where you need to consider the culture of the company.

I can give one real-life example:

> *The company, with 300 staff, had one floor in a shared building, and there had been problems with outsiders coming in, and property being stolen.*
>
> *My first draft policy said 'all staff must wear the identity badge issued to them', and 'all staff are to challenge anyone not known to them' Not too excessive you would think, however, the CEO did not like all staff to wear an identity badge, since he himself felt self-conscious doing so. The policy had to be changed to 'all staff must have an identity badge'.*
>
> *Senior managers balked at challenging strangers, because they said they would take forever to get to the loo in the morning. This section of the policy became 'if you see someone in your area who you don't recognise you should query this with departmental managers or* HR'.

In such cases you have to accept the culture, amend the policy and save yourself for the review in a few months. No surprise to say, the thefts of property continued.

The lesson to be learnt here is that the policy must cover all staff. If the policy says 'wear a badge' it sends the wrong signal if senior management and higher take the view that 'everyone knows me' and leave their identity cards in their wallets.

Ok, write the policy, based on your experience, knowledge and research and remember to involve IT, Legal, HR and DP. Use the standard company format. Circulate the draft to all parties who made comments, remembering to include any member of the board who has shown an interest. After all, you only want to go to the Board once for acceptance; having to make changes and return will only weaken your credentials as the company security guru.

What next?

OK, you've done your homework and written a policy which has been accepted by the Board and signed by the CEO. Is that it? No. There is more to do

Having written the policy you want it to be read, and there are many ways to do this:

- Send a printed copy to all staff:
- Have HR send a copy to all new staff with the new joiner details;
- Email a copy to all staff;
- Lodge a copy in a shared area and email all staff the shortcut;
- Put a copy on the company Intranet and send all staff the link;
- Posters, mouse mats, and logon banners can all be effective in reaching your audience.

However, having listed several ways to communicate your policy, do be selective in their application to avoid staff getting so many copies that they switch off and ignore the message.

You also need staff agreement that they have read, and will comply with the policy. This will prove to be useful evidence should a member of staff dispute the fact that he/she has read and understood the policy having committed some act that contravenes the policy.

Whichever method(s) you select to send the policy to staff you need to receive back a signed document of agreement or a specific email acknowledging acceptance of the policy.

I believe a form, which the user can read, sign and return, is preferable. This can then be kept by HR and form part of the users staff file.

Once your policy has been issued it is important to review the policy and procedures on a regular basis, say every 6 months or so. Questions you may ask include:

- Are the documents still relevant - does the policy still refer to floppy disks even though there are no PCs with floppy disk drives in the company.
- Have you changed the way things are done? Does this make the policy irrelevant - or just wrong?
- Do you have new technology that isn't addressed at all?
- Are IT considering any new equipment that will not be addressed by the policy?

I wonder how many companies have an old policy, which does not mention Internet usage at all? How many policies do not refer to the PDA's and hand-held computers that so many people use for company business these days?

The follow-on from reviewing the policy is to update it, following the same route you used to get the policy accepted in the first place - and don't forget, the CEO must sign it.

Staff awareness

Although it is the responsibility of the security department to produce and maintain the security policy, security is a process that should involve all members of staff.

If staff see security as something that only gets in their way when they are trying to work, they will not take on their proper responsibility, and worse, will go out of their way to find a work-around to any security measure they do not understand.

You need staff to understand why security is important, and that they themselves are being protected.

