



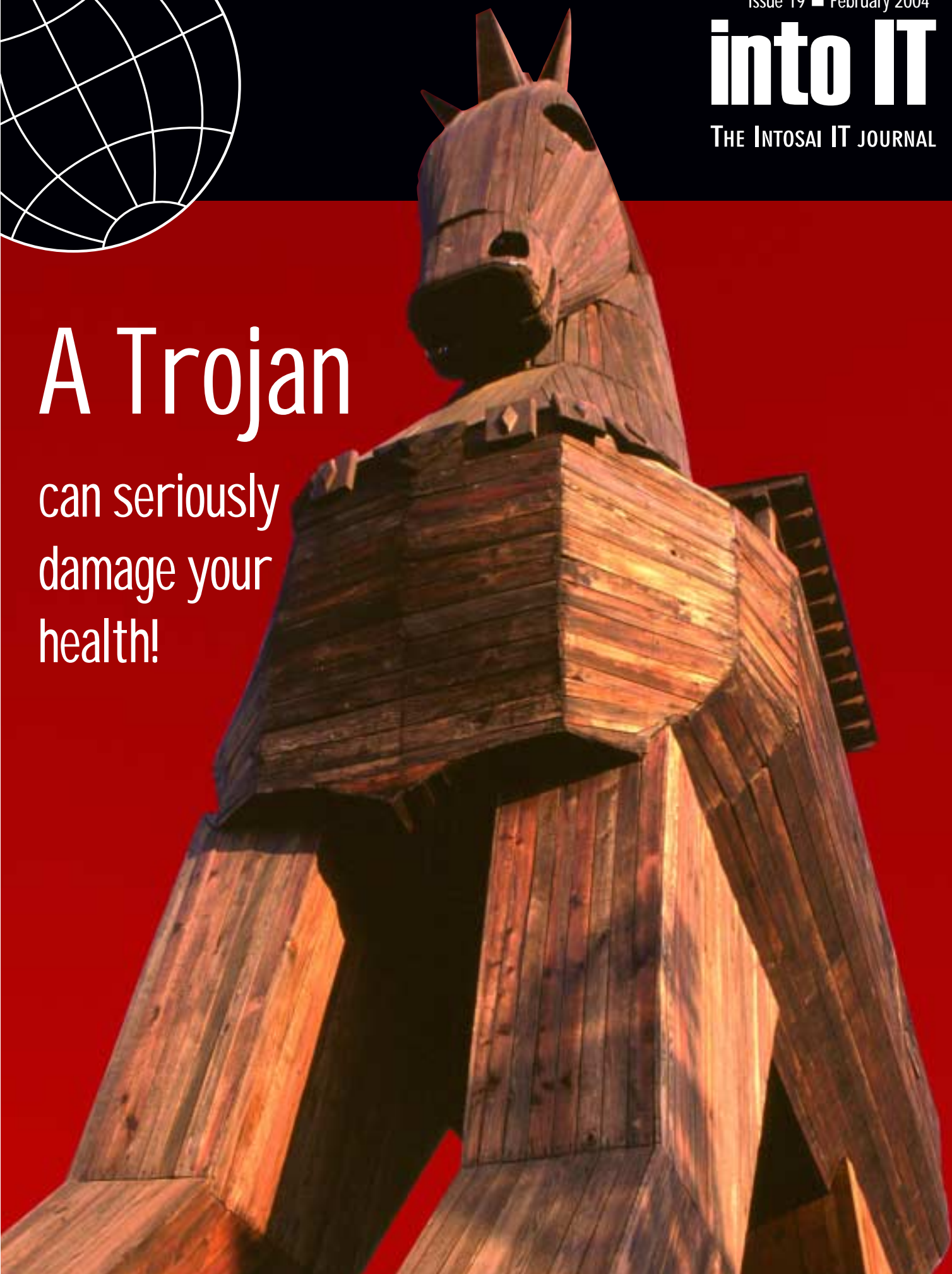
issue 19 ■ February 2004

into IT

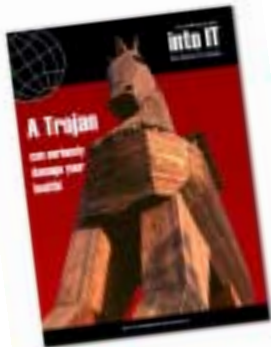
THE INTOSAI IT JOURNAL

A Trojan

can seriously
damage your
health!



into IT editorial



intoIT is the journal of the INTOSAI Standing Committee on IT Audit. The journal is normally published twice a year, and aims to provide an interesting mix of news, views and comments on the audit of ICT and its use in Supreme Audit Institutions (SAIs).

Material in the journal is not copyrighted for members of INTOSAI. Articles from intoIT can be copied freely for distribution within SAIs, reproduced in internal magazines and used on training courses.

The Editor welcomes unsolicited articles on relevant topics, preferably accompanied by a photograph and short biography of the author, and short news items for inclusion in future issues.

The views expressed by contributors to this journal are not necessarily those of the editor or publisher.

editorial address

Contributions should be sent to:

The Editor of intoIT
National Audit Office,
157-197 Buckingham Palace Road,
London
SW1W 9SP
United Kingdom

E-mail intoit@nao.gsi.gov.uk
Web site www.intosaiitaudit.org

New legislation before the U.S. House of Representatives requires all publicly quoted companies to conduct independent, computer security assessments and report the results in their annual reports. The Corporate Information Security Accountability Act of 2003, if approved, requires companies "to assess the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems," and "determine the levels of information security appropriate to protect such information and information systems".

The Act requires companies to hire an independent auditor to assess existing information security controls and ensure that they meet basic standards that the U.S. Securities and Exchange Commission has yet to determine. It will be interesting to see whether the standards will also extend to the independent auditor's qualifications and experience for reaching a meaningful and reliable conclusion. Is the auditor likely to be a thoroughgoing, information security professional, or a financial auditor who has completed the (5-day, or whatever) course? Will the audit merely confirm the existence of the right documents - suitably dated and authorised - that say the right sorts of things? Or will the auditor be required to conduct more searching tests to assess whether the documentation is a façade that, in good 'cowboy town' tradition, is propped up by nothing more than a few scaffolding poles? And will organisations who, having acquired the auditor's seal of approval, rest complacently on their laurels for the next 12 months? We await developments with interest.

A recent prime-time UK television programme featured real-time burglary. An ex (so we were told) professional burglar was hired by the programme producers to break into the homes of volunteers and 'borrow' their valuables. It was disturbing to witness the ease with which our resident expert generally accomplished his task. Truly, "penetration testing" in the raw.

Entertainment aside, there was much to learn from the ensuing debate, which considered the vulnerabilities uncovered and the countermeasures that ought to have been in place¹. Door and window locks, security lights and their positioning, intruder alarms, and a host of other techniques were examined and discussed. Household security was then strengthened and retested, and while the improvements did not always withstand further attack, an important point emerged. *Potential intruders are deterred by effective countermeasures* because their penetration is time-consuming and likely to attract unwelcome attention. The trade much prefers soft targets from which, it seems, that there are plenty to choose.

Although this scenario relates to the real world, it maps easily onto cyberspace, where network administrators have daily to pit their wits against increasingly sophisticated intrusion techniques. As IT systems become increasingly interconnected, more national and global networks are emerging, and while this opens up unprecedented opportunities and benefits for both citizens and state alike, it presents the criminal with new opportunities. Systems connected to the Internet and to other networks become potential targets and the high level of attacks against commercial and government systems, as well as

¹ See... <http://www.bbc.co.uk/crime/prevention/yourhome.shtml>

contents

individuals, continually demonstrate the skill and determination of cyber criminals to exploit technical vulnerabilities and human naivety. There can be no doubt that, as more business is transacted online, the potential for cyber crime and its incidence will increase. Although most network administrators take sensible precautions, they have other responsibilities and cannot always be blamed if they are not abreast of the latest, often highly ingenious, technical exploits that facilitate cyber crime. This is work for the specialist, and it is here that well planned and conducted penetration testing can expose serious vulnerabilities.

In this edition we highlight some of the technical and procedural countermeasures for protecting networked information systems, including penetration testing, a technique that despite its risks is becoming a more widely accepted strategy for protecting online information and services.

Our first theme article provides a layman's guide to hacking. For the benefit of readers who are unfamiliar with the subject, N. Nagarajan of the Office of the Comptroller and Auditor General of India explains some of the approaches to computer hacking and the terminology that often crops up in connection with it.

Our second theme article describes a penetration-testing project that was planned and supervised by the Office of the Auditor General for North Carolina. The article is interesting both for its description of the outcome (21 of the 22 target systems were penetrated successfully, most in less than 30 minutes) and for the approach to the task.

The focus of network security used to be at the perimeter, where firewalls were positioned to keep uninvited guests



out of the internal network, but growing recognition of the risk of attack from within and the advent of e-mail as a vehicle for planting a Trojan in the system has changed the picture. Our next three articles develop this theme. Written by staff at the UK's National Infrastructure Security Coordination Centre² they provide an overview of recent developments in intrusion detection systems; of e-mail spoofing, a technique sometimes used by hackers to obtain system passwords; and of Trojan horse software. And believe me, a Trojan can seriously damage your health!

To round off this edition's theme of hacking, we have received an excellent article from the Auditor of Public Accounts of the Commonwealth of Kentucky, USA. Ed Hatchett takes a robust stance on the subject of network security, commissioning detailed technical appraisals of state departments' controls and not being shy about publishing his findings. In his article, Ed describes the results of an audit of the Transportation Cabinet network in which his team uncovered both hackers at work and criminal activity. And yet top of his recommendations is the simple expedient of applying a good standard of password management.

² NISCC's role is to co-ordinate and develop the UK critical national infrastructure's defences against electronic attack... <http://www.niscc.gov.uk>

Country Focus:
The UK National
Audit Office

2

Not Knowing What
You Do Not Know

12

State of
North Carolina

20

Trojan Horses and
Kernel Root Kits

24

Intrusion Detection V
Intrusion Prevention

26

Email Spoofing

29

A State Auditor's Network
Security Case Study

31

Risk Based Sampling
Using COBIT

36

Going Electronic

40

Freedom of
Information

43

Dig the Spacedirt

48

GAO Working
with Congress

51

A Chilling Thought!

55

Country Focus:



The UK: some facts and figures

UK: 244sq km - approximately the size of the U.S. state of Oregon or the African country of Guinea - comprises England, Wales, Scotland and Northern Ireland, plus many surrounding islands but excluding the dependencies of the Isle of Man and the Channel Islands. No part is more than 75 miles from the sea.

Population: 60M

Ethnic groups: English 81.5%, Scottish 9.6%, Irish 2.4%, Welsh 1.9%, Ulster 1.8%, West Indian, Indian, Pakistani, and other 2.8%

Languages: English and Welsh, but Gaelic, Urdu, Hindi, Punjabi and other languages are spoken.

Religions: Anglican and Roman Catholic 40 million, Muslim 1.5 million, Presbyterian 800,000, Methodist 760,000, Sikh 500,000, Hindu 500,000, Jewish 350,000

Government: parliamentary monarchy and part of the European Union. Everyone over the age of 18 can vote.

Legal system: common law with early Roman and modern continental influences. Judicial review of Acts of Parliament under the Human Rights Act of 1998. The UK does not have a written constitution.



National Audit Office

The UK: historical background

What scant knowledge we have of Britain before the Roman conquest comes mainly from archaeology, which provides clues about our early culture and economic development but rarely identifies personalities, motives, or exact dates. Julius Caesar left us his impressions of Britain at the time of his brief visits in 55 & 54BC, which is the earliest coherent account we have. Even in later Roman times, Britain was considered to lie at the periphery of the civilised world, and Roman historians left us little more than a framework in which to slot the results of archaeological research.

The Roman invasion of Britain began in 43AD. While many British tribes made political deals with the invaders, they also encountered stout resistance. Indeed, the Romans never fully occupied Britain, concluding that Scotland wasn't worth the effort. Roman Britain's northern border was eventually stabilised on a heavily fortified wall in northern England, slightly south of the existing border. Much of "Hadrian's Wall" still exists and is a popular tourist attraction.

For over three centuries, Roman life prospered in what is now England. The local tribes became integrated into an urban, governmental system, and grew accustomed to a peaceful, ordered way of life. Roman towns had properly drained and metalled streets, water supplies, forums and other public buildings. But perhaps the Roman's greatest achievement was their system of magnificently engineered roads, built to allow the swift movement of troops, munitions, and supplies from one strategic centre to another (the English

were to use the same strategy to subdue the Scottish clans during the 18th century).

Following the collapse of the Roman Empire early in the fourth century, urban life in Britain declined and we sank again into an age of intellectual darkness and barbarity that was to continue for 600 years. Christianity and the use of money ceased for some two centuries, while the physical character of our people, language, and institutions changed. Germanic tribes from Europe replaced a significant part of our lowland population, their dialects replaced Latin and Celtic (later giving rise to the English spoken today), and loosely knit and feuding hereditary kingships replaced the centrally governed Roman provinces. Among these illiterate and pagan tribes were the Angles and the Saxons, and Britain came to be called "England" after the former (a derivation of "Engla-land" or "land of the Angles"). Although the Anglo-Saxons were not as sophisticated as their Roman predecessors, within a few centuries they had built a hierarchical, regulated society in which agriculture and trade flourished.

Later in the millennium, the Anglo-Saxons found themselves invaded from Scandinavia by the "Vikings". Sometimes the Vikings were beaten back, at other times not. Eventually they were granted parts of the country where their own laws prevailed, although by 1066 - a highly significant year in our history - an Anglo-Saxon king was in control.

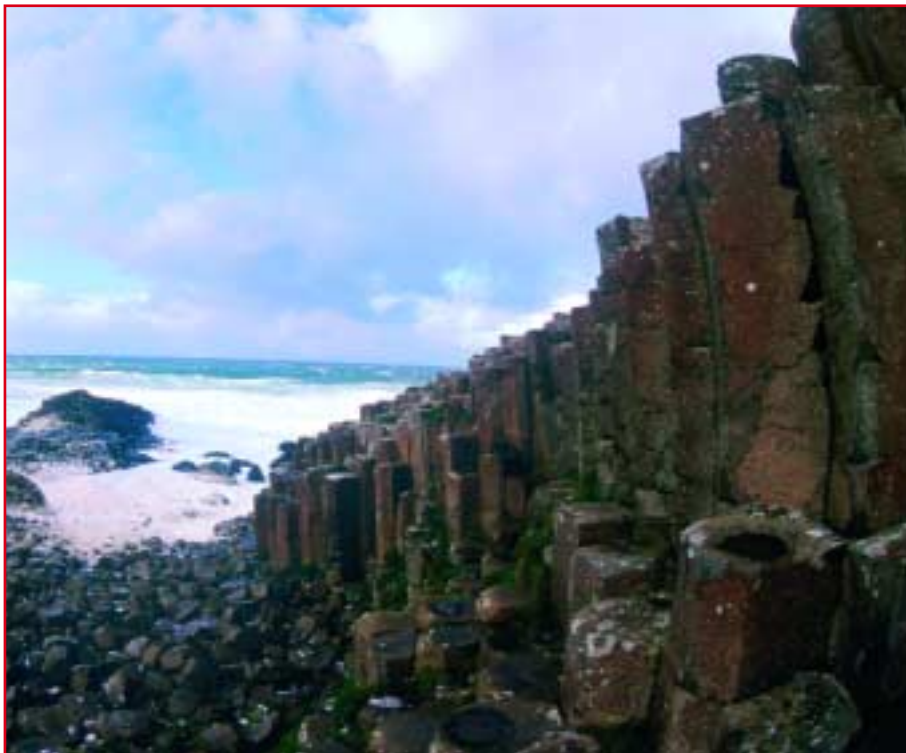
Reliable written evidence from the first millennium is limited¹, but archaeology provides many clues about Roman, Anglo-Saxon and Viking settlements and daily life, and all of these peoples left us examples of beautiful jewellery, pottery, sculpture, and metalwork. The study of names and language shows more enduring effects, while in the case of the Vikings DNA analysis provides some insight into their effects on our genetic stock.

¹ For anyone interested in delving deeper, there is a good source is at... <http://www.britannia.com/history/docs/>



Carew Castle

The English built a fine set of castles in Wales to help encourage the indigenous population to toe the line. Many remain and are worth visiting.



Giant's Causeway

When the giant Finn McCool fell in love with a lady giant on Staffa, an island in the Hebrides, he built this wide commodious highway to bring her across to Ulster.

In 1066, our neighbours, the Norman French, successfully invaded England; they were the last to do so. Since then, despite occasional periods of civil war, England has remained a unified entity.

Under the Normans, government was again centralised, a bureaucracy built up, and written records maintained. The roots of the English "common law" legal system date from this period.

Wales and Scotland, originally independent kingdoms, both strongly resisted English rule. King Edward I conquered Wales in 1282 and an Act of 1536 completed the political and administrative union of the two countries; 1707 saw the union of Scotland and England and our adoption of the name "Great Britain".

As for, Ireland, invasion by the Anglo-Normans in 1170 was to lead to centuries of strife, with successive English monarchs (and Oliver Cromwell) seeking to gain control, with varying degrees of success. To cut short a painful story, the Anglo-Irish treaty of 1921 formalised a partition of Ireland. The six counties that constitute "Ulster" maintain their constitutional links with Great Britain, while the other 26 counties became the "Irish Free State" (and in 1949 the "Republic of Ireland").

In 1927, we adopted the name "United Kingdom of Great Britain and Northern Ireland", usually abbreviated to 'United Kingdom' or 'UK'.

The British Empire

The British Empire began to grow at the beginning of the 17th century, eventually expanding over much of the globe, particularly in North America and India. It was built on colonial trade, which originally went hand in hand with slavery; slaves bought in West Africa were shipped to the Americas where



Stonehenge, Wiltshire, England

Erected in stages between 3000 and 1500 BC, no one really knows why.

they were sold to plantation owners in exchange for produce, which was then shipped back to Britain. Later came the Industrial Revolution, which was to dominate 19th century British history. Queen Victoria's reign in particular saw the products of our engineering expertise together with our commerce, language, and systems of law and government spread throughout the Empire, which at its zenith encompassed roughly one-fifth of the globe.

The heyday of Empire ended in 1914. During the following decades, our economic strength was devastated by two World Wars. The post-war years saw the rapid dismantling of our Empire and our transition to a European nation.

The UK today

The UK today is a leading trading power and financial centre, and one of the four 'trillion dollar' Western Europe economies. Our agriculture is highly efficient by European standards,

producing about 60% of our food needs with only 1% of the labour force. We have significant coal, natural gas, and oil reserves, primary energy production accounting for 10% of GDP, one of the highest shares of any industrial nation. A decline in our manufacturing industry has been offset by our expanding service sector - particularly in banking, insurance and business services - which accounts for by far the largest proportion of our GDP.

Our long-established parliamentary system is currently the subject of reform. Hereditary membership of our upper legislative assembly, The House of Lords, is being abandoned in favour of politically appointed representatives. Scotland and Wales now have National Assemblies with varying degrees of power, and further assemblies for the English regions seem likely.

The UK's role as a major world financial centre, our strong ties with the Commonwealth, and a permanent seat on the UN Security Council help us continue to exert significant influence in world affairs.

About the NAO: the early years

The National Audit Office has existed in its present form since 1983, but the public audit function in central government has a long history.

The earliest surviving mention of a public official charged with auditing government expenditure is a reference to the *Auditor of the Exchequer* in 1314. The *Auditors of the Imprest* were established under Queen Elizabeth I in 1559 with formal responsibility for auditing Exchequer payments. This system gradually lapsed and in 1780, *Commissioners for Auditing the Public Accounts* were appointed by statute. From 1834, the Commissioners worked in tandem with the *Comptroller of the Exchequer*, who was charged with controlling the issue of funds to the government. However, Parliament's role in this process was limited.

Parliament had for several centuries been responsible for raising revenue and authorising expenditure (the English



Forth Railway Bridge, Scotland

Civil War had been fought largely on this issue) but their control and scrutiny of public spending was weak. It was not until the 1860s that the first major steps were taken towards proper financial accountability to Parliament.

Parliamentary audit

The Exchequer and Audit Departments Act of 1866 established a cycle of accountability for public funds in which The House of Commons authorised expenditure, the Comptroller and Auditor General (**C&AG**) controlled the

issue of funds, and accounts were produced by departments and audited by the Comptroller and Auditor General. The results of the C&AG's investigations were considered by a dedicated Parliamentary committee, the Committee of Public Accounts (**PAC**). From the 1870s, the PAC took evidence from senior officials, normally Heads of Departments, who were designated as "Accounting Officers" by the Treasury.

Initially, the C&AG and his staff were required to examine every transaction, but this became unrealistic as the level of government activity expanded, particularly during the First World War. New

legislation, the Exchequer and Audit Departments Act 1921, addressed this by allowing the C&AG to rely in part on departmental systems of control and thus examine only a sample of transactions. This Act also required the C&AG to report to Parliament that money had been spent in accordance with Parliament's wishes.

Reform

Pressure for the reform of the public audit system again grew from the 1960s, following concerns expressed by

Is Comptroller a misspelling?
Should it not read Controller?

"Comptroller" first appeared around 1500 and is thought to be a misspelling of "controller". This embodied an older error arising from the false presumption that the responsibilities involved were somehow connected with "accout" or account, the controller being the "contrarolutator", one who kept a counter-roll as a double check on transactions.

The Cycle of Accountability

Once public money has been spent by a central government body, the C&AG is free to report to Parliament on the regularity, propriety, and value for money with which this has been done.

The Committee of Public Accounts can take evidence on this report from the most senior official in that public body and can then make recommendations to which the Government must respond within two months. The C&AG and/or the PAC can decide to conduct a follow up investigation into the issues raised.

We are also willing to assist Parliament in whatever way we can. Each year, we respond to over 400 queries from Members of Parliament on issues affecting public spending.

Parliamentarians and academics that the scope of public audit needed to be modernised to reflect the significant changes in the role of government over the course of the twentieth century. In particular, it was argued that there was a need for a specific power to allow the C&AG to report to Parliament at his own discretion on the value for money achieved by government departments. Reformers also argued that more robust arrangements should be put in place to ensure the independence of public auditors from government.

These changes were reflected in the National Audit Act 1983, under which the C&AG formally became an "Officer of the House of Commons" with the express power to report to Parliament at his own discretion on the economy, efficiency, and effectiveness with which government bodies have used public funds. The Act also established the National Audit Office (NAO) - which replaced the Exchequer and Audit Department - to support the C&AG in discharging his role.

Further important changes have occurred in recent years. Following devolution, new Auditors General have been appointed in Scotland and Wales to audit the expenditure of the new Parliament and Assembly. In Scotland, the Auditor General is supported by a new body, Audit Scotland², which oversees local government audit. The NAO in Cardiff provides audit services to the Auditor General for Wales³. There has been a separate C&AG for Northern Ireland since the foundation of the state in 1921. He heads the Northern Ireland Audit Office⁴ and reports to the Northern Ireland Assembly.

The introduction of resource accounting and budgeting is another important development for the NAO, involving a change from a 'cash' to an 'accruals' based system of planning and accounting for expenditure.

"The Committee of Public Accounts would not get very far as a bunch of 15 Members of Parliament, unless we had the quality and depth of research contained in the reports we receive from the NAO."

*Rt Hon Alan Williams MP, Chairman,
The Public Accounts Commission*

The development of audit

The work of successive C&AG's had reflected changes in the nature of government over the years.

In the later years of the nineteenth century, much audit work concentrated on issues of propriety, with the C&AG repeatedly reporting to Parliament on irregular payments and practices by Government departments. The expansion of government in the twentieth century led to substantial changes in the C&AG's work, with reports to Parliament concerning large budgets, such as those for old age pensions, hospital construction programmes, and payments to universities.

Over time, the focus of our work has shifted from reporting simply on the details of expenditure to consideration of the value for money achieved by government expenditure, a process that was accelerated greatly by the passing of the 1983 National Audit Act.

Gladstone's reforms

Champion of reform, William Ewart Gladstone, was Chancellor of the Exchequer from 1859-1866 (and, for good measure, four times Prime Minister - 1868-74, 1880-85, 1886, and 1892-94).

As Chancellor, Gladstone initiated major reforms of public finance and Parliamentary accountability. His 1866 Exchequer and Audit Departments Act required all departments, for the first time, to produce annual accounts, known as appropriation accounts. The Act also established the position of Comptroller and Auditor General and an Exchequer and Audit Department to provide supporting staff from within the civil service.

The C&AG was given two main functions; to authorise the issue of public money to government from the Bank of England, having satisfied himself that this was within the limits Parliament had voted, and to audit the accounts of all Government departments and report to Parliament accordingly.

Gladstone also created the Public Accounts Committee.



William Ewart Gladstone

² Audit Scotland... <http://www.audit-scotland.gov.uk/>

³ Auditor General for Wales... <http://www.agw.wales.gov.uk/>

⁴ Northern Ireland Audit Office... <http://www.niauditoffice.gov.uk/>

The Three E's

Under the 1983 Act, the C&AG can examine and report on the economy, efficiency, and effectiveness of public spending. We use the following definitions for the 'three Es':

- **Economy:** minimising the cost of resources used or required - **spending less;**
- **Efficiency:** the relationship between the output from goods or services and the resources to produce them - **spending well;**
- **Effectiveness:** the relationship between the intended and actual results of public spending - **spending wisely.**

Our current role

Under the law, the C&AG and the NAO are responsible for auditing the accounts of all Government departments and agencies, and reporting the results to Parliament. The C&AG also audits over half of the 'arms-length' public bodies (also known as *non-Departmental public bodies*), all National Loans Fund accounts, and several international clients, who we win in open competition against other auditors. Currently, we audit over 600 accounts covering some £298 billion of expenditure; £29 billion of income; £336 billion in tax revenue; fixed assets worth £203 billion; and long-term liabilities of £37 billion.

The C&AG is required to form an opinion as to whether audited accounts are free from material misstatements and that the transactions they contain have appropriate Parliamentary authority. He will issue a qualified

opinion where material misstatements are identified, but where this is not the case, may still report to Parliament on other significant matters. Even where no report is made, we often write to our clients suggesting ways they could improve their systems; such "management letters" often lead to significant changes.

In addition to financial audit, the C&AG presents around 50 reports to Parliament each year on the value for money obtained by Government departments and other public bodies. In the last 3 years, savings resulting from our work have amounted to £1.46 billion, £487 million each year.

Our value for money work covers a wide range of topics, ranging from examining the entire operation of the criminal justice system to major defence procurement projects and the administration of agricultural schemes funded by the European Union. We identify the topics for examination by carefully monitoring and analysing the risks to value for money across the full range of our responsibilities, and in undertaking reviews, we use staff with a wide range of professional expertise, including external consultants where necessary.

Auditing information technology

IT provides many opportunities to deliver better services to citizens. It also has considerable potential to improve the efficiency of government organisations in all aspects of their business. Achieving Information Age Government is central to the UK's modernisation programme, but for this to become a reality, citizens must have confidence in departments' IT systems in terms of their reliability and the protection of personal information.

We support the development of Information Age Government through our examinations of the implementation of IT projects and of the reliability of IT systems. Here, our work has revealed that complex IT projects often encounter serious problems, resulting in delays and the disruption of e-Government services. We have sought to promote improvements by drawing out the lessons learned so that poor performance is not repeated.

Other subjects that our IT-related value for money reports have touched on include information security management; software licensing; identifying and tracking livestock (essentially about information management); and on-line learning (essentially about fraud control).

Information and communications technology in support

The 1970s saw us getting to grips with the technical aspects of computers. Some of our more adventurous colleagues acquired the skills necessary to extract information from the payroll, bill paying and stores inventory systems that were then emerging during our government's first wave of computerisation. This was the punched card/mainframe era, and extracting information from these early systems required a good knowledge of data storage techniques, programming skills (that often extended to a need for assembly language), much ingenuity - and hours of card-punching!

Things remained much at this level until the 1990s, when the first of the powerful and truly portable (rather than 'transportable') PCs - plus software tools to match - arrived to lift audit computing out of the realm of the technical

specialist and place it firmly within everyone's grasp. Today, all our professional staff are allocated a modern laptop PC with which to access our corporate systems - remotely if necessary - to exchange e-mail and other documents, and to search the World Wide Web. We continue to maintain technical support teams to support our financial and value for money auditors in the more difficult tasks, but audit computing now lives very much on the auditor's laptop.

Good software can make an important contribution to the various stages of audit, particularly in collecting, sorting, analysing and interpreting data, and in presenting the results. Each of our laptops carries a comprehensive software toolkit comprising Microsoft Office XP, IDEA and TeamMate, and staff receive in-house training in their use. In addition, our technical support teams are equipped with specialist software packages for designing questionnaires, analysing survey results, providing statistical analysis, etc.

The 1990s saw our original local area network, which provided internal e-mail, text-based word-processing and spreadsheet, and rudimentary search facilities. Our second-generation Intranet system, "Merlin", began to roll out in 1998, and what an improvement it was! Merlin provides us with access to our internal databases, with external e-mail, with access to information held on the UK Government Intranet and, via the Internet, to information held on the World Wide Web. Merlin is an object lesson on how a business can come to depend on good information and communications technology - we would be lost without it! For this reason we devote considerable resources to IT service management, where we model our management processes on BS

Many of the value for money reports we publish focus on government's use of IT. Recent examples include:

e-Accessibility: older people are major users of public services but, as a section of society, are far less likely to access those services electronically. However, these e-services are potentially a great boon to older people, many of whom have mobility problems, have difficulty in gaining access to sources of information, live alone or want to remain independent and involved. If government is to take full advantage of the potential of technology, it must make sure its e-services are accessible to all and work to avoid a 'digital divide'...

...http://www.nao.gov.uk/publications/nao_reports/02-03/0203428.pdf

The Libra Project: described by the Chairman of the Public Accounts Committee as "one of the worst IT projects ever seen", Libra was intended to provide our magistrates' courts with a standard computer support system. By 2003, the initial project budget, set at £146M in 1998, had rocketed to £318M with reduced functionality...

...http://www.nao.gov.uk/publications/nao_reports/02-03/0203327.pdf

Tax Credits: the Inland Revenue introduced new tax credits, but the systems did not work as intended, causing major problems for claimants, employers and the Department. There were serious problems with system performance, which affected stability (staff could not complete the processing of claims and had to start again); speed (staff had to wait too long to access information and records); and availability (significant time in the working day was lost when the system was closed down to clear internal queues)...

...http://www.nao.gov.uk/publications/nao_reports/02-03/02031072.pdf

Government Communications Headquarters: houses one of Europe's largest computer complexes and its new accommodation exhibits radical differences from most office building projects. To sustain the flow of vital intelligence to the Government, GCHQ retained responsibility for moving its technical capability into the new building. In doing so, GCHQ failed initially to consider all the implications of the move. As a result estimates for the technical move increased more than ten fold from £40M to £450M...

...http://www.nao.gov.uk/publications/nao_reports/02-03/0203955.pdf

Government Call Centres: can provide services and information in a way that is convenient and cost effective. Most of the public tell us that they are willing to use them and are mostly satisfied with the service received. However, there is room for improvement. In particular, call centres need to collect full and reliable information about their services, and departments need to ensure that efficiency and quality are delivered...

...http://www.nao.gov.uk/publications/nao_reports/02-03/0203134.pdf

You can find information about our work in progress, including contact details on our website at...

<http://www.nao.gov.uk/publications/workinprogress/index.htm>



Teamate

.. is an electronic documentation package marketed by *PriceWaterhouse Coopers*. It's easily customised to individual needs and does not prescribe a particular way of performing an audit. Its main benefits are that it:

- stores and references audit working papers electronically;
- makes for easier and more timely review of audit work. The package highlights important issues, and their review does not have to wait until the paper file is in your hand. Many staff can work on the audit at the same time and at different locations;
- generates reports easily and quickly, and allows them to be customised to meet individual client requirements;
- makes for better management of audits by identifying completed tests (and also those that should be complete, but are not!); following audit by rolling forward one year's audit to the next.

TeamMate also provides the opportunity to embed and enhance underlying methodologies, thus providing consistent minimum standards across all audit work.

IDEA is a comprehensive file interrogation tool for auditors that can be used to...

- Import data from a wide range of file types
- Perform analyses of data including comprehensive statistics, profiles, summaries and ageing
- Conduct exception tests of unusual or strange items using simple or complex criteria. IDEA has 103 built-in special functions as well as normal arithmetic capabilities
- Perform calculations
- Test for missing or duplicate items
- Select samples using systematic, random or monetary unit techniques
- Match or compare different data sources

Helping the nation spend wisely

The UK National Audit Office scrutinises public spending on behalf of Parliament.

The Comptroller and Auditor General, Sir John Bourn, is an Officer of the House of Commons. He is the head of the National Audit Office, which is based in London (with regional offices in Cardiff, Newcastle, and Blackpool) and employs some 800 staff. He, and the National Audit Office, are totally independent of Government. He certifies the accounts of all Government departments and a wide range of other public sector bodies; and he has statutory authority to report to Parliament on the economy, efficiency, and effectiveness with which departments and other bodies have used their resources.

Our work saves the taxpayer millions of pounds every year.

At least £8 for every £1 spent running the Office.

15000⁵, and to the management of information security. And under the latter heading, we are currently using government-approved specialists to carry out "penetration testing" of our network to provide positive evidence of effective security.