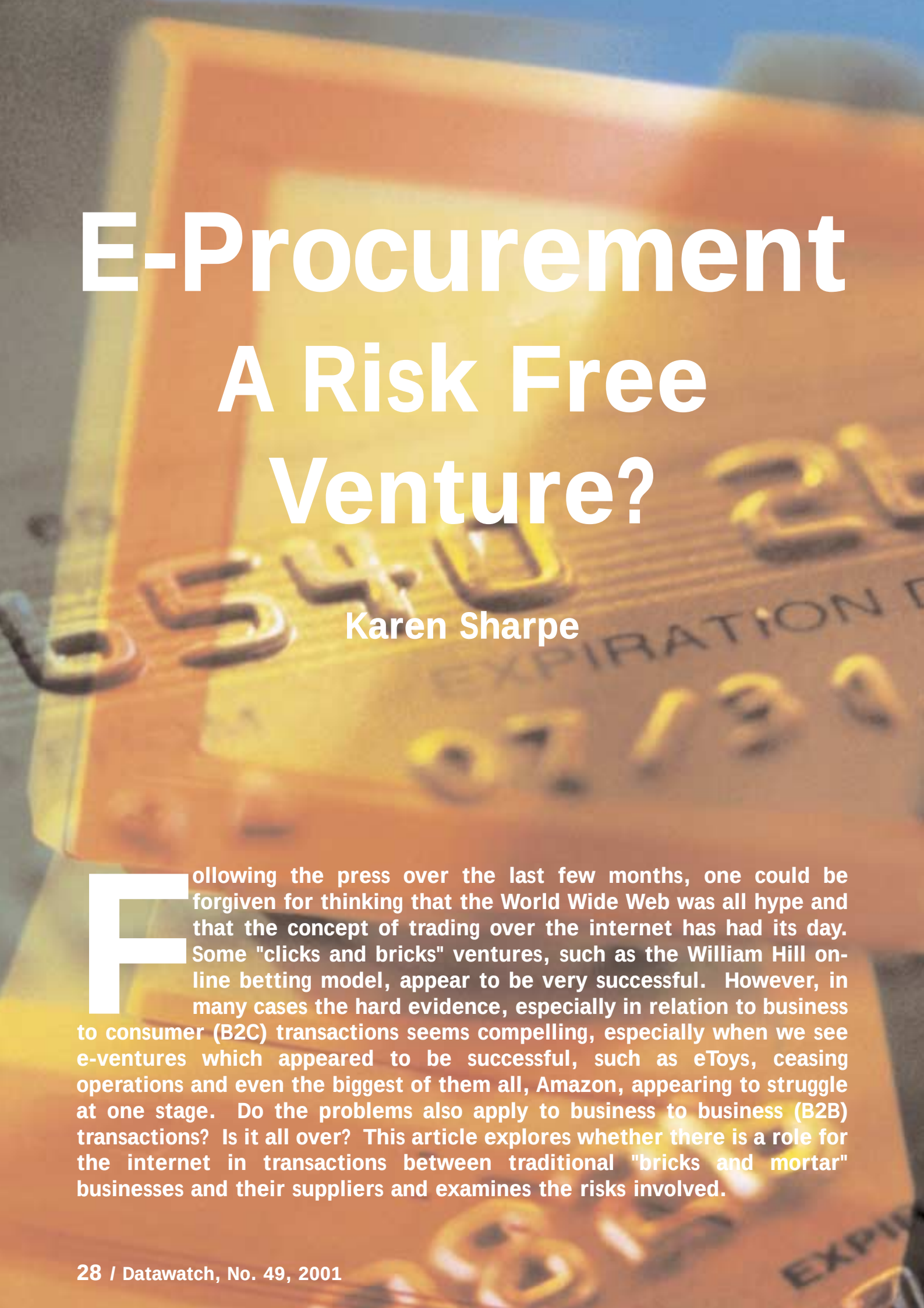
A staff awareness process will start this.

- Change the logon banner to a 'message of the day' with a security item - but keep it simple.
- Institute a short training session with new joiners, and existing staff - keep it short and relevant.
- Add a security note to the company newsletter.
- Posters, mouse mats, and post-its can all be effective in reaching your audience.

However, having listed several ways to get your point across, do be selective in their application to avoid reaching overload so that staff switch off and ignore the message. Remember, you can't be everywhere at once; an educated staff can go a long way towards acting for you. A user is more likely to pick a good password, challenge a stranger, or lock the PC when going for a coffee, if he/she is aware of the consequences of not doing so.

Of necessity, this is a brief, and personal, view of the security policy. I'm happy to discuss and debate any part.

Brian.Shorten@wcom.co.uk



E-Procurement A Risk Free Venture?