Our IT Strategy will continue to evolve with technological development. The main thrust of future developments is to improve audit efficiency through improved audit support tools, remote working, and knowledge management, and to providing wider access to

information by staff and more efficient administrative support. Our medium term (3-5 year) vision is to enable staff to work efficiently at client sites for much longer periods, with access to the full range of resources available to staff at NAO offices. Currently we use dial-up for remote access, but are looking to exploit broadband technology further as it becomes more widely available.

Overall, ICT has come to play a vital support role in achieving our corporate vision of "Helping the Nation Spend Wisely".

⁵ BS 15000 is the first worldwide standard specifically aimed at IT Service Management. It describes an integrated set of management processes for the effective delivery of services to the business and its customers.

The INTOSAI IT Audit Committee

INTOSAI celebrated its 50th anniversary last year. It has grown from a small group of 34 supreme audit institutions (SAIs) that met in Cuba in 1953 to become the voice of the worldwide SAI community. Its nearly 190 members represent a wide spectrum of audit institutions working in many different ways to provide their parliaments and citizens with an effective audit of public finances. INTOSAI, as an apolitical international institution working for the mutual

The International Training Course

Since 1993 the National Audit Office (NAO) has offered staff from overseas SAIs the opportunity to participate in an annual audit training course in London (usually in September). To date staff from many countries have participated in the course, which includes intensive training in the National Audit Office's methodologies for both Financial audit and Value for Money work. The training approach is classroom based but both modules include practical illustrations, examples and case studies drawn from accounts audited and value for money studies carried out by the NAO. The course aims to be interactive and participants are encouraged to question and introduce elements from their own experience. Extensive course notes, booklets and reference materials are provided for the participants retention and future reference.

Course applications are available on our web site...

http://www.nao.gov.uk/conferences/international_training_application.pdf



SIR JOHN BOURN
COMPTROLLER AND AUDITOR GENERAL
NATIONAL AUDIT OFFICE OF THE UNITED KINGDOM

Sir John Bourn has been Comptroller and Auditor General of the United Kingdom since 1988 and, as well, Auditor General of Wales since 1999. He was educated at the London School of Economics, where he took the BSc (Economics) degree and a PhD. He has worked in several government departments, including the Treasury, the Northern Ireland Office and at the Civil Service College. Before his present appointment, he was Deputy Under Secretary of State for Defence Procurement at the Ministry of Defence. Sir John sits on the Financial Reporting Council of the United Kingdom, is a member of the UK's Financial Review Panel and a Member of the Panel of External Auditors of the United Nations.

Sir John is a Visiting Professor at the London School of Economics.

exchange of ideas on best practice, is without parallel anywhere else in the public sector.

Recent years have seen a substantial growth in bilateral and multilateral cooperation among SAIs. Increasingly, SAIs recognise the need to learn from each other if they are to keep pace with the rapid changes in public sector management, accounting and auditing standards, and expectations of the role of public auditors. Many formal and informal structures have been developed by SAIs to identify and promote good practice and to tackle issues that cross national boundaries. Among these, the INTOSAI IT Audit Committee is extremely active, with a regular programme of liaison meetings and IT seminars hosted by member countries. Members also collaborate in the development of training and guidance material, our current programme including the development of a range of guidance on auditing electronic government and on electronic records management.

The UK NAO plays an enthusiastic role in these activities. We host the INTOSAI IT Audit Committee web site (<http://www.intosaiitaudit.org>), which offers both our members and the world at large a range of training and guidance material on various aspects of IT audit, while other areas of the site catalogue material useful to the IT auditor that can be found on SAI's, state auditor's, and government web sites. The UK is also a member of the INTOSAI Governing Board and chairs the INTOSAI working group on the audit of privatisation and regulation. Oh! - we also publish this magazine.

During 2003, 600 representatives from 70 countries visited our office. In turn, we sent more than 50 NAO staff abroad on short-term assignments ranging from a few days to several months. We often enrich our projects with expertise drawn from across the UK and beyond.

You can manage what you know about; it's what you don't know about that creeps up and stabs you. For the IT manager, computer hacking is one such sword of Damocles for which sensible preventive and detective measures have become essential. And in common with other disasters in waiting, infiltration should feature in contingency planning.

For the benefit of those readers unfamiliar with computer hacking, N. Nagarajan of the Office of the Comptroller and Auditor General of India gives an overview and explains some of the terms associated with it.

The hacker

Technically, a "hacker" is someone who is enthusiastic about computer programming and all things computer related, and is motivated by curiosity to reverse engineer software and to explore.



**Not knowing
what you do
not know**

The basics of protecting against computer hacking

The term "cracker", on the other hand, describes those who apply hacking skills to gain *unauthorised* access to a computer facility, often with sinister motives. But "cracking" never really caught on, perhaps due to the grey area that exists between the two activities and to the media's widespread use of "hacking" as a term synonymous with computer crime. I will not therefore try to buck the trend in this article.

Computer hacking

Hacking is in some ways the online equivalent to burglary; in other words *breaking into* premises against the wishes of the lawful owner - in some jurisdictions a crime in itself - from which other criminal acts such as theft and/or damage generally result.

Computer hacking refers to gaining *unauthorised* access to, and hence some measure of control over, a computer facility, and most countries now have specific legislation in place to deter those who might wish to practice this art and science. In some jurisdictions, unauthorised access alone constitutes a criminal offence, even if the hacker attempts nothing further. However, in practice, hackers generally have a particular target in mind, so their unauthorised access leads to further acts, which national law might also define as criminal activities. These can be summarised under the headings of unauthorised:

- **obtaining of confidential information:** perhaps the major growth area in computer crime is "identity theft", in other words the obtaining of personal information that can then be used to commit other serious offences, usually in

the area of fraud. However, other motives include espionage (both governmental and commercial secrets) and the obtaining of personally sensitive information that might be used for tracing people, deception and blackmail;

- **alteration or deletion of data and code:** most organisations now depend to some extent on computerised information systems, and any act resulting in significant corruption or deletion of corporate data could have serious implications on their ability to transact business;
 - **degradation or cessation of service:** acts that result in systems being unable to carry their workload or that fail altogether, could also have serious business implications;
 - **use of computer resources:** this impact is really inherent in the previous three, but it's worth mentioning separately because an emerging problem is the use by hackers of other people's systems (extending to home PCs) to store illegally obtained data or to mount attacks on other systems. There are documented cases of systems hacked in this way - sometimes referred to as "zombies" because they are no longer in the full control of their unsuspecting owners - being used to store child pornography and material that breaches copyright law (e.g. copyrighted music files), to mount distributed denial of service attacks on other systems, and to distribute spam e-mail.
- Finally, it's worth emphasising that the term "hacker" applies both to outsiders and to otherwise authorised personnel who misuse their system privileges, or who impersonate higher privileged users. This sad fact needs to be recognised when formulating corporate security policy.

The Ten Immutable Laws of Security

- 1 If a bad guy can persuade you to run his program on your computer, it's not your computer anymore.
- 2 If a bad guy can alter the operating system on your computer, it's not your computer anymore.
- 3 If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.
- 4 If you allow a bad guy to upload programs to your web site, it's not your web site any more.
- 5 Weak passwords trump strong security.
- 6 A machine is only as secure as the administrator is trustworthy.
- 7 Encrypted data is only as secure as the decryption key.
- 8 An out of date virus scanner is only marginally better than no virus scanner at all.
- 9 Absolute anonymity isn't practical, in real life or on the web.
- 10 Technology is not a panacea.

Source - www.microsoft.com/technet

Just another security update for Microsoft Internet Explorer

Are You on a Network?

If your computer is part of a managed network, contact your organization's system administrator before making changes to your computer.

Why We Are Issuing This Update

A number of security issues have been identified in Microsoft® Internet Explorer that could allow an attacker to compromise a Microsoft Windows®-based system and then take a variety of actions. For example, an attacker could run programs on a computer used to view the attacker's Web site. This vulnerability affects computers that have Internet Explorer installed. (You do not have to be using Internet Explorer as your Web browser to be affected by this issue.) You can help protect your computer by installing this update from Microsoft.

Source - Microsoft Security Bulletin MS03-032

Approaches to hacking

There are several basic strategies for hacking a computer facility: physical intrusion; password attacks; network access; web server attacks; and e-mail attacks, but there are a multitude of tactics that can be used to implement them. For example, security flaws (or design

weaknesses) in infrastructure software and communications protocols offer seemingly endless tactical possibilities, as is evidenced in the never-ending stream of security updates (see example).

Physical intrusion: an attacker's work is made easier by gaining physical access to a machine's keyboard or to network junction boxes. Physical access opens up such possibilities as

installing a keystroke logger¹; installing unauthorised hardware devices (e.g. linking a modem that bypasses the corporate firewalls to the network); tapping junction boxes through which network traffic might be analysed; gaining access to system documentation, printouts and to written notes of their passwords left by reckless users. Even access to confi-

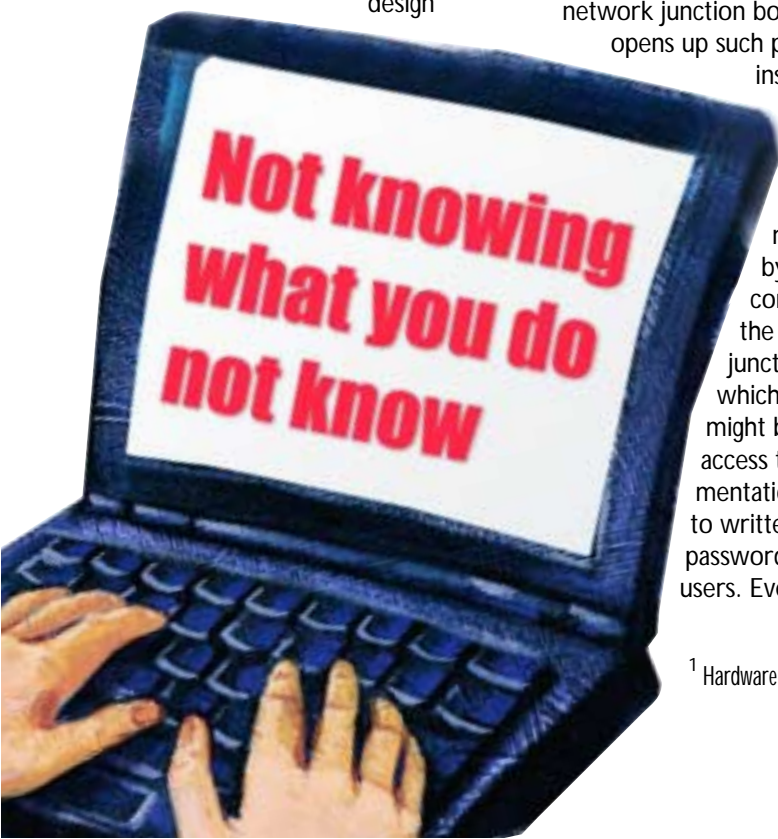
dential waste can prove fruitful.

Perhaps the quickest and easiest way to gain physical access to an organisation's computer facilities is to join the contract cleaning force, which often works unsupervised and outside normal office hours.

Password attacks: obtain a valid password to the system and you become just another legitimate user. This is particularly dangerous where the hacked account has special privileges assigned to it that permit wide-ranging system access and use. A successful password attack is both difficult to detect and difficult to prevent because password security depends largely on the user. Keystroke loggers and social engineering (see terminology below) are methods of capturing passwords, while people often share their personal passwords with others, write them on notes that they attach to their terminals, and fail to change them periodically. Password cracking programs perform an elaborate process of guessing 'weak' passwords by trial and error, using combinations of words from different languages, names (places, people, characters in books), jargon, slang, and acronyms. These are tried backwards, in two-word combinations, in combinations with numbers substituted for letters, etc. Vendors often ship infrastructure software with the administrator account passwords set to default values; because these are widely known in the hacking community, they provide an easy route into a computer facility if left unchanged.

Network Access and Web Server Attacks: computers forming part of a local area network that is in turn

¹ Hardware or software that captures the user's keystrokes, including their passwords.





connected to the Internet are exposed to a range of potential logical access risks. A network's primary purpose is to permit users to access resources and exchange information, but hackers can also use the network for the same purpose. There are different ways to achieve unauthorised access under this heading, many being technically sophisticated. One set of approaches exploits features of networking software that make it accessible from outside the network. Another set exploits browsers; for example, browsers maintain or have access to information about the user and computer that a hacker can exploit. A hacker could also cause a browser to launch an "applet" (a program that runs in conjunction with the browser) to hack the computer or network, or to send back information that is not normally accessible from outside. Once access is gained, "island hopping" through the network is sometimes possible by exploiting trusted relationships between interconnected computers - *the fact is that a network of computers that trust each other is only as secure as its weakest link.*

The basic solutions to this family of security risks are to keep abreast of vendor security updates - such as the Microsoft example illustrated - and to maintain an effective "firewall"².

Email Attacks: e-mail is a major route into networked computers. Typically, a Trojan horse program is buried within an innocuous-looking attachment to an e-mail message (see the *Autorooter* example). The Trojan is launched when the attachment is opened (or sometimes viewed) and covertly passes control of the computer to the hacker.

² A combination of hardware and software that limits external access to networked computers and resource.

³ The least level of privilege consistent with performing a particular role.

Managing common vulnerabilities

A compromised system can be a self-inflicted injury due simply to the basic precautions having being ignored:

- ensure that your computer has good physical security, consistent with both its value in terms of replacement cost and the consequences that could stem from its data being disclosed or destroyed. Secure sensitive areas; manage access keys; consider installing intruder alarms. Ensure communications junction boxes are secured and inspect them periodically for signs of tampering - network administration packages can detect unauthorised physical devices connected to the network. Provide a secure waste disposal service for computer printouts and removable media;
- formulate a sensible password policy for authenticating users and *enforce it*. Consider the need to strengthen password authentication with tokens or biometrics. Disable unnecessary services and accounts promptly;
- systems administrators occupy positions of extreme trust; it follows that they should themselves be trustworthy. Be very careful who you permit to have system administrator-level access to your network particularly when hiring new staff or appointing people to cover for absences. Consider implementing a policy of "least privilege"³ and review periodically the privileges that have been allocated, to whom and for what purpose;
- infrastructure software - in particular the operating system and firewalls - generates logs that record who is using (or attempting to use) the system, for what purpose and when. This information can prove vital in detecting unauthorised activity - for example, attempted access to particularly sensitive accounts or files - and system use at unusual times. Logs should be reviewed frequently - it may be necessary to develop or purchase a log monitoring and analysis package to enable key system messages to be detected quickly. An unplanned increase in

Autorooter

...a Trojan horse, potentially spread by e-mail, which exploits a Windows vulnerability to allow a hacker to gain control of infected computers.

This DCOM-RPC exploit only affects Windows XP/2000 Pro/NT computers, which can use Remote Procedure Call. As the Trojan is incapable of spreading by itself, the file reaches computers through infected e-mail messages, inside files downloaded from the Internet or even on floppy disks.

When run, Autorooter creates files, including RPC.EXE, which exploit the operating system vulnerability by opening communication port 57005 and logging on with the same privileges as the computer's user. It also downloads a file called LOLX.EXE, which opens a backdoor in the computer. After that, the infected computer is at the mercy of the hacker who can gain remote control through the port created.

Because it doesn't show any messages or warnings that may indicate that it has reached the computer, Autorooter is difficult to recognise.

disc storage, slower than expected network performance and suspicious-looking outbound connections can be other indicators that you have a cuckoo in the nest;

- make sure that your system files (including the Registry) are well protected from unauthorised change. Apply the principle of least privilege to limit what users are able to do. Implement a change control procedure to ensure at least two people are involved in important system changes and that all changes are recorded. Periodically audit your system software for unauthorised executables;
- never run or download software from an untrusted source (the source from which it was obtained might not be the same as the developer). If you run a web site, you should control closely what visitors can do; in particular, you should only permit programs on the site that you obtained from a trusted developer;
- typically, a new virus or Trojan does the greatest amount of damage early in its life when few people are able to detect it. Thus, an out of date virus scanner is only marginally better than no virus scanner. New viruses and Trojans are created virtually every day, so it's vital to keep your scanner's signature file up to date - virtually every vendor provides a means to obtain free updated signature files from their web site.

When you're satisfied that the basics are both in place and operating, why not consider hiring a reputable firm of security specialists to undertake a "penetration testing" programme to assess the extent to which your scheme of control rests on solid foundations rather than on sand?

It's vital to appreciate that:

- security consists of both technology and policy; that is, it's the combination of the technology and how you use it that ultimately determines how secure your systems are;
- security is journey, not a destination. It's not a problem that can be "solved" once and for all, but a continual series of moves and countermoves between the good guys and the bad guys;
- the key is to ensure that you have good security awareness, appropriate security policies (*that you enforce*), and that you exercise sound judgment.

Planning for hacking incidents

So, you discover that your system has been hacked. What next? Well, first it's necessary to backtrack and consider planning for this possibility. Sit down with colleagues and write down a strategy to guide your response, exactly as you would for any other aspect of contingency planning. Who will form your incident response team? What are your goals going to be and in what order of priority? In most cases they are likely to be first, to prevent further intrusion, then to identify the vulnerabilities that led to the attack, assess the damage and consider what remedial action needs to be taken (e.g. what would you do were you to suspect identity theft?). Will you assign resources to identifying the intruder? Will you involve the police?

One of the first points to consider is whether to disconnect from your external networks to limit damage and prevent further infiltration to other trusted networks. Assuming the attack is external, remaining connected may leave the hacker able to observe and negate the response team's actions. Organisations that have reliable (i.e.

successfully tested) disaster recovery arrangements in place may find it comparatively easy to transfer their key operations to a disaster recovery site while they thoroughly investigate and sanitise their home site.

You should consider the extent to which you back up your firewall and other significant logs. Assuming the vulnerability that gave rise to the attack is not apparent, you may need to look back, perhaps weeks, to identify when and how the intrusion occurred (another plus in favour of frequent log reviews). Furthermore, should events finish up in the hands of the police, the police are likely to need the evidence contained in your logs to support a prosecution.

You will also need to consider who to inform when you discover the problem. This will involve striking a balance between those who need to be involved in the investigation, top management - but only when you have concrete proposals to make to them - and everyone else, at least until the evidence has been preserved.

Investigation needs to be thorough; focusing on a single vulnerability before restoring service might overlook the existence of backdoors that the hacker has inserted to enable easy re-entry later. A thorough investigation will involve advanced networking techniques, adeptness with software tools, system administration, data/system recovery, technical skills that might not be at your immediate disposal. Thus, it might be prudent in

The hackers' hit parade

Security firm Qualys produces a real-time index of the vulnerabilities that are the current favourites of the Internet's computer hacking community. You can obtain details of each vulnerability by clicking on each entry in the 'ID' column of the vulnerability table.

<http://www.qualys.com/services/threats/current.html>

Responding to intrusions

- understand the extent and source of an intrusion;
- protect sensitive data contained on systems;
- protect the systems, the networks and their ability to continue operating as intended;
- recover systems;
- collect information to better understand what happened. Without such information, you may inadvertently take actions that can further damage your systems;
- support legal investigations.

Source: www.cert.org

your planning to identify reputable security specialists well versed in penetration testing that might be called upon to assist with sanitising and rebuilding your systems.

In addition to identifying the system vulnerabilities exploited by the hacker, a critical review and reconciliation of activated accounts (particularly those of guests, supposedly disabled accounts and those whose presence can't be explained) and their associated system privileges, while tedious, could reveal other unused entry points the hacker has set up against a rainy day; likewise, you should confirm the status of all interconnected 'trusted' systems.

Scan the system for Trojans. These are typically identified by antivirus packages, but their scan engines have varying degrees of success, particularly if not up-to-date, so scan using (up-to-date versions of) several packages.

Note: there is more information on incident response at...

<http://www.cert.org/security-improvement/modules/m06.html>

Conclusion

In the context of computer hacking, *knowing what you do not know* is manageable, hence the importance of good preventive and detective measures, such as log review and intrusion detection systems. The less fortunate are those who remain in self-inflicted ignorance - maybe for weeks or months - that their system has been infiltrated and their business is being damaged.

Regardless of the strength of your preventive and detective measures, *be prepared for hacking incidents*, particularly if your organisation relies heavily on networks (the Internet, WANs and LANs) for its operations and customer services. Should you fall victim, a thorough investigation of a compromised system - while disruptive, time-consuming, expensive, and tedious - is essential. The temptation is to give in to pressure to resume operations quickly by closing the obvious vulnerabilities and trusting to luck that the system is clean. That could easily be a false economy.

Some terminology

Buffer overflows - are due partly to a characteristic of some programming languages, such as C, which poor programming practices then exacerbate. An overflow occurs when a program attempts to store more data in temporary storage area, or "buffer", than it can hold. Since buffers are of finite size, the extra information overflows into adjacent buffers thereby corrupting or overwriting the valid data held in them. This would normally cause a program failure or even a system crash, but a skilfully crafted overflow can also be exploited as a form of security attack. The attacker can gain control by creating an overflow containing code designed to send new instructions to the attacked computer, hence the relevance of buffer overflows to hacking.

Firewall - the online equivalent of the 'man on the door' who, when a visitor arrives in the foyer, asks for proof of identity, checks the appointments book, contacts the host, issues a temporary pass and perhaps inspects the visitor's baggage before permitting - or denying - entry.

A network firewall sits at the junction point or gateway between two networks - usually a private network and a public network such as the Internet - its purpose being to reduce the risk to networked computers of intrusion. It may be a hardware device or software running on a secure host computer. In either case, a firewall has at least two network interfaces, one for the network it is protecting and one for the untrusted network to which it is exposed. Because firewalls cannot decide for themselves whether traffic is hostile or benign, they must be programmed with rules (a "security policy") that govern the types of traffic to allow or deny.

In addition to guarding external connections, firewalls are also sometimes used internally to provide additional security by segregating sub-network that give access to highly sensitive applications.

Honey Pots - decoy servers or systems designed to gather information about attackers. A honey pot, which is set up to be easier prey for attackers than genuine production systems, incorporates modifications that enable intruders' activities to be logged and traced. The theory is that when an intruder breaks into a system, they will return. During subsequent visits, additional information can be gathered and additional attempts at file, security, and system access on the Honey Pot can be monitored and saved. Most firewalls can be configured to alert system administrators when they detect traffic entering or leaving a honey pot.

Identity theft - involves taking over an individual's identity by stealing critical private information, such as the Social Security number, driver's license

Example of a buffer overflow vulnerability

The Phone Book Service that runs on Internet Information Services (IIS) 5.0 has an unchecked buffer (a temporary data storage area that has a limited capacity but no specification for the amount of information that can be written into it) in the code that processes requests for phone book updates. A specifically malformed HTTP request from a malicious user can cause a buffer overflow in the Phone Book Service, which might allow the malicious user to run unauthorized code on the server, or cause the service to fail.

Source: extract from a Microsoft security update.

number, address, credit card number, or bank account number. The identity thief can then use the stolen information to obtain loans or credit lines to buy goods and services under the stolen name. Identity thieves typically change the consumer's mailing address to hide their activities.

Intrusion detection - the art and science of detecting when a computer or network is being used inappropriately or without authority. An ID system monitors system and network

resources and activities and, using information gathered from these sources, alerts system administrators on identifying possible intrusion.

Firewalls (see above) work only at a network's point of entry with packets as they enter and leave the network. An attacker that has breached the firewall can roam at will through a network - this is where an ID system becomes important.

Intrusion Prevention - systems monitor for suspicious activity with the aim of proactively blocking potential attacks. Typically, an IP system comprises a software agent that resides near to the host's operating system kernel, which monitors system calls before they reach the kernel using a rules engine to identify potentially suspicious activity. This can then be halted, or the systems administrator alerted. A drawback is that IP systems can respond to legitimate activities and generate false alarms. Defining exceptions can reduce such false alarms, but there are pros and cons to this.

Keystroke logger (or keylogger) - is a program that runs in the background recording all keystrokes. Once logged, the keystrokes are returned to the hacker who peruses them carefully to identify passwords and other useful information that could be used to

compromise the system, or be used in a social engineering attack. For example, a keylogger will reveal the contents of all e-mail composed by the user. Keylogger programs are commonly included in rootkits and remote administration Trojans. A keystroke logger can also take the form of a hardware device, independent of the operating system, which plugs in between the keyboard and the main system (for PCs). They simply record what is typed at the keyboard; the hacker can later retrieve the device and examine its contents.

Phishing - occurs when a consumer receives a deceptively legitimate looking e-mail from what appears to be a reputable company (see Spoofing). The e-mail might ask a recipient to, for example, update their credit card information, and/or provide other personal details to avoid their account being terminated. Another approach is for the sender of the message to offer a service, for example to protect their credit cards from possible fraud. Those stung by phishing are victims of "identity theft" (see above).

Attempted identity theft

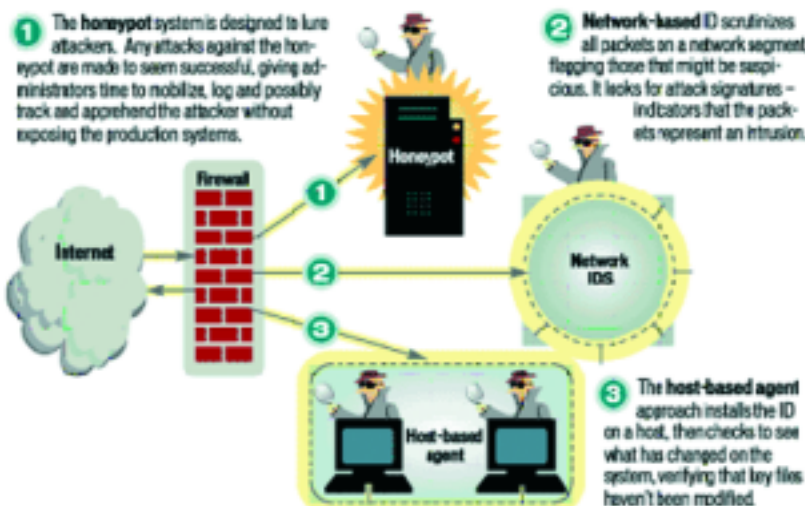
National Australia Bank customers became targets for an e-mail fraud in which they were sent (grammatically incorrect) requests, purportedly from the bank, requesting them to connect to the NAB web site.

"Dear valued customer," it read, "Our new security system will help you to avoid frequently fraud transactions and to keep your investments in safety." The e-mail encouraged recipients to click a link in the body of the message, which then connected them to a site that mimicked the NAB Web site but that had been set up to capture their login and password details.

The scam used a message previously used to targeted other banks' customers.

Intrusion-Detection Systems

ID stands for intrusion detection, which is the art of detecting inappropriate, incorrect or anomalous activity. ID systems that operate on a host to detect malicious activity are called host-based ID systems. ID systems that operate on network data flows are called network-based ID systems. These two systems can be used in conjunction with each other.



Rootkit - a collection of tools and utilities that a hacker can use to hide their presence and gather data to help them further infiltrate a network. Typically, a rootkit includes tools to log keystrokes (see keylogger above), create secret backdoor entrances to the system, monitor packets on the network to gain information, and alter system log files and administrative tools to prevent detection.

Social engineering - in his book, *The Art of Deception: Controlling the Human Element of Security*⁴, arch hacker Kevin Mitnick poses the question: why bother attacking technology when the weakest link lies not in the computer hardware or software, but in humans who can be tricked into giving up their passwords and other secrets? Mitnick goes on to state that social engineering "uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. The social engineer is able to take advantage of people to obtain information with or without the use of technology."

⁴ Wiley, ISBN 0-471-23712-4

Spoofing - in essence a technique that depends on forging the identity of someone or something else ("masquerading"), the aim being to alter the trust relationship between the parties to a transaction.

In the online world, there are different flavours of spoofing. A hacker might employ sophisticated e-mail spoofing to make it appear that an e-mail requiring the victim to confirm their account details, including such information as their logon ID and password, has been sent by a reputable person or organisation (see "phishing" and "social engineering" above).

IP spoofing is another common form of online camouflage, in which a hacker attempts to gain unauthorised access to a computer or network by making it appear that a packet has come from a trusted machine by spoofing its unique Internet IP address. A countermeasure is to use of a Virtual Private Network (VPN) protocol, a method that involves encrypting the data in each packet as well as the source address using encryption keys that a potential attacker doesn't have. The VPN software or firmware decrypts the packet and source address, and performs a checksum. The packet is discarded if either the data or the source address has been tampered with.

Trojan horse - a name derived from the classic Trojan horse in Homer's Iliad. After spending many months unsuccessfully besieging the fortified city of Troy, the Greeks evolved a strategy. They departed leaving behind them as a gift a large wooden horse, which the citizens of Troy brought into town. Unknown to them the horse contained Greek warriors, who at night jumped out and opened the city gates letting in the Greek army who had been in hiding.

In the IT environment - and setting aside the legitimate use of network administration tools - Trojans are generally considered a class of "malware" that, like their predecessor, contain covert functionality. They act as a means of entering a target computer undetected and then allowing a remote hacker unrestricted access and control. They generally incorporate a rootkit (see above).



About the author

N. Nagarajan CISA joined the Office of the Comptroller and Auditor General of India in 1989, and is presently employed as Senior Deputy Accountant General in Mumbai. In addition to his wide experience in auditing IT (particularly in the field of Electronic Data Interchange) and in training staff in IT audit skills, Nararajan has also worked as a developer of pensions systems.

Nagarajan's international work includes audit assignments at the United Nations in New York, and a two year secondment to the Office of the Auditor General of Mauritius where he was involved in training staff and in the audit of EDI systems operated by the Customs department. Nagarajan has been published in a number of international journals.



State of North Carolina



Office of the State Auditor:

INFORMATION SECURITY VULNERABILITY ASSESSMENT

The State Auditor of North Carolina supervised a penetration test on 22 of the state's network security systems - in 21 cases the test team were able to take control of the target computers using programs that are readily available to hackers and the public.

This article describes the approach to testing taken by the Office of the State Auditor. The full audit report can be downloaded from the State Auditor's web site at...

<http://www.osa.state.nc.us>

Overview

In a series of projects to evaluate the network and computer security in place within selected areas of state government, contractors employed by the Office of the State Auditor (OSA) attempted to penetrate the network security systems at 22 of the State's computer systems. The outcome was



"Capitol Building, Raleigh"

that security engineers gained control of computers in 21 of the target systems using programs that are readily available to hackers and the public.

To further assist agencies achieve a "best practice" level of information security over their internal systems, data and assets, we performed a comprehensive information security assessment at the Dept of Revenue, Dept of Treasurer, Office of the State Controller, and Dept of Health and Human Services. While our assessments identified well-defined and effective security controls, we also identified several areas that posed extreme security risks and exposed the agency concerned to possible internal or external attack. We classified control weaknesses as *High*, *Medium*, or *Low* in relation to the level of risk, and on this basis concluded that the overall risk that the agency or state network could be compromised was *High*.

Phase I - preliminary state-wide assessment

Our assessment determined that the State's systems were at high risk for Internet-based attacks. We subjected the twenty two agencies that hosted the critical information systems for the Executive, Legislative, and Judicial branches of state government to an External Network Penetration Test. This was broken down into four separate phases:

Phase 1 - intelligence gathering: using common communications protocols and applications, our security engineers determined what information was available to the general public regarding the State's network. This information was then reviewed to determine whether it offered potential intruders an adequate view of the network infrastructure from which they could develop a network blueprint.

North Carolina Office of the State Auditor

The State Auditor is a member of the Council of State and is elected by the voters of North Carolina every four years. Under the State's Constitution and General Statutes the State Auditor is responsible for conducting and coordinating audits of state agencies and programs supported by state funds. The audits conducted by the Office of the State Auditor include financial and compliance audits on state agencies including community colleges, the Clerks of Superior Court, and the Smart Start partnerships; performance audits to evaluate the effectiveness and efficiency of state agencies and programs; information systems audits on the state's data processing systems; and special reviews to investigate allegations of fraud, waste, or abuse in the state supported agencies or programs.

Phase 2 - active reconnaissance: our security engineers used a combination of "hacker" utilities along with the contractor's internally developed audit tools to identify specific hosts and services that were accessible from the Internet. This resulted in a partial list of accessible hosts and a list of possible services offered.

Phase 3 - attack and toehold: the object of this phase was to gain user level access to (at least) one host in each agency. Using a combination of "hacker" utilities and internally developed auditing tools our security engineers tested the vulnerability of popular services offered on various hosts to undetected, unauthorized access to the State's network. In cases where automated scanners did not determine the nature of a specific service, the engineers connected directly to the service to verify the security issues.

Phase 4 - privilege escalation: our security engineers manually demonstrated their ability to increase their privileges on host sites managed by each Agency in the presence of the Agency Head (or Chief Deputy) and the Information Systems Director. This technique provided a real-time perspective for agency representatives regarding the amount of time required to penetrate their networks and gain

control of proprietary agency information. It also provided an additional buffer for service restoration; should a target machine break down during an attack the responsible individuals could be notified immediately.

Our security engineers succeeded in penetrating 21 of the 22 agencies identified as part of this test. In almost every case they gained full control of an agency computer or device in 30 minutes or less, and in some cases were able to monitor work being carried out while having complete control over the computer. After gaining control they were able to monitor network traffic, capture other user ids and passwords, and launch other attacks that went undetected. However, in one case, due to the vulnerability identified

and exploited being on a device owned by a different agency, our security engineers were unable to complete the attack in the 1 hour and 30 minutes allowed them.

Conclusion

At the time of our testing the security posture of the State's network offered little protection from hacker attacks via the Internet and was therefore at high risk of compromise. Our testing enabled us to provide each agency and Information Technology Services with detailed reports describing the weaknesses we had identified and our recommendations for corrective action. These security enhancements have been acted on.