Karen Sharpe

Following the press over the last few months, one could be forgiven for thinking that the World Wide Web was all hype and that the concept of trading over the internet has had its day. Some "clicks and bricks" ventures, such as the William Hill on-line betting model, appear to be very successful. However, in many cases the hard evidence, especially in relation to business to consumer (B2C) transactions seems compelling, especially when we see e-ventures which appeared to be successful, such as eToys, ceasing operations and even the biggest of them all, Amazon, appearing to struggle at one stage. Do the problems also apply to business to business (B2B) transactions? Is it all over? This article explores whether there is a role for the internet in transactions between traditional "bricks and mortar" businesses and their suppliers and examines the risks involved.

Why interact with suppliers on line?

There are a number of benefits to doing so, including:

- bulk discounts can be negotiated. Streamlining the number of suppliers used and ensuring that all parts of the company use the same suppliers will increase the volume of orders enabling economies of scale to be realised;
- "maverick spending" can be avoided. Many companies have seen the situation where they have negotiated beneficial rates for goods and services, such as air travel, with a discount dependent upon volume of transactions only to find that employees continue to order flights from their own travel agents and reclaim the costs through expenses. Ensuring that all orders are placed on-line to the preferred supplier can avoid this situation, providing more visibility and control over spending;
- purchasing costs can be reduced. If employees are able to place an order directly with an authorised supplier through the company intranet much of the paperwork can be eliminated, cutting the cost of purchase administration;
- the trading community can be extended, so that companies are no longer trading one to one, but are instead trading with a group of similar entities and suppliers; and
- search time for new suppliers can be reduced, because the search can take place centrally for the whole company rather than many times across different divisions and departments.

Is e-procurement new?

It should come as no surprise to hear that e-procurement has been around for some time now. Many organisations have already established electronic links, especially with their key suppliers, using Electronic Data Interchange (EDI). This technology was introduced in the 1980's and has proven to be very effective. The systems have been reliable over time and have led to close collaboration with valued suppliers and already reaped many of the benefits described above. Companies that have made the investment in EDI certainly don't want to throw it away now. After all, we've all heard the advice "if it ain't broke, don't fix it"!

EDI has some distinct disadvantages, however. The technology is based on dedicated lines between participants via a Value Added Network (VAN), a third party which sits between supplier and customer enabling them to do business with one another. In addition, unique data rules, or protocols, have to be agreed between the parties to enable them to be certain that both internal systems can understand the information being exchanged. This means that EDI is very expensive and has become the province of big companies, largely restricted to core suppliers with whom a good relationship is essential.

Is there any demand for internet e-procurement?

A recent survey revealed that 46% of businesses do not transact on-line today, but only 7% do not expect to do so in two years' time. This suggests that the interest in e-procurement is already established. When we consider that a big company typically spends more than 30% of its revenues on indirect goods and services, which are unlikely to be purchased using existing EDI systems, the potential for e-procurement over the internet seems promising, especially since reductions in these costs have a direct impact on bottom line profit. This view is further supported if we take into account the potential pent-up demand from SMEs which were excluded from EDI because it was too expensive.

How do B2B transactions take place over the internet?

There have been a number of technological changes that have facilitated communications between businesses in the last couple of decades. Not only has hardware become more powerful, enabling companies and individuals to run more sophisticated applications more quickly, but it has also become cheaper and therefore more accessible to smaller organisations. In addition, a number of standards have been adopted which enable different systems to understand one another. The two standards which have had the greatest impact are TCP/IP, which enables any two computers on the same network to communicate with one another and HTML, which when coupled with a browser, provides a common format for presenting web based information.

Procurement activities on the internet can range from simply using it to research suppliers, goods and services to conducting fully interactive transactions, including placing orders and effecting payment over the net. A number of different means of carrying out transactions on the internet have been developed.

Some examples are:

- procurement hubs, online exchanges and trading communities. For example, Httprint, which has a similar business model to letsbuyit.com, where purchasers club together to buy stationery thereby increasing order sizes and reducing prices;
- private portals, where one company sets up a web site through which suppliers can bid to supply its needs. Examples are Lockheed Martin and General Electric; and
- collaboration, where a number of companies in the same industry sector with similar requirements form purchasing alliances. Examples are Exostar, an aerospace consortium

including Boeing, Lockheed Martin, BAE Systems and Raytheon and Covisint, a motor manufacturers hub set up by GM, Ford, Renault, DaimlerChrysler and Nissan.

What are the risks?