This comprehensive information security assessment focused on five key areas:

- **Security Policy Assessment**, which evaluates the implementation of security policies and procedures.
- **Network Architecture Assessment**, which is a detailed review of a network design.
- **Network Vulnerability Assessment**, which provides a thorough understanding of security-related weaknesses and exposures in networks.
- **Host Vulnerability Assessment**, which reviews the current security configuration of mainframes and operating systems.
- **Secure Build Review (one agency only)**, which is a security analysis in a non-production environment for the build procedure for a desktop client computer.

Agency	Security Policy Assessment	Network Architecture Assessment	Network Vulnerability Assessment	Host Vulnerability Assessment	Secure Build Review
Dept of Revenue	X	X	X	X	X
Dept of the State Treasurer	X	X	X	X	
Office of the State Controller	X	X	X	X	
Dept of Health and Human Services			X	X	

Risk Levels	Dept of Revenue	Dept of State Treasurer	Office of the State Controller	Dept of Health and Human Services
High	7	5	4	23
Medium	7	6	2	6
Low	5	2	1	3
Overall	Moderate	High	Moderate	High

Phase II - comprehensive vulnerability assessment

Following Phase I, four agencies volunteered to be subjected to a more comprehensive assessment of their production networks. Phase II addressed five key areas: Security Policy Assessment, Network Architecture Assessment, Network Vulnerability Assessment, Host Vulnerability Assessment, and Secure Build Review (Dept of Revenue only).

The table shows the tests we carried out at each agency. These can be summarised as follows (further details are set out in the Annex):

Security Policy Assessment: our objectives here were to:

- **evaluate current security policies and practices:** this involved

reviewing security policy and associated procedures for completeness, accuracy, and appropriateness. We also reviewed current incident response policies and procedures;

- **provide recommendations** based on best practices and knowledge of the client's business objectives and organisational infrastructure.

Network Architecture Assessment: in this stage we focused on the internal network infrastructure, Wide Area Network (WAN) connections to remote locations, and Internet connectivity through the North Carolina Integrated Information Network. We examined the business and technical requirements of the current network infrastructure to ensure a proper balance between functionality, cost, and security.

Network Vulnerability Assessment: having gained an understanding of the network architecture, we assessed network vulnerabilities. We examined the configuration of network devices, firewalls, and public web servers to provide a current view of vulnerabilities and threats. Our assessment consisted of a review of devices owned and maintained by each agency and devices owned and maintained by Information Technology Services.

Host Vulnerability Assessment: the aim in this stage was to provide a current view of threats and vulnerabilities. Our assessment covered the agency's client services and supporting infrastructure, and consisted of a review of a number of hosts owned and maintained by the agency.

Secure Build Review (Dept of Revenue Only): During the Secure Build Review we examined the build process created by the Information Technology group (within the Department of Revenue) for building desktop client computers.

Findings

Our testing uncovered a number of weaknesses at each of the agencies, some being sufficient to permit unauthorised access, data manipulation, or data destruction. We classified each weakness according to its relative risk using the following definitions:

High-level Risk: defined as a vulnerability that could cause grave consequences if not addressed and remedied immediately. This type of vulnerability is evident within the most sensitive portions of the network, as identified by the data owner. This vulnerability could cause network functionality to cease or control of the network to be gained by an intruder;

Medium-level Risk: defined as a vulnerability that should be addressed within the near future. There is urgency in correcting this type of vulnerability; however; this may be either a more difficult exploit to perform or of lesser concern to the data owner;

Low-level Risk: defined as a vulnerability that should be fixed; however, it is unlikely that this vulnerability alone would allow the network to be exploited and/or it is of little consequence to the data owner.

We provided each agency with a detailed report that set out the specific vulnerabilities we had identified together with our recommendations for corrective action. In each of the four agency assessments we also identified vulnerabilities affecting devices controlled by Information Technology Services, and we disclosed these to ITS for corrective action.

The vulnerability assessment performed at the Department of Health and Human Services covered nine of the Department's divisions. Although the results have been consolidated for this article, we evaluated and reported on each division separately.

Next Steps

The four agencies that volunteered to participate in this vulnerability assessment should be commended for their concern for information systems security. The results of these tests will assist both them and ITS to strengthen network security. However, every state government agency should be subject to a thorough vulnerability assessment, with regular follow-ups.

Our participation in these assessments helped the Office of the State Auditor's Information Systems Audit Division to develop the skills and testing expertise to perform these tests in the future. To be successful in these efforts, OSA must acquire the testing software necessary to analyse networks for vulnerabilities, establish testing facilities, and continue to receive specialised training in the latest advances in networks and the related vulnerabilities.

**North Carolina Office
of the State Auditor**

Annex

Further details of our test objectives during "**Phase II - Comprehensive Vulnerability Assessment**" are as follows:

Network Architecture Assessment

This assessment was divided into the following key areas:

- Network Overview;
- Segmentation Model;
- IP Routing;
- Redundancy;
- Encryption;
- Remote Access;
- Network Management;
- Anti-Virus;
- Intrusion Detection Systems;
- Backups;
- Firewalls.

Our key objectives were to:

- interview business and technical representatives to gain a solid understanding of business objectives and requirements;
- review technical requirements for the network;
- review required data flows;
- assess security zones and access controls;
- review at a high level the host and network management strategy;
- review at a high level the enterprise backup strategy;
- review at a high level the enterprise virus strategy;
- identify applicable industry best practices;
- identify and validate security issues of immediate consequence;
- develop long-term recommendations to enhance security;
- transfer knowledge.

Network vulnerability assessment

Our key objectives in this stage were to:

- develop a picture of the network, including topology, devices and hosts, and services for correlation against provided information and documentation;
- assess network device configuration for vulnerabilities or insecure configurations;
- use active probing to assess network security features such as firewall configuration, intrusion detection systems (IDS), and virtual private networks for vulnerabilities or insecure configuration;

- analyse the perimeter firewall's rule set;
- assess the configuration and architecture of directory services;
- assess the mainframe environment's security configuration;
- identify and validate vulnerabilities in network components, and overall architecture;
- identify quick fixes for vulnerabilities;
- develop long-term recommendations to enhance security.

Host vulnerability assessment

The key objectives of this assessment were to:

- assess server configuration (domain controllers, web servers, application servers, database servers) for vulnerabilities or insecure configurations;
- identify and validate vulnerabilities in network and server components, and overall architecture;
- identify quick fixes for vulnerabilities;
- develop long-term recommendations to enhance security.

Secure Build Review (Department of Revenue Only)

The key objectives of this review were to:

- interview technical and business representatives to gain a solid understanding of the demands placed upon the system and how they impact the host;
- review the intended use of the platform to understand requirements and tailor recommendations;
- establish secure build methodology for evaluating the build;
- examine existing hosts in the production environment for the application of patches and upgrades;
- assess operating system configuration, including: insecure services, permissions, and registry settings as well as unnecessary services and packages;
- identify and validate security issues of immediate consequence;
- develop recommendations to enhance security.

Trojan Horses and

A Trojan horse program - "Trojan" for short - is a piece of computer software that provides intentionally hidden or covert functionality.

This definition includes a wide range of malicious software, such as keystroke loggers¹ and logic bombs². However, the commonest types of Trojans are those that, once executed, enable attackers to bypass existing security measures to access a computer. Among these, the most effective incorporate a "rootkit" program designed to conceal their presence.

Trojans are usually network applications that typically comprise a server installed on the victim's computer and a client on the attacker's computer. The server listens for commands sent from the client and responds by returning data to the client. It is also possible for Trojans to be "peer-to-peer" applications, such as file sharing software or Internet Relay Chat (IRC). Although these types of applications may be installed by attackers on compromised machines, they are not Trojans in themselves.

Trojans, which are continually evolving, can undermine the central pillars of information security; **confidentiality**, **integrity**, and **availability**. For "stealthiness" reasons, they have an increasing tendency to make their network traffic appear as existing services in order to obscure their presence. For example, Setiri, a recent proof-of-concept Trojan, bypasses network intrusion detection devices and firewalls by using commands embedded in web traffic to communicate.

Rootkits designed to hide Trojans fall into three types: file system rootkits, library rootkits and kernel rootkits.

Traditional rootkits simply modify common user programs so that the Trojan is invisible to the system administrator when file and process listings are

made. A variation on the traditional rootkit replaces some system library functions with Trojan versions, thereby avoiding detection by a system administrator who was using checksum and file integrity checking software to identify changes to key programs. However, changes to library files are also likely to be detected by integrity checking software, although the system administrator may ignore the warning because new programs might at any rate require updated libraries.

The most sophisticated type of Trojan modifies some objects or processes that run with system privilege. Some techniques used by hackers are to:

- modify the system kernel executable file and its integrity checking;
- install a device driver, loadable kernel module or other program running at system level, and use it to modify the code executed by another system process;
- patch system memory or running processes.

Each of these techniques requires administrator access to load a system level executable or to patch a system file, while writing an effective rootkit of this kind also requires a good knowledge of system programming. There are, however, kernel rootkits available for both Windows (for example, NT Rootkit) and UNIX systems (for example, Adore/ava) and a number of do-it-yourself guides. It's important to appreciate that because kernel rootkits undermine the trusted computing base, they represent the most serious way in which a computer can be compromised.



"Trojans, trust not the horse. Whatever it be, I fear the Greeks, even when bringing gifts."

Virgil (70-19BC) - Aeneid, Book II

¹ Keystroke loggers - software that covertly monitors what is typed at the keyboard (including passwords).

² Logic bombs - software that can be triggered to damage data on your computer system.

Kernel Rootkits

...an anti-virus or Trojan detection program might detect malicious software on your system, but it might not, especially if the system kernel has been compromised.

Common examples of Trojans - which should be detected by your organisation's firewall - are Subseven, *Back Orifice 2000 (BO2K)*, Netbus and distributed denial of service tools such as *Trinoo* and *Stacheldraht*. They provide a rich set of functionality, including:

- logging the victim's keystrokes (including passwords);
- representing the victim's screen on the attacker's computer;
- monitoring network traffic on the victim's network;
- hijacking TCP sessions involving the victim's computer;
- recording conversations via the victim computer's microphone or controlling a webcam;
- sending files from the victim's computer to the attacker;
- using the computer as a platform for attacks on other computers (denial of service, for example);
- using the compromised host for email, chat and file storage;
- modifying data on the victim's computer.

With a kernel rootkit installed a computer becomes totally untrustworthy and might not implement any of the security measures that the standard operating system implements.

A key message to conclude this brief overview of Trojans and rootkits is that **prevention is far better than cure**.

Fortunately there are a number of steps that you can use to reduce the chances of system compromise by a Trojan:

- follow good network security practice³;
- because e-mail is a common way for a Trojan to be sent to a victim's computer, block all *executable* mail attachments at the network

perimeter, or at the very least ensure that they are digitally signed by a trusted party;

- ensure that the security permissions of all users reflect least privilege (for example, restricting installation privileges to a sensible number of system administrators);
- follow the vendor's best practice security advice for operating system and application configuration;
- use an appropriate virus/Trojan scanner on a regular basis.

Least privilege can be hard to enforce, but system administrators should ensure that users have appropriate read, write and execute permissions on system objects, including keys in the Microsoft Windows registry.

If you suspect that your system has been compromised, an anti-virus or Trojan detection program might detect

malicious software on your system, but it might not, especially if the system kernel has been compromised. In general you will need to employ specialist analysis tools, perhaps through a specialist security consultant.

N.I.S.C.C. (<http://www.niscc.gov.uk>)

Editor: the major anti-virus software suppliers provide good descriptions of many Trojans (and viruses and worms) on their web sites. For example:

Sophos... <http://www.sophos.com/virus/info/analyses/>

Symantec... <http://securityresponse.symantec.com/avcenter/vinfodb.html/>

Network Associates... http://www.mcafee.com/antivirus/virus_glossary.asp

MessageLabs (managed service)... <http://www.messagelabs.com/viruseye/threats/default.asp>

³ See NISCC Technical Note 01/02... <http://www.uniras.gov.uk> (see **Alerts & Briefings** for 2002)

intrusion detection

V intrusion prevention



Intrusion Detection Systems are the burglar alarms of the network security world, while Intrusion Prevention Systems can additionally be programmed to respond to an attack. This article describes the concepts behind both IDS and IPS technologies, and compares and contrasts their different approaches.

Introduction

Firewalls have long been the mainstay of network security. Their role is to control access to network components or services in accordance with the policy defined by the system owner. They achieve this by examining the headers of IP packets and making decisions accordingly. However, this does leave the host system potentially vulnerable to attacks against its permitted services - such as exploits against a publicly-accessible web server - because in general no account is taken of the content of the packet, only that it corresponds to a permitted service.

Intrusion Detection systems (*IDS*) are the 'burglar alarms' of network security, designed to go off when activated by a particular trigger. In common with burglar alarms, the response then often depends on past experience - if your neighbour's house alarm has gone off by mistake five times in the last week, do

you recognise the significance on the sixth occasion or just ignore it? Alternatively, the response may depend on the availability of someone with the right experience to analyse the event and take appropriate action.

Intrusion Prevention systems (*IPS*) also aim to detect indications of an attack in progress, but they can respond automatically and in a predefined manner to prevent an attack from impacting the target system. This ability to respond means an IPS offers the potential to enable a system to remain on-line despite being under attack.

Intrusion Detection Systems

This article only summarises the principles of IDS, but interested reader may wish to refer for further information to the NISCC Technical Note 05/02: *Understanding Intrusion Detection Systems*, which is available on our web site (<http://www.uniras.gov.uk>).

IDSs come in two main flavours, Network-based IDS (or *NIDS*) and Host-based IDS (or *HIDS*). As their names imply, NIDS systems examine data on the Network link being monitored for signs of attack, whilst HIDS reside on a Host machine (for example a file server or a web server) and examine transactions with that particular Host for signs of malicious activity (this may be achieved using data passed to the application or logs generated by the application or server). IDSs are generally 'passive' - they observe and report on potentially malicious activity rather than actively responding to stop an attack.

There are three main mechanisms by which IDSs attempt to identify attacks:

- **Rule based:** in this architecture the IDS contains a library of '*signatures*' that correspond to known attack vectors. For example, a signature for detecting the actions of the *Code Red* worm may involve detecting a request for 'default.ida' over HTTP. Each data item - for example, a packet that passes 'on the wire' (i.e. in transit on the network) or data that arrives at a particular host - is compared to the signature library and an alert or log entry is generated as appropriate.
- **Anomaly detection:** this category of IDS attempts to determine the presence of an attack based on the

presence of data items or activities that fall outside the 'normal' pattern of behaviour. For these to be effective, the system needs **'training'** to learn what constitutes normal behaviour.

- **Protocol Analysis:** attempts to detect protocol elements that do not conform to the appropriate standard, anomalies that may indicate an attempted attack.

Of these differing modes of operation, the signature based approach to IDS is the more mature technology, and most commercially available IDS systems fall into this category.

NIDS systems are usually deployed where they can view the most traffic, or at least the traffic on those segments that are considered most important. On a segmented network, they can be connected to a monitoring port on a switch, although data aggregation can result in problems for the IDS. HIDS would normally be deployed on the more important servers within a network. Figure 1a shows an example of a deployment architecture, the idea being that IDSs are transparent to the end user and do not add any processing overhead to the data passing between the end points of a transaction.

Signature based IDS systems are very good at detecting known attacks, but they are not so at detecting 'new' attacks due to the time delay between a new vulnerability or attack being discovered, and a vendor releasing a signature to detect it. Ideally, the IDS should provide an interface by which administrators can define their own signatures relevant to local conditions.

When discussing IDS, it is impossible to avoid considering 'false positives', which are alerts generated by an IDS due to benign activity. Signature based IDSs are prone to generating false positives, though a good understanding of the network being monitored and a period of 'training' should ensure that these are minimised.

Anomaly detection engines are designed to detect attacks through comparison with a baseline of the normal system behaviour. This approach will always be more prone to 'false positives' because a statistical metric is used to determine 'good' and 'bad'; thus benign traffic from an application that wasn't in the 'training set' of the IDS could be flagged as anomalous and raise an alert.

Intrusion Prevention Systems

IPSS, which are relatively new to the market, respond in a proactive manner when they detect a potential attack. The response may take a number of different forms, such as:

- logging the event (like a standard IDS);
- blocking the transit of the data;
- resetting the connection between source and destination;
- limiting the rate of connection between source and destination;
- re-writing firewall rules for particular conditions.

IPSS are designed to sit 'in-line' with the target system (see figure 1b), effectively acting as a 'bridge' between the internal systems requiring protection and the rest of the network. In this architecture all traffic must pass through the IPS device, which inspects all the data for signs of attack (against the signatures it has been configured to use).

An immediate issue with this type of architecture is the potential consequence of the IPS crashing, which may effectively cut off the target system from the rest of the network. Depending on the nature of the business, it may be preferable for the system to fail 'open' thereby providing continued availability of the network services at the cost of removing the additional layer of security provided by the IPS.