The first risk to consider is that the company executives may treat e-procurement as a software purchase. The majority of the benefits that we have claimed for e-procurement will, in fact, derive from strategic and cultural changes rather than software changes. No amount of investment in software can achieve the benefits desired without being accompanied by changes to the way that the company and its employees relate to suppliers.

The internet also has technical limitations in that it is not yet the flexible tool that companies need to operate a free market because it lacks the necessary protocols. Simple communications, such as e-mail, are easy to deal with, but more complex communications, such as producing standard order forms, are not. Software companies have developed e-procurement applications, some of the largest of these being Ariba and Commerce One. However, although this software enables companies to exchange complex information with one another, it has the limitation that the supplier must use the same software as the customer and operate in the same market place before trading can take place.

As with other areas relating to the internet, a rash of procurement hubs and applications have been developed, not all of which will survive. This means that companies currently need to try to second guess which the survivors will be prior to investing. The risk is that not everyone will back the right horse. Good news is on the horizon in this respect. A new standard language, XML, which was first written in 1998, is being backed by some of the biggest software companies in the world, Microsoft, HP, IBM and Sun. XML will enable all systems, irrespective of the underlying applications being used, to understand complex instructions and promises to provide the flexibility for truly open markets to be developed. This still amounts to "jam tomorrow" however, without a tangible date attached to its availability. If the benefits that can accrue from electronic purchasing result in the in cost reductions that are widely quoted, companies will not want to miss out on the competitive advantage, so can they afford to wait?

In addition to the commercial risks above, there are also security risks to be aware of. Opening up the purchasing functions to employees to reduce the paper trail and gain more control over the items ordered results in more individuals being given greater access to computers and more reliance being placed on electronic authorisation. The company must have a strong security culture, supported by good policies and procedures, to ensure that security is adequate to protect the company from fraud. Password sharing and poor security design within the applications will undermine many of the potential benefits. The company's systems must also be protected from attack from external hackers, with effective and regularly tested firewalls in place.

There are other risks to be considered. For example, the more reliant a company is on its computer systems to carry out transactions, the greater the impact of a loss of those systems will have to day to day running of the business. This raises the importance of good business continuity plans, which cover both recovery of IT resources and maintenance of operational functions. In addition, there are legal and tax risks, which may arise if cross border transactions are taking place.

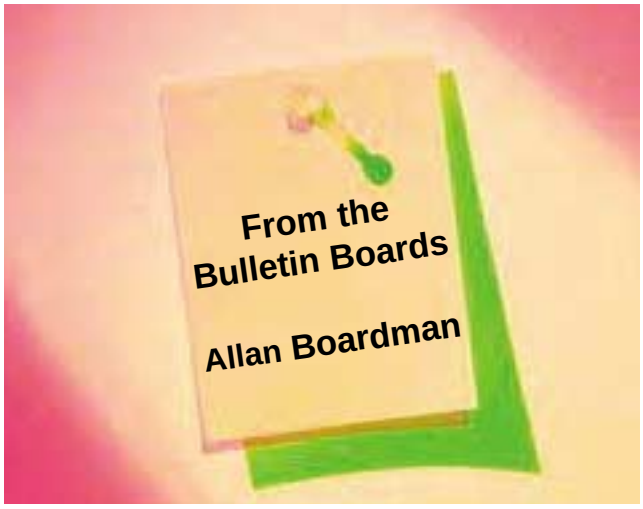
Conclusion

In conclusion, the evidence of increasing interest in on line procurement suggests that there is a role for the internet in transactions between traditional "bricks and mortar" businesses and their suppliers. Whilst many large businesses are already established in this arena with EDI arrangements, there is pent up demand from SMEs which were excluded from EDI because of cost and complexity. In addition, large companies only tend to use EDI for transactions with essential suppliers, but there are opportunities to purchase non-core, indirect goods and services for which a cost reduction would have an impact directly on bottom line profit.

The internet is not a risk free environment, however, and there are a number of risks to be considered. Strategically, culture and internal processes need to be changed to gain the benefits enabled by e-procurement software. At a more detailed level, greater reliance on computer systems requires a more diligent security culture and stronger, more effective business continuity plans.

Karen Sharpe is the President of the London Chapter of ISACA and a Senior Manager in Deloitte & Touche's Enterprise Risk Services group in London.

Do you have any burning question about Information Security or Audit related matters? There is now a range of online forums and bulletin boards where your questions, general or technical, can be answered by experts, or sometimes just by people with a keen interest in sharing their knowledge. Here are some examples.



From:
www.computerworld.com

Question:

What do you think will be the top issues facing executive-level security managers next year? And how do you think those managers will resolve them?

Response from Nigel Willson - the Burton Group:

From experience of a rapidly growing .com together with mergers, acquisitions and, new opportunities, security can become an enabler that allows an enterprise to become agile and competitive.

There is a major convergence underway as the intranet and extranet converge, public and private networks converge and, the concept of inside and outside disappear.

As global network security perimeters allow richer and richer connectivity inwards and extend outwards to employee homes, we can no longer afford to drop critical servers on the intranet and "assume" that the inside is special and/or protected. It is a recipe for failure.

What is necessary is the adoption of a distributed, modular and, flexible architecture that supports an underlying general-purpose infrastructure, a substrate leveraging directory and security as a common authentication and authorisation model.

Through integrated security, the consolidation of fragmented infrastructure servers that were intranet-facing and now serve customers and partners pushed into Internet-based data centres that act as enterprise portals B2B, B2C, and, B2E; the security problem can be simplified and solved in a 2-3 year migration strategy.

My advice is to remove internal trust of global LANs, treat all users the same be they employees, customers, or partners, use the WAN as a transport with no greater trust than the Internet and above all, KISS.

From www.itsecurity.com/asktecs/asktecs.htm

Question:

As a doctor, I use a dial-up Internet connection in order to download patient-related data in the form of encrypted messages. The problem is in protecting the existing data held on my PC (unencrypted) from the possibility of being tampered with while I am on line. An ISP is used, and therefor the dial up machine will be given a different IP address each time (I know that this reduces the already minimal risk), but the query is just "Would the addition of Zone Alarm eliminate all risk?"

Response from hal.lockhart@entegrity.com:

One of the most important things to understand about security is that there is nothing that can "eliminate all risk."

If your system does not run any servers, as is likely in the configuration you describe, the highest probability threat is to be infected by a Trojan Horse carried in an e-mail attachment. In other words, you probably need a virus checker more than a personal firewall.

Supplementary question related to personal firewalls:

In the UK, although DSL is still slow to get going, we are beginning to find ISPs that will provide fixed fee surfing. For example, BT offers a service that allows you to connect for as long as you like at no extra cost. In this instance, the line automatically drops after 2 hours - but nevertheless most users will stay online for 2 hour chunks. Does this type of 'extended' surfing increase the risk?

Further response from hal.lockhart@entegrity.com:

The simple answer is, of course. The longer you are online, the more time an attacker has to poke around and find a weakness.

It is important to understand that all the methods of attacking your system involve getting some code to run on your system that the attacker can take advantage of. Some typical examples are:

- Exploit a bug, such as a buffer overflow in a privileged server you are running.
- Take advantage of a misconfigured server, e.g. ftp to write a file in a specific place on your system.
- Send you a Trojan horse as an e-mail attachment and somehow get you to run it.
- Get you to download and run some program from a web page.

The chance of attacks like #3 and #4 is essentially independent of connect time. (Except that if a Trojan is installed, the attacker will only be able to control it while you are connected.) Attacks like #1 and #2 can easily be prevented by disabling all servers on your system.

In summary, if you only use your system as a client, i.e. Web surfing, downloading and e-mail:

- turn off all servers,
- get a good virus checker and keep it up to date and
- be careful about executing any downloaded programs.

With these simple precautions you should be reasonably safe regardless of how long you stay connected each day. If on the other hand, you are using your system to host a web server or ftp server, life gets a lot more complicated.

Thanks to the Authors and Websites for permission to use the material.

Security Column

John Hunter

Let's all upgrade to Digital radios

We've recently opened an office in Moscow to service a project there. Its shared with an internet company so has all the technology that we want. I'm mentioning this because, as luck would have it, they are also security specialists. The guy was explaining how the local law had recently changed to make to sale of copied software illegal and so he had to pay the full price for his new Windows Office XP even though it was on sale in the local bus station booth for £1.50 (This was a week or so before its release in the West).