Fig 1a Possible deployment architecture for NIDS

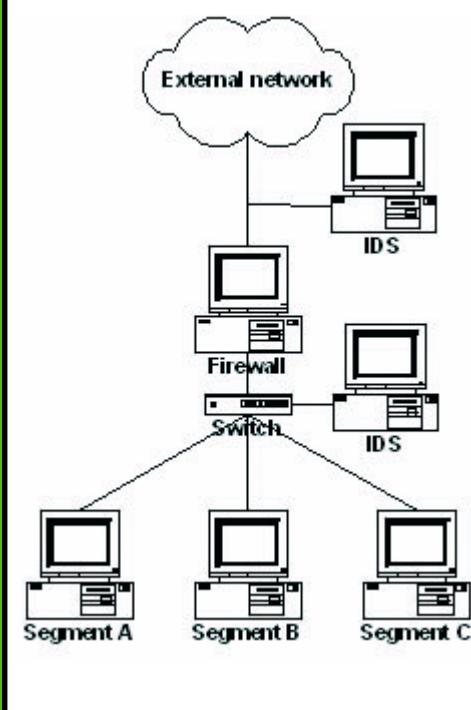
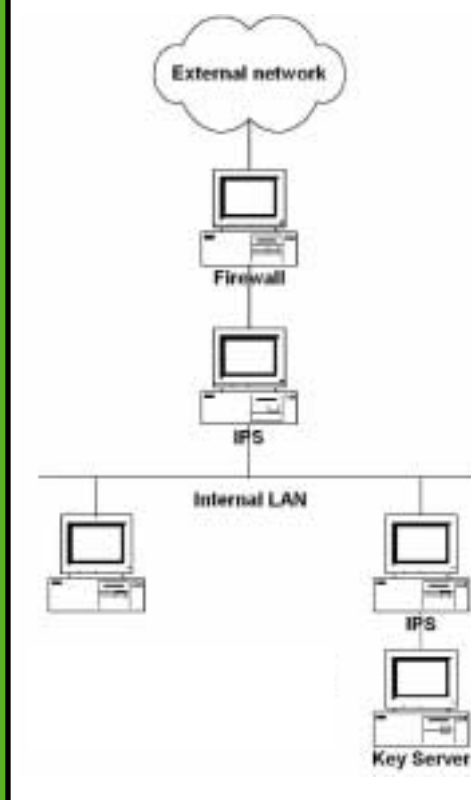


Fig 1b Possible deployment architecture for IPS



IPS systems do have the potential to form a valuable tool for network security, and they provide a means for reducing the amount of attack traffic reaching vital systems within a network.

The different types of IPS system that are available commercially include:

- **Network (or Gateway IPS):** sit in the network line, monitoring all network traffic for malicious activity, and are able to block packets that are designated as attacks;
- **Web server shields:** sit on the web server, effectively 'wrapping' the server software. Attacks are detected by monitoring the activity undertaken by the web server account;
- **Web application firewalls:** sit in the network path and inspect the contents of packets destined for any web server or web application for signs of attack.

Trusted operating systems can also be considered to be a form of IPS because they implement access control functionality and enforce user privilege restrictions.

Attack detection within the IPS can be achieved in several ways, including:

- **Signature Detection:** the IPS holds a library of signatures (similar to IDS) corresponding to known attacks that it compares with data on the wire. Ideally, the administrator should have the capacity to define additional signatures relevant to local conditions.
- **Protocol Analysis:** here the IPS compares the elements of the data on the wire with protocol definitions that it understands. Any deviations from the accepted protocol

definition may indicate an attack, the IPS then responding in the manner in which it has been configured.

- **Anomaly Detection:** similar to IDS, uses techniques to determine anomalous traffic and then respond.

Issues with detection of attacks within IPSs are similar to those within IDSs - the time delay between new attacks and signature availability, false positive rates, etc. However, in this instance the consequences of 'false positives' may be more serious, especially if the IPS is configured to block traffic from a source in the event of an 'attack' being detected.

IPS systems have the potential to form a valuable tool for network security, and for providing a means of reducing the amount of attack traffic reaching vital systems within a network. Their use to filter out traffic corresponding to known worms (such as *CodeRed* and *Nimda*) may, for example, greatly reduce the load on a web server. However, this must be offset against the risk of misidentification of attacks on service 'availability'. In common with an IDS, implementing an IPS is not a 'set and forget' task. Careful performance monitoring is necessary both to ensure that an IPS is meeting its objectives, and that the administrators remain aware of what is happening in their networks.

Summary

IDSs and IPSs are useful tools in the system administrator's armoury for helping to ensure the security of their networks. The choice of which system to deploy will depend on a number of local considerations, such as:

- cost;
- which parts of the network are to be protected by the deployed system;
- availability of resource to administer the system;
- requirement for alerts or a system making proactive defence responses;
- availability of resource to investigate the causes of alerts generated by IDS systems;
- applicability of detection techniques to local network services; and.....
- the degree of tolerance to loss of service.

Neither type of system can be considered to be 'set and forget'. Each requires monitoring to ensure that it meets its objectives; that signature libraries remain up to date and accurate; and that administrators are aware of what is happening in their networks. Where an IPS is used to respond to an attack proactively, administrators must be aware of any configuration changes made by the IPS (such as addition/modification of firewall rules) to their network.

N.I.S.C.C. (<http://www.niscc.gov.uk>)

Email spoofing is a technique frequently used by perpetrators of all manner of email hoaxes to hide their identities and point the blame at somebody else. It is a favourite with spammers and also used by hackers. Spoofing received some media coverage recently when a 12-year-old was able to demonstrate how he apparently sent an email purporting to come from the UK Prime Minister to the Chancellor of the Exchequer.

email spoofing

Background

The sending of spoof email is usually carried out for the purposes of causing embarrassment or the misinterpretation of the individual or organisation whose address has been spoofed.

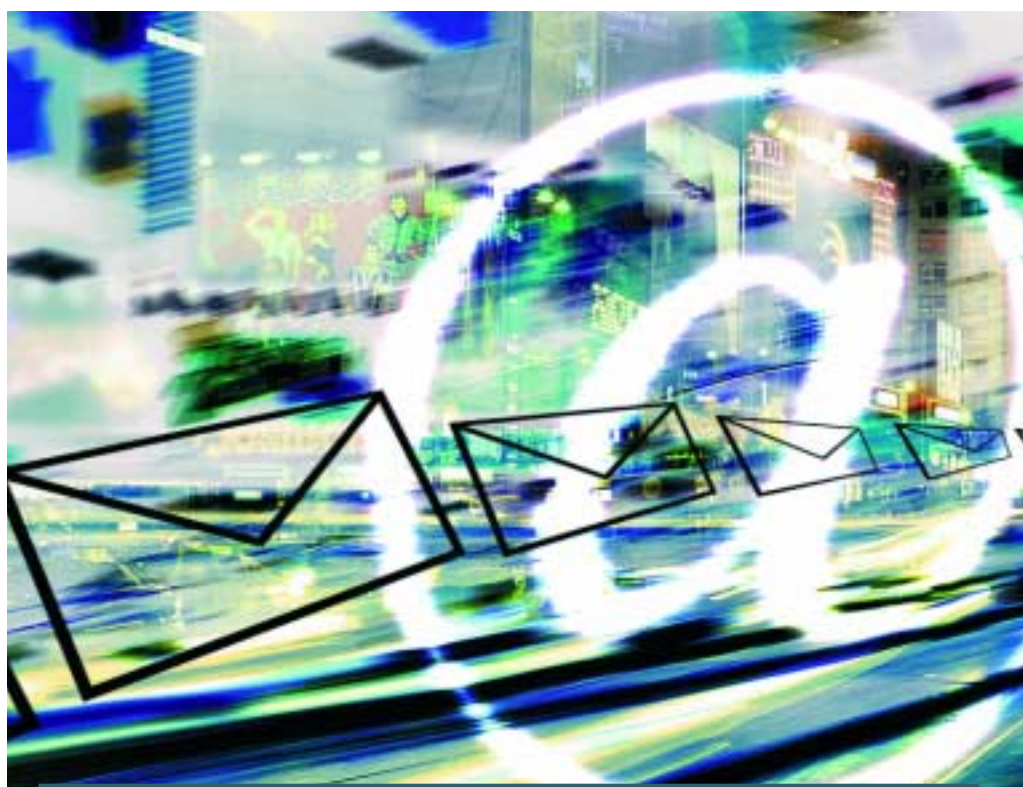
Consequences could include recipients of the email divulging information to those not entitled to have it. The information may then be used in a manner detrimental to the victim of the spoof. For example, interference with customer records, with a resultant impact on the customer. In the UK, the sending of spoof email is, in itself, not illegal although there is scope for legal action where personal information is obtained by deception or the email has threatening content.

Methodology

Sending spoof email is very simple. Most email software displays the "date received", "from" and "subject" fields.

The email header containing address and routing information is generally hidden from view to prevent cluttering the screen and confusing the user.

Consequently a user can be deceived if the sender simply changes the "from" field. The address is not normally checked at any stage in the process of sending an email and does not even have to be a valid address. There is little



Email spoofing - the threat

Any IT literate individual or group could use simple email spoofing. The effects which they can achieve with such attacks are limited only by their imagination and ability to write a convincing bogus content. The following scenarios could be imagined:

- Producing spoof press releases from a company or Government department to cause embarrassment.
- Causing disruption and wasted time by feeding misinformation to critical national infrastructure organisations.
- Encouraging users to switch off IT security features or passwords by spoofing emails from a security department.



that can be done at the server end to stop this, the only available options being:

- to make employees aware of the email spoofing risk;
- to require all email addresses to contain a valid domain name. This is currently being done, but even though the domain names can be checked, the email addresses themselves cannot;
- for internal mail servers to require all source email addresses to contain the organisation's domain, unless the email is coming from an external mail server;
- to provide some form of digital signature, as per Public Key Infrastructure (PKI). This is the only real countermeasure, but even this is not perfect;
- authentication on the mail server (SMTP AUTH), which can provide assistance in tracking down internal staff who create spoofed email, as can the use of the IDENT protocol, which may provide the username of the sender.

Various domain name checks, such as allowing the recipient server to check the existence of the source domain as well as that of the recipient, can be done, but this will depend on the software being used.

Sending spoof email is very simple... Once an email has been received, there is likely to be little about it that immediately identifies it as spoofed.

Identification

Once an email has been received, there is likely to be little about it that immediately identifies it as spoofed. The only technical indicators, to be found in the "internet" or full email header are:

- Instead of being marked as "From:" the email is marked as "Apparently-From:". This usually indicates a hand-built email and as such the address is likely to be false.
- The "Message-ID:" header and the "Received" header immediately above it in the internet headers list contain different domain names. This usually indicates that the headers have been faked.
- The "Message-ID" header contains a domain that differs from the domain in the "From:" address. However, this does not guarantee that the email is spoofed.
- The domain in the first "Received:" header is different from that in the "From:" address. Again, this does not guarantee that the email is spoofed.

Other indicators may include:

- The grammar, language or style of writing is not consistent with the email address the email claims to come from.
- The email may be missing the standard 'signature' the apparent sender may use.
- The email claims to be from an individual who doesn't exist within the organisation in question.
- If email purports to come from a government site, but does not bear a government address.

With all of the above, the common requirement is that users should be both aware of and alert to what indicators they should be looking out for.

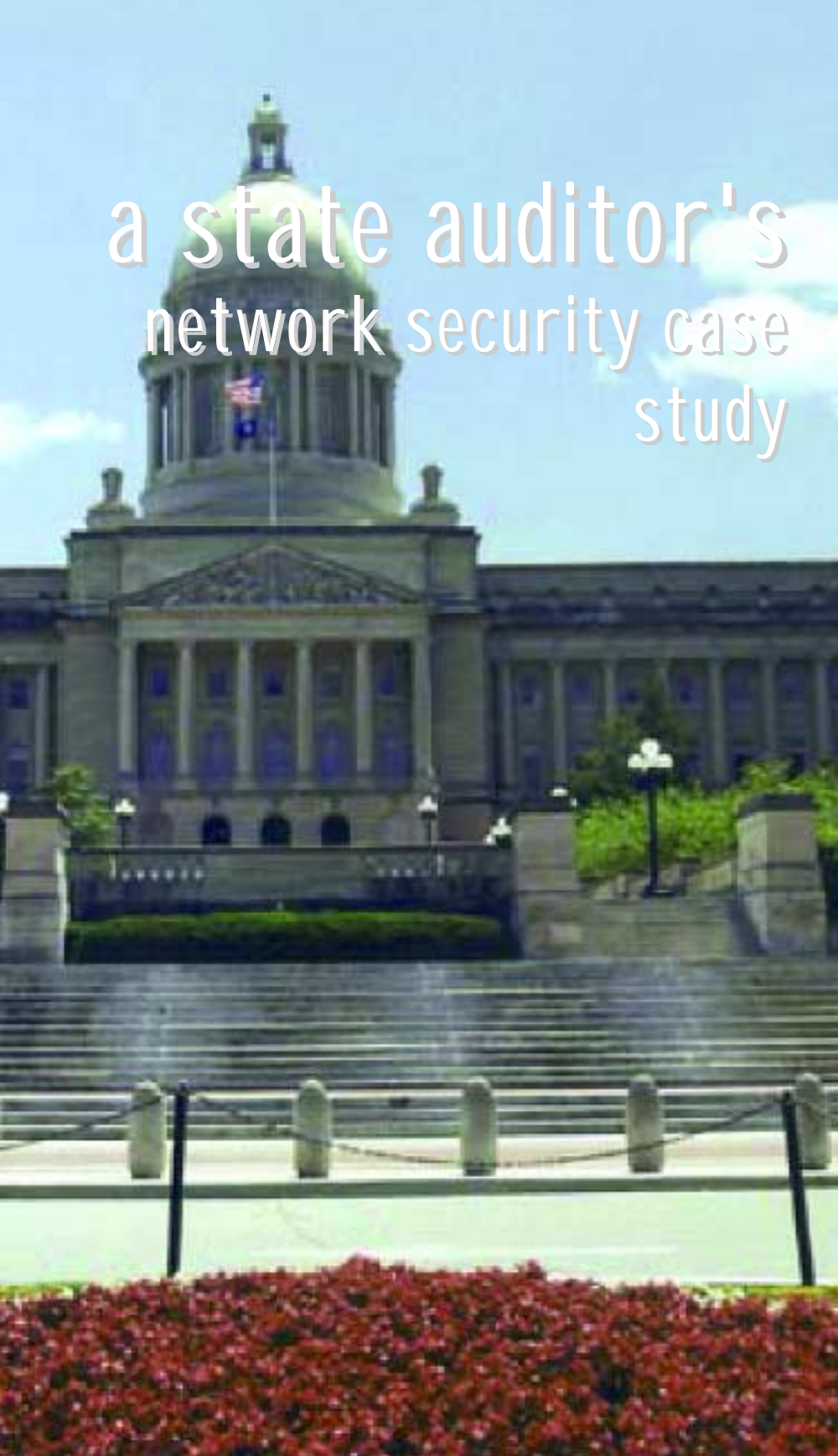
If the sender desired further concealment, they could use an open email relay server. These are poorly secured servers that allow anybody on the Internet to connect to them and send email out. In this case, investigators examining the header of the email would only be able to trace back as far as the open mail relay, and not to the true originator.

Conclusion

The effects of email spoofing can be limited by the appropriate configuration of email servers and improved user awareness of the problem. Currently, the only real countermeasure is the use of digitally signed messages that allow a recipient to authenticate the identity of the sender.

N.I.S.C.C. (<http://www.niscc.gov.uk>)

a state auditor's network security case study



Capitol Building, Frankfort

The first vulnerability assessment performed by Kentucky's Auditor of Public Accounts tested the security of the Commonwealth's accounting and reporting system in June 2000. Within minutes, auditors were able to gain administrator control over 14 of 17 system servers. Thus began three years of random, surprise vulnerability tests in 16 state government cabinets and agencies.

Vulnerability Assessment becomes Incident Handling in Kentucky's Transportation Cabinet

Abstract

The Commonwealth of Kentucky's Auditor of Public Accounts began performing network vulnerability assessments in state agencies in June 2000. One such assessment performed in July 2003 revealed a significant, long-term intrusion during which hackers with French addresses broke into Kentucky's Transportation Cabinet network and used it to:

- Store and distribute pirated recently-released movies, music CDs and DVDs, TV shows, and new computer games;
- Post and distribute copyrighted French medical textbooks;
- Host an Internet chat room.

In addition, auditors found that Cabinet computers had been used to visit and view thousands of pornographic websites or images.

Auditors provided detailed evidence of the intrusion and misuse to Transportation Cabinet officials and state and federal law enforcement, highlighting for network administrators seven security issues, to wit:

- Persistent null passwords;
- Vulnerable administrative accounts;
- Compromised data;
- Password harvesting by hackers;
- Hacker-installed tools;
- Pirated copyrighted materials on servers;
- Widespread viewing of pornographic sites by system users.