We are deep in a Ministry building and physical security is not an issue - you'd have to be very brave to get past the two large ladies sat in their cubicle at the entrance. I was being shown some neat 'Bluetooth' devices and we were musing on how times had changed. There had been revolutionary books like 'Secrets of a Super Hacker', 'The big Book of Secret hiding Places' and my favourite title 'Lip Reading Made Easy'. I remember being at home using Prestel on a Spectrum and being astonished to suddenly find myself on a US Government site. No logon had been needed, so I don't think that it was hacking. We'd read books about message interception and I'd tried to read data using crocodile clips on network cables. I don't remember getting it to work, but I did acquire a nifty bit of kit to capture data from dumb terminals. It was before the days of cheap hard disks and so had an integral 3¼" diskette drive and its own operating system so that it could properly write real-time giving you time to change diskettes, buffering to memory. We used it to get data off all forms of 'mainframes' and 'minicomputers' in the mad race to transfer everything to the new fashionable 'micro computers'. It was big and difficult to carry around, and eventually it was replaced by a card to fit in a pc. Of course, the portable computers of those days were big enough to accommodate one or more standard pc expansion cards. However, we soon moved to 'laptops' which couldn't accommodate it so reluctantly we had to go back to using the original dedicated capture box.

Then there were the Dutch who discovered that you could read a PC's screen from a hundred yards away if you pointed your TV's aerial at it. That was a bit hit and miss, obviously, as you could only get to see what the user was displaying on his/her screen at the time.

The internet came and suddenly it became so easy to steal information. You didn't have make a physical connection - everybody was already connected to everthing. For anyone with the resources it would always now be easy to keep one step ahead of the security systems, and then there will always be those sites that don't bother to keep up-to-date with the security patches.

One of the main reasons this activity is limited to 'professional' hackers (or fools) is the fear (or not) of being caught. If there was a way of being totally anonymous, impossible to trace, what would the new hacker community look like? I'm sure that the focus would move away from outsiders getting in to your systems; staff would be eaves-dropping on their bosses, payroll departments a constant reference resource to everyone in the building, 'I'll just look up how my fellow salesman is doing'. Sit back now and consider yourself in a world where anyone could look at any of the data on your system without any fear of being identified; who would it be?

Welcome to wireless networking...

The Career Column

Adrian Simpson

It does not seem that long ago, certainly less than a year, I reported in this column, that for the first time in many years, there appeared to be unemployment amongst computer auditors. Something to do with a Y2K hangover. You will be pleased to learn this phenomenon has proven temporary and the market has again entered a period of chronic shortage of computer auditors and I.T. security specialists.

Now it is likely, given the relationship between supply, demand and price, that computer auditors would consider this to be unalloyed good news and have every reason to anticipate healthy salary increases. Without doubt such forces are at work and computer auditors are in a stronger bargaining position than most. Positive developments have also included older computer auditors and perhaps those with less conventional CV's being able to find work. The opportunities to undertake contract work and more flexible working practices, as I reported last quarter, have also grown.

There is, however, a potential downside. It has become apparent that a number of companies have grown tired of attempting to recruit and retain computer and to a lesser extent other types of auditors. The opportunity to throw money at the problem has not always been available or worked when it was. A reaction to this has been to enter partnering or outsource agreements with external providers, primarily the big 5. Unfilled computer audit positions and many that are already filled are transferred across to external providers. The computer audit positions still exist, the work is still done, but they are external rather than internal.

Now, in many parts of the UK this does not matter. The local recruitment markets are of sufficient size to offer a wide choice of potential employers. However, in other parts of the country, employment opportunities are thinly spread. There are only a very limited number of internal audit departments within effective commuting distance. As these are the ones that are more likely to contract out, the choice of where and for whom you work can become very restricted.

Now I would like to believe that choice and the opportunity to work in different environments and business cultures contributes to the quality of most people's professional lives. I am sure there are many computer auditors who would prefer to retain a wider element of choice even at the expense of a lower salary. Although strictly from my point of view smaller numbers of larger departments makes recruitment easier, it detracts from the diversity of a market that is already constantly under attack from takeovers and mergers. Healthy markets also require a sufficient number of buyers and sellers to provide liquidity, which is really just another way of saying that computer auditors can find new employers and employers can find new computer auditors. That in some parts of the country shows every sign of being eroded.

Perhaps after almost a decade of unbroken growth the economy is about to stagnate or even contract. Certainly the threat of a recession in the United States and Japan appear real and Europe and the UK are not proving as immune as perhaps previously thought. However, to date, there has been no effect on computer audit recruitment. Surprisingly, the technology companies that have born the brunt of recent redundancies are not significant employers of computer or even general auditors. Even the manufacturing sector, which has been contracting for over a year, employs fewer computer auditors than most other sectors. To date, manufacturing companies have shown no propensity to shed audit staff.

This does not mean that any significant slow down in the economy would not effect computer audit recruitment; it would. However, what is not always widely appreciated is that the number of computer auditors employed in the economy has been falling steadily for the last ten years. Most companies not only use internal audit departments to contain costs, but expect the cost of internal auditing to fall. There is no longer the potential to save costs by slashing the size of internal audit departments that there once was.

It is perhaps a testament as to how far the economy has changed. Partnering and contracting out agreements as in other specialist areas have provided far greater flexibility in resourcing internal audit departments. They have also developed, promoted and helped to disseminate best practice and have without doubt benefited internal and computer auditing over the last decade. However, whether they will ultimately contribute to the employment choices available to computer auditors is another question.

INTERNET RESOURCE LIST

AUDIT

http://www.isaca-london.org
www.isaca.org
www.auditnet.org
www.acua.org
www.gallaudet.edu/~auditweb/index.html
www.gallaudet.edu/~auditweb/kits.html
www.anao.gov.au/reports.html
www.theiia.org
www.iia.org.uk
http://www.methodware.com/links/
www.itaudit.org
www.barclaysimpson.com

SECURITY

www.cert.org
ciac.llnl.gov/ciac/
spam.abuse.net
www.cl.cam.ac.uk/spam/
www.iki.fi/liw/mailfilter.html
csrc.nist.gov/secpubs/unix_security_checklist.txt
www/ntsecurity.net/
www.first.org
www.cauce.org/
http://www.securityportal.com/
http://www.antionline.com/
http://www.cerias.purdue.edu/coast/hotlist/
http://www.sse.ie/securitynews.html
http://www.infosyssec.org/infosyssec/index.html
http://web.mit.edu/security/www/gassp1.html
www.eSecurityOnline.com
http://www.pki-page.org/
http://www.microsoft.com/TechNet/win2000/win2ksrv/prodfact/pkiintro.asp
http://www.sans.org/topten.htm
www.securitywatch.com

COMPUTER COMPANIES AND SYSTEMS

www.microsoft.com
www.alw.nih.gov
ntresearch.com/
www.acl.com/audit/audit2.htm
www.caseware-idea.com
http://www.sap.com/mysap/
www.windowsitsecurity.com

OTHER ORGANISATIONS

www.bcs.org.uk
http://www.auditserve.com/frmain.htm
www.coactiveconnection.com/
www.mc2consulting.com/

HACKERS AND VIRUSES

www.2600.com/mindex.html
www.sophos.com/virusinfo
www.drsolomon.com/vircen
http://www.cnn.com/TECH/specials/hackers
http://www.l0pht.com/

AREAS OF AUDIT INTEREST

www.disastercenter.com/audit.htm
http://www.teleport.com/~jhw/csa/
http://www.clark.net/pub/mjr/pubs/fwfaq/index.htm
http://ecommerce.internet.com/
http://www.ecrc.ctc.com/about.htm

Answers to Word Puzzle on page 3.

Een, eer, enter, entire, entre, ere, ern, erne, inert, inner, intent, inter, intern, interne, ire, nee, neer, nene, net, nett, nine, nit, niter, nitre, ree, rein, rennet, rent, ret, rite, tee, teen, teer, ten, tenet, tenne, tent, tenter, tern, terne, tete, tie, tier, rin, tine, tinner, tint, tinter, tire, tit, titer, titre, tree, treen, trente, tret, trier, trine, trite.

[All words from Concise Oxford English Dictionary]