Auditors recommended a variety of measures designed to strengthen user passwords, fortify firewalls, remove compromised machines from the network, assume tainted application and data back-ups, rebuild compromised machines from the ground up, refer forensic evidence to proper authorities, notify business partners and the public, and anticipate retaliatory attacks.

Network security weaknesses threaten taxpayer dollars and facilitate identity theft. Three years of performing vulnerability assessments leads Kentucky's Auditor of Public Accounts to conclude that (1) a universal formula such as ICAMP¹ for quantifying the economic cost of insecure government networks must be adopted, (2) accountability for network security is largely absent in Kentucky state government agencies, and (3) auditors must perform surprise vulnerability assessments and publicize their findings in order to have the greatest impact upon network security.

Introduction

While auditors have performed information systems audits for many years, it was the Y2K alarm that foreshadowed a more systematic, focused inquiry on network security. Insecure government networks place taxpayer dollars at risk of cyber-theft and loss through network downtime. They also jeopardize the security of the unique identifiers like social security numbers and other confidential financial information of which government agencies are the repositories. Moreover, hackers may exploit insecure systems in the commission of other crimes. Known variously as ethical hacking, penetration testing, and vulnerability assessments, the procedures applied by auditors at every level of government have revealed alarming weaknesses, indifferent network managerial attitudes, and costly intrusions. Kentucky's Auditor of Public Accounts has performed surprise

assessments and publicized embarrassing findings to motivate government IT managers to give network security the priority it must have. Experience shows that if you exclude the element of surprise and the specter of adverse publicity, network insecurity may go undetected and important findings may be unaddressed, leaving systems unprotected.

Common among the findings of the vulnerability assessments was an institutional failure to observe basic security principles. Perhaps the most basic security measure, the use of passwords, was frequently ignored or ineffective.

The first vulnerability assessment performed by Kentucky's Auditor of Public Accounts tested the security of the Commonwealth's accounting and reporting system in June 2000. Within minutes, auditors were able to gain administrator control over 14 of 17 system servers. Following weeks of extensive consultations with network administrators, the assessment was re-performed in December 2000, revealing a significant strengthening of system security.

Thus began three years of random, surprise vulnerability tests in 16 state government cabinets and agencies. Each assessment produced both a written report of findings and recommendations for agency managers and contributed to a rising sense of alarm at the weak network security discovered throughout state government. During the first two years, the Auditor of Public Accounts refrained from publicizing assessment findings so as not to imprudently alert opportunistic hackers

to system weaknesses. As random testing continued, however, frustrating similarities emerged to reveal a government-wide inattention or indifference to network security. The Auditor of Public Accounts reluctantly concluded that raising public interest in the subject was essential to strengthening network security in government, and the office shifted toward making a public example of those agencies found to have disturbing weaknesses.

Common among the findings of the vulnerability assessments was an institutional failure to observe basic security principles. Perhaps the most basic security measure, the use of passwords, was frequently ignored or ineffective. In agency after agency, auditors found computers and servers with no password protection. Many administrator accounts were discovered to have null or weak passwords.

Another issue brought to light by the vulnerability assessments is the widespread belief by state government employees that network security is a responsibility reserved for the highest level of administrators. There is a mindset that network security is not a universal component in the job description of every network user. This rejection by network users of personal accountability for security has been fostered by the tendency of state

The failure to implement internal controls is too costly not to implement, as was demonstrated in 1996 when the failure to properly employ and manage passwords allowed a five million dollar embezzlement in the Kentucky Revenue Cabinet.

¹ Incident Cost & Analysis Modeling Projects... www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/archive/Report/ICAMP.shtml

government systems managers to seek rational explanations, and make excuses, for insecure systems.

One such excuse refers to the democratic, open culture of government. Government's information systems are therefore logically open and accessible. Polemics aside, it is disingenuous to assert that prudent security measures should be compromised by fidelity to open government and transparency.

Cost is the most frequently cited impediment to network security, and to be sure, the latest architectural advancements in network security may require significant investment. Unfortunately, tight state budgets characteristically leave few, if any, dollars for security. Still, there are fundamental security measures and attitudes absent from Kentucky government agencies that require few additional resources beyond a commitment of reasonable diligence. For example, the Auditor of Public Accounts' work revealed a widespread failure of agency administrators to timely apply free downloadable system patches, resulting in significant, costly downtime when assorted viruses and worms attacked. Furthermore, auditors are quite accustomed to effectively rebutting the argument that internal controls are too costly to implement. The failure to implement internal controls is too costly not to implement, as was demonstrated in 1996 when the failure to properly employ and manage passwords allowed a five million dollar embezzlement in the Kentucky Revenue Cabinet.

Government managers seem surprisingly oblivious to the cost of insecure networks. It has been difficult, therefore, to get their attention. System crashes, downtime, and labor-intensive triage for compromised networks take a verifiable and meaningful economic toll, but network managers are often conflicted about revealing such problems and agency heads have no accepted formulae for calculating the losses.

The Kentucky Auditor of Public Accounts' vulnerability assessments during the last three years included two highly publicized findings that resulted in the issuing of separate *Auditor Alerts* to all state and local government agencies. In one such assessment, a randomly tested surplus agency computer was found, without password protection, to contain in clear text significant components of Kentucky's STD and AIDS database, including identities of those tested, their test results, and their sexual partners. An *Auditor Alert* advising effective methods of scrubbing the hard drives of surplus machines was issued.

In another assessment, a series of penetration tests was performed on agency wireless networks by "war driving." The ease of penetration led to issuance of an *Auditor Alert* discussing the special challenges posed to network security by wireless networks, including the widespread failure of network administrators to enable the security components of such systems. One unexpected collateral finding of this work was the absence of an effective firewall separating Kentucky's state government network from the University of Kentucky's network.

Tempered by this body of work, the Auditor of Public Accounts undertook a vulnerability assessment of the information systems in the Kentucky Transportation Cabinet in July 2003.

Case Report

The Kentucky Transportation Cabinet's system is a centrally managed, enterprise class network, serving thousands of users at hundreds of remote sites, and interfaces with other state and federal networks. The system is used to manage massive road construction and maintenance projects, warehouse vehicle registration records, and house the personal, confidential information of licensees. It is directly linked to the Commonwealth's accounting and reporting system. The Transportation Cabinet's system uses industry standard rather than proprietary hardware and software.

As part of the audit of the Commonwealth's Comprehensive Annual Financial Report, the Auditor of Public Accounts performed a risk assessment of the Transportation Cabinet's information system. This assessment consisted of two activities: scanning and enumeration.

During the scanning phase, auditors used **fscan.exe**, **nmap.exe**, and **superscan.exe** to identify potential vulnerabilities among the Transportation computers and servers providing exploitable services such as web, telnet, and Microsoft shares.

Auditor analysis... led to the discovery of a malicious, on-going intrusion. This discovery transformed the auditors' vulnerability assessment into an incident-handling project where criminal activity was observed.....

- Hacker installed applications and services operating in stealth mode;
- A list of cracked administrative passwords;
- Gigabytes of data in daily transport;
- Harmful software stored on the system, e.g., netcat for creating covert backdoors, pwdump for extracting passwords, regedit for altering a system's registry, and prockill, for terminating procedures.



Kentucky Senate Chamber

During the enumeration phase, auditors used **enum.exe**, **net.exe**, and **nbtDump.exe** to analyze vulnerabilities identified by the scans. This enumeration highlighted (1) the existence of devices and user accounts lacking passwords, (2) version numbers of running programs, (3) user names and groups, including assigned privileges, and (4) unprotected Microsoft shares allowing privileged access to file systems of many computers.

Auditor analysis of one of the first vulnerabilities that came to light during enumeration led to the discovery of a malicious, on-going intrusion. This discovery transformed the auditors' vulnerability assessment into an incident-handling project where criminal activity was observed.

The following hacker exploits were observed:

- Hacker installed applications and services operating in stealth mode;
- A list of cracked administrative passwords;
- Gigabytes of data in daily transport;
- Harmful software stored on the system, e.g., **netcat** for creating covert backdoors, **pwdump** for extracting passwords, **regedit** for altering a system's registry, and

prockill, for terminating procedures.

Auditors acquired irrefutable evidence that these programs, and several others, had been used. They observed hackers actively managing their ownership of the system, and unauthorized persons uploading and downloading pirated multimedia software. This material included (1) pirated new release movies, music CDs, DVDs, TV shows, and new computer games, and (2) newly copyrighted French medical textbooks.

Included in the hacker configuration files and documentation was the following statement, in clear text French.

Auditors used *babelfish.altavista.com* to produce the following translation:

- This server was hacké by SuBy on request of a person. SuBy declines any responsibility towards this person and could not be held for person in charge for though it is;
- This server does not exist 2) all this Of course is legal ;D 3) SuBy rox 4) racism No (ouai C rare I C ;p) 5) the 1337 are not authorized 6) the files are has an informative title ;D 7) the hackers could not be held for persons in charge! 8) the files must be unobtrusive in the 24 hours 9) \$\$\$--- IT IS NECESSARY TO OBSERVE the RULES ---\$\$\$;

- We wish you a pleasant stay on this pubstro;
- Thank you has all those which make live the French scene.

Among the hacker configuration files and logs, auditors observed 25 IP addresses of intruders. Using McAfee's **neotrace** program, auditors traced these addresses to their geographic points of origin in France, Croatia, and Canada. They also found that a remote Internet relay chat room was being controlled by **eggdrop**, a hacker program residing on a Transportation Cabinet server. This allowed the hackers to control admittance to the chat room and to exploit the anonymity it provided.

Unrelated to the intrusion noted above, auditors discovered web proxy logs detailing the browsing habits of system users. A cursory examination of these logs revealed that several hundred computers were used to visit several hundred unique, pornographic websites in violation of the Commonwealth's acceptable use policies governing information technology systems. The auditors chose to focus on pornographic site browsing because such sites are known to be a disproportionately large source of malware, software intended to compromise a visitor's computer or system. Such attacks go largely unreported by victims because they are self-incriminating.

Later, more detailed analyses of the web proxy logs indicated the intentional, persistent browsing of websites displaying pornographic images of children. Some 34 computers were found to have been used to search for and access child pornographic material. The findings were promptly referred to state and federal law enforcement.

For two weeks, auditors performed their scanning, observing, and evidence gathering undetected, even though no attempt was made to mask the activities.

Conclusion

The Auditor of Public Accounts found Kentucky's Transportation Cabinet network to be inadequately protected and unmonitored. While firewalls, activity auditing software, content managing software, and intrusion detection systems were in place, none was being used effectively, and some not at all.

Auditors recommended a variety of measures designed to recover from the malicious intrusion and establish effective defenses. The detailed findings of the vulnerability assessment and its accompanying recommendations were communicated to the Transportation Cabinet prior to public disclosure. The recommendations included:

- Applying strong passwords;
- Enabling and fortifying firewalls;
- Removing compromised machines from the network;
- Working from the assumption that application programs and data backups are tainted;
- Rebuilding compromised machines from the ground up;
- Quarantine compromised machines and make them available for forensic analysis;
- Notifying business partners and the public;
- Anticipating retaliatory attacks;
- Installing network sniffers to detect traffic to or from previously identified hacker addresses.

Network security weaknesses threaten taxpayer dollars and facilitate identity theft. Three years of performing vulnerability assessments leads Kentucky's Auditor of Public Accounts to conclude that (1) a universal formula such as Incident Cost and Analysis Modeling Projects, (www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/archive/Report/ICAMP.shtml) for quantifying the economic cost of insecure government networks must be

adopted, (2) accountability for network security is largely absent in Kentucky state government agencies, and (3) auditors must perform surprise vulnerability assessments and publicize their findings in order to have the greatest impact upon network security.

Edward B. Hatchett, Jr.,
Auditor of Public Accounts,
Commonwealth of Kentucky

<http://www.kyauditor.net>
e-mail to... ED.Hatchett@KYAuditor.net

B.J. Bellamy, SANS GSEC, GCIH, GCFA,
Chief Information Officer



Lincoln Statue, Capitol Rotunda.

Abraham Lincoln was born in Hodgenville, Kentucky, and served as the 16th president of the United States.

The Commonwealth of Kentucky

Originally part of Virginia, the land that is now Kentucky became Kentucky County in 1776 and the fifteenth of the United States in 1792. The use of "commonwealth" doesn't have any particular significance, being a term commonly used in the eighteenth century meaning the same as "state".

Kentucky covers a land area of 40,395 square miles (104,623 sq km) and has a population of just over 4 million people. The State is divided into 120 counties, its capital Frankfort being in Franklin County. Kentucky's state constitution was adopted in 1891. The Governor is elected for a term of four years, the General Assembly, or legislature, is bicameral, with a senate of 38 members and a house of representatives of 100 members. Kentucky is represented in the U.S. Congress by six representatives and two senators, and has eight electoral votes.

Within the Commonwealth's Constitution, the role of the Auditor of Public Accounts is to ensure that public resources are protected, accurately valued, properly accounted for, and effectively employed to raise the quality of life of Kentuckians. Within the State Audit Office, the Information Technology Branch audits government computer systems and the data they generate. The branch also produces auditable information for financial and performance auditors by extracting, analysing, and reporting data derived from agency computer systems.

Editor

Kentucky Legislature Home Page.....
<http://www.lrc.state.ky.us/home.htm>

Kentucky Constitution.....
<http://www.lrc.state.ky.us/Legresou/Constitu/intro.htm>

Risk-based Sampling Using COBIT



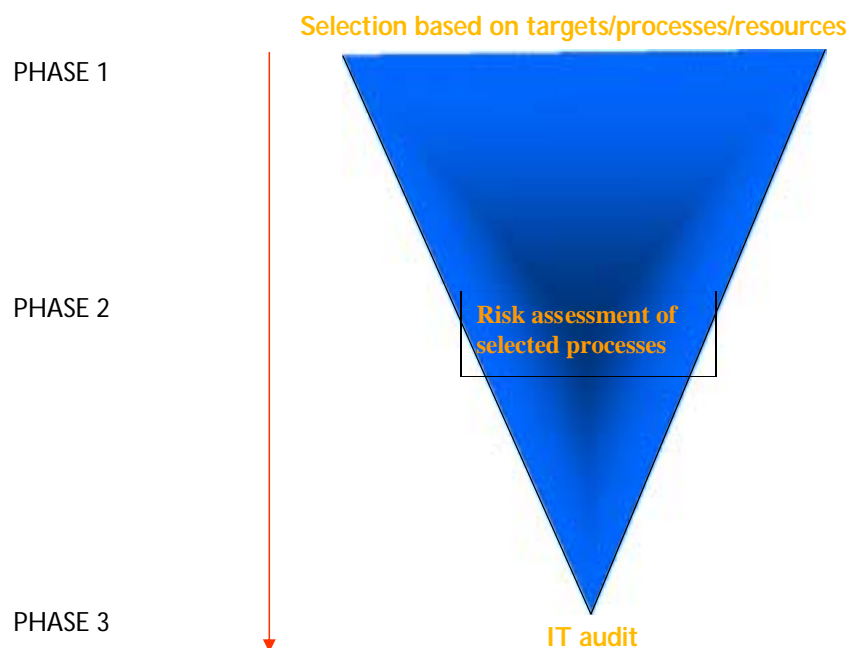
Riksrevisjonen

By Rune Johannessen CISA, CIA, Dip. Internal Audit

In this article, I would like to share some useful experiences that I have gained in my work with the COBIT (Control Objectives for Information and related Technology) tool kit. The following is not intended to be a template for the execution of risk-based audits, but rather a tentative suggestion towards a possible audit method.

Many public and private organisations now use COBIT, and I am fairly confident that anyone who has experience of the tool would confirm that it is highly comprehensive and its use quite time consuming. This is often in stark contrast to our everyday situation, where time is a critical factor of which we often have too little to carry out the tasks that have been assigned to us. It is therefore important that within our given time frames we select the areas and processes that are most important and pose the highest risk, in order that we provide our client with maximum added value.

In my opinion, COBIT does not provide clear guidelines on how to carry out an overall (or "high level") audit risk assessment; in other words how to select the most important areas and/or processes for auditing. I have therefore chosen to illustrate my solution with a general model for carrying out the auditing cycle. My method, which is based on qualitative assessments and allows considerable flexibility in relation to the audit client, can be represented in graphical form thus:



Phase 1: Selection based on targets/processes/resources

This phase consists of deciding, at a general level, what to focus on, which may be a sample of domains, processes, IT resources and/or a sample of information criteria. On the basis of the selected priorities the auditor derives a list of processes that it might be relevant to examine in more depth. In the following example I have tried to illustrate this for the domain "**Acquisitions and implementation**", where the processes "*Change management*" and "*Acquisition and maintenance of software*" are identified as highly important to the audit client and are therefore selected as relevant to the audit.

Phase 2: Risk assessment of selected processes

As a result of the selections made in Phase 1, the auditor now has a sample of processes that have been ascribed priorities. In the example above, A12 and A16 were identified as relevant within the domain "Acquisitions and implementation". As a result of restrictions on time and resources, it is often necessary to further limit the amount of work. In Phase 2 the auditor again ascribes priorities to the processes selected in phase 1, and then selects those with the highest risk. I have tried to illustrate this in the following example, where the auditor completes the following form for each of the processes that were selected in Phase 1, in this case A16:

The table lists a number of control questions linked to each process - these have been derived from the points listed under the title "and takes into consideration" on the first page of each process¹. On the basis of a sample, the auditor formulates some general control questions intended to give a 'feel' for the routines, documentation and processes in use in this area. The information required to answer the sample questions can be gathered through interviews and by observation of the routines in use. At this stage, the auditor does not make any comprehensive assessments of the content and quality of the available material.

The column for control routines should be marked as *documented*, *undocumented* or *don't know*. The following criteria may be used to answer the questions:

Scale	Control routines
Documented	The audited entity has a routine, process or documentation that deals with the matter.
Undocumented	The audited entity does not have routines, processes or documentation that deal with the matter.

Importance				IT process
Very important	Important	Not very important	Don't know	
				ACQUISITIONS AND IMPLEMENTATION
		X		A11 Identification of solutions
X				A12 Acquisition and maintenance of software
		X		A13 Acquisition and maintenance of technological infrastructure
		X		A14 Development and maintenance of IT procedures / routines
		X		A15 Installation and approval of systems
X				A16 Change management

IT process	Control routines			Risk			Ref.	
	Documented	Undocumented	Don't know	Probability	Consequence	High		Medium
A16 Change management								
1. Are all requests regarding change and system maintenance documented and subject to formal and structured change procedures?								
2. Are all change requests categorised and prioritised according to clear criteria?								
3. Do the organisation's routines for change management ensure that consequences as a result of the particular change are identified and assessed before it is approved / rejected?								
4. Have procedures been established that ensure monitoring between the system for change management and the organisation's configuration control system?								
Etc.								

The next step involves making an overall assessment of the probability of there being errors, weaknesses or loopholes in a process. This assessment will have as its starting point a preliminary review of the process and, as appropriate, the auditors' own opinions. The auditor should include internal and external factors that can adversely affect the process. The results are presented in a matrix with the following scale:

Scale	Probability
H	It is regarded as highly probable that this process will be negatively affected by internal or external events.
M	It is regarded as possible that this process will be negatively affected by internal or external events.
L	It is not regarded as very probable that this process will be negatively affected by internal or external events.

¹ See full COBIT documentation set. This can be downloaded from... <http://www.isaca.org/>

The next step is to assess the consequences of a negative incident. In addition to any monetary losses, factors such as reputation and working environment should also be taken into consideration.

Scale	Consequence
H	Negative internal or external incidents are expected to have major consequences for the process.
M	Negative internal or external incidents are expected to have medium consequences for the process.
L	Negative internal or external incidents are expected to have minor consequences for the process.

In this way, each process is subject to a risk assessment through probability and consequences being considered together. On the basis of how the process is rated in terms of risk (H high, M medium, L low), a sample is selected to be used in the following IT audit phase.

Phase 3: IT audit

An IT audit is then carried out on the processes that have been identified as having the highest risk, using the COBIT "Audit Guidelines":

IT process and audit questions		Results of evaluation and testing	Recommendation	Ref.
AI6	Change management			
	<p>Has a method been established for prioritisation of change recommendations from users, and if so, is it being used?</p> <p>Have procedures been compiled for sudden changes, and if so, are they being used?</p> <p>Is there a formal procedure for monitoring changes, and if so, is it being used?</p> <p>Are changes logged in a way that shows whether they have been carried out in a satisfactory way?</p> <p>Etc.</p>	<p>Observation:</p> <p>Method for changes... There is no procedure for sudden changes ... Etc.</p> <p>Assessments:</p> <p>The methodology is incomplete in terms of sudden changes...</p> <p>Conclusion:</p> <p>The methodology is inadequate...</p>	We recommend...	

I hope that these observations and suggestions will contribute to development of a practical approach to how a risk-based audit can be carried

out using COBIT. I also hope that this article will inspire others to share their experiences and describe their routines when using this tool.

About the author

Rune Johannessen is a Senior Audit Adviser at the Office of the Auditor General of Norway, where he is involved in both IT auditing and the development of methodology. Rune has 7 years experience in the field of internal auditing, financial auditing, IT auditing and quality assurance in IT projects. Before joining the Auditor General of Norway, he worked as a senior adviser for PricewaterhouseCoopers on quality assurance in system development projects and in IT security.

Rune holds a bachelor of management degree from the Norwegian School of Management and a higher degree from the University of Oslo, and is certified CISA and CIA.

COBIT

COBIT, developed by ISACA, is a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners.

COBIT comprises the following main products:

Framework: a successful organisation is built on a solid framework of data and information. The *Framework* explains how IT processes deliver the information that the business needs to achieve its objectives. This delivery is controlled through 34 high-level control objectives, one for each IT process, contained in the four domains. The *Framework* identifies which of the seven information criteria (effectiveness, efficiency, confidentiality, integrity, avail-

ability, compliance and reliability), as well as which IT resources (people, applications, technology, facilities and data) are important for the IT processes to fully support the business objective.

Management Guidelines: to ensure a successful enterprise, you must effectively manage the union between business processes and information systems. The new *Management Guidelines* is composed of Maturity Models, Critical Success Factors, Key Goal Indicators and Key Performance Indicators. These *Management Guidelines* will help answer the questions of immediate concern to all those who have a stake in enterprise success.

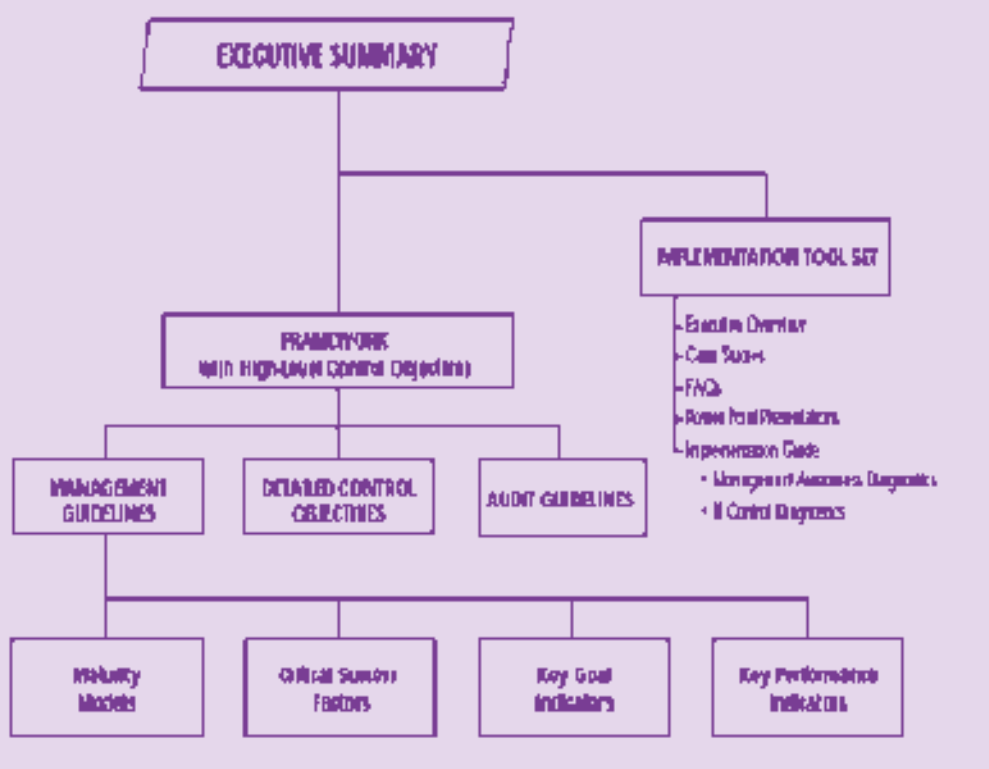
Detailed Control Objectives: the key to maintaining profitability in a technologically changing environment is how well you maintain control. COBIT's *Control Objectives* provides the critical insight needed to delineate a clear policy and good practice for IT controls. Included are the statements of desired results or purposes to be achieved by implementing the 318 specific, detailed control objectives throughout the 34 high-level control objectives.

Audit Guidelines: analyse, assess, interpret, react, implement. To achieve your desired goals and objectives you must constantly and consistently audit your procedures. *Audit Guidelines* outlines and suggests actual activities to be performed corresponding to each of the 34 high-level IT control objectives, while substantiating the risk of control objectives not being met.

Implementation Tool Set: an Implementation Tool Set, which contains Management Awareness and IT Control Diagnostics, Implementation Guide, frequently asked questions, case studies from organizations currently using COBIT and slide presentations that can be used to introduce COBIT into organizations. The tool set is designed to facilitate the implementation of COBIT, relate lessons learned from organizations that quickly and successfully applied COBIT in their work environments and assist management in choosing implementation options.

COBIT can be downloaded from... <http://www.isaca.org>

COBIT FAMILY OF PRODUCTS



Going electronic

By Andrée Lavigne
and Caroline Émond



Using information technologies and computer systems to gather, process, transmit, maintain and present information is nothing new. What is new is an added dimension. In the past, automation affected only some aspects of information processing. Today, the development and convergence of IT and the integration of information systems allow for the seamless flow of information. An integrated IS environment is a paperless environment where information is exchanged without space constraints and transmitted from one application to another, one entity to another, or one country to another via electronic networks.

Paperless environments are commonplace and in this context auditors have to gather electronic information as audit evidence. What is electronic audit evidence (EAE)? What are its attributes? How does it differ from traditional audit evidence? How does it impact the audit approach? What are the risks and the controls that can be applied to reduce them? These questions are being addressed by a CICA study group, which, at the request of the Assurance Standards Board and Information Technology Advisory Committee, is preparing a report on EAE issues.

EAE has an impact on the reliability of evidence and professional competence, knowledge of the entity's business, the audit approach, detection of misstatements and illegal acts and documentation of audit evidence. The report will set out recommendations for assurance standards to provide guidance on these issues and will deal with the risks of using EAE, the controls and technologies that may mitigate these risks, and the legal

issues deriving from the use of electronic documents (e-documents) and signatures.

EAE is information created, transmitted, processed, recorded, and/or maintained electronically that supports the content of an audit report. The information can only be accessed using proper equipment and technologies such as a computer, software, printer, scanner, sensor or magnetic media. E-documents may take such forms as text, images, audio or video. EAE includes accounting records, source documents and such vouchers as electronic contracts, e-documents pertaining to billing, procurement and payment, electronic confirmations and all other electronic data pertinent to the audit.

EAE differs from traditional audit evidence in several respects. First, it consists of information in a digital format whose logical structure is independent of the information. Second, the information's origin, destination and sent and received dates are not an integral part of the e-document, message or other information format.

The more integrated the IS, the more business transactions will be processed and documented solely by electronic means. Auditors are most likely to use EAE in internal and external integrated IS environments - for example in ERP systems, e-commerce or e-business environments. Some risks inherent in these types of environments include the entity's dependence on its own IS and on those of its partners and third-party service providers, together with the risk of failure at each of these levels. Other risks are loss of integrity, non-authentication, repudiation and violation of confidentiality of data, as well as loss of an adequate audit trail, and legal uncertainties.

A study group examines the issues auditors face in gathering electronic information as evidence and its impact on the audit.

Paper versus electronic	
Paper audit evidence	Electronic audit evidence
Origin	
Proof of origin easily established	Proof of origin difficult to establish solely by examining electronic information. It is determined using controls and security techniques that allow for authentication and non-repudiation.
Alteration	
Paper evidence difficult to alter without detection.	Alterations difficult, if not impossible, to detect solely by examining the electronic information. Information integrity depends on reliable controls and security techniques.
Approval	
Paper documents show proof of approval on their face.	Approval difficult to establish solely by examining the electronic information. It is determined using controls and security techniques.
Completeness	
All relevant terms of a transaction usually included in one same document.	Relevant terms often contained in several data files.
Reading	
No equipment needed.	Various technologies and equipment needed.
Format	
Integral part of document.	Separate from data and can be changed.
Availability and accessibility	
Not usually a constraint during the audit.	Audit trail for electronic data may not be available at the time of the audit and accessing the data may prove more difficult.
Signature	
Simple matter to sign a paper document and review the signature.	Appropriate technologies are required to issue a reliable electronic signature and review it.

To assess the sufficiency and appropriateness of the EAE gathered to support the audit report, the auditor should consider the specific risks associated with the use of such evidence. These can't be assessed solely by reviewing the documentary evidence, as is usually the case with paper documents. A printout of the electronic information, or onscreen reading, is only one format. And it provides no indication of origin and authorization, nor does it ensure the integrity or completeness of the information. Auditors should ensure that controls and technologies to create, process, transmit and maintain electronic information are sufficient to guarantee its reliability. The table below presents the criteria to assess the reliability of electronic information as audit evidence. The importance of each criterion depends on the nature and origin of the electronic information and its intended use for audit purposes. In addition to assessing reliability of audit evidence, the auditor looks into the availability of electronic evidence for audit purposes. Data confidentiality is also of interest to the auditor as a breach of confidentiality could represent a business risk that could impact the entity's financial position.

The reliability of electronic information depends on the reliability of the IS and supporting technologies. Where significant information underlying one or more assertions in financial statements is gathered, processed, recorded or maintained electronically, it may be impossible to reduce detection risk to an acceptable level by relying solely on the application of substantive procedures. In such cases, there is a high risk that misstatements in the electronic information obtained as audit evidence may not be detected. The auditor may need to adopt a combined approach and perform tests of controls to get appropriate audit evidence.

Because signing documents takes on a new dimension in an electronic environment, this issue needs to be examined closely. A signature primarily functions as a symbol signifying the signer's intention and authenticating the document. A handwritten signature on a paper document is affixed by an identifiable person and is intended to authenticate the intention inherent in the signed

Assessing reliability of electronic information as audit evidence	
Authentication	The identity of the person or entity that created the information can be confirmed.
Integrity	The completeness, accuracy, current nature and validity of the information. Integrity is the assurance that the information was validated and was not intentionally or accidentally altered or destroyed when it was created, processed, transmitted, maintained and/or archived.
Authorization	The information was prepared, processed, amended, corrected, sent, received and accessed by persons entitled to do so or responsible for doing so.
Non-repudiation	A party, person or entity having sent or received an information cannot deny having taken part in the exchange and repudiate the information content. Depending on whether there is irrefutable proof of origin, receipt or content of the electronic information, there is non-repudiation of origin, non-repudiation of receipt or non-repudiation of content.
The criteria could be used to assess the reliability of any documentary information, whether in paper or electronic form.	

document. In a virtual environment, the signer cannot be identified visually. That is why the signature has to be used to confirm consent and to identify the signer. When a handwritten signature is affixed on a paper document, it is "merged" so to speak with that document. Since electronic information can migrate easily from one medium to another, the signature and the document are independent of one another. The signature has to be bound with a specific document and the document's integrity needs to be established. The objective is to reduce the legal uncertainty as to the electronic signature's admissibility.

Electronic signature is a generic term to describe a technology-neutral signature in electronic and binary form. It may take various forms and be created in different ways. It may be created without any controls (a name typed at the end of a document); created using non-cryptographic security techniques (password, PIN number, biometric ID, digitized signature); or created using cryptographic security techniques (symmetric or secret key cryptography, asymmetric or public key cryptography or a digital signature).

Relevant controls and technologies must be used to obtain a reliable electronic signature. Non-cryptographic security techniques, based on a shared secret, help control authentication and authorization of the electronic document and signature. However, these security methods have limitations. Shared-secret authentication supposes that the parties have already exchanged information to agree on the secret. Moreover, a secret is only effective if it hasn't been forgotten or discovered. Non-cryptographic security techniques offer no security as to the non-repudiation, integrity or confidentiality of e-documents and signatures. Cryptographic security techniques, on the other hand, offer a secure way to ensure the authentication, non-repudiation, integrity and / or confidentiality. Non-cryptographic and cryptographic security techniques are often used in tandem to deliver a high level of reliability.

Digital signatures are based on asymmetric or public key cryptography. This technique involves mathematically generating a related key pair and using it

Reliability criteria for an electronic signature

Authentication	<ul style="list-style-type: none"> ● identification of the signer ● unique to the user ● authentication of the signed document
Authorization	<ul style="list-style-type: none"> ● confirmation of consent; the mechanism for incorporating the signature is the sole responsibility of the signer
Integrity	<ul style="list-style-type: none"> ● confirmation of the integrity of the signed document
Non-repudiation	<ul style="list-style-type: none"> ● confirmation of the link between the document and the signature ● continuation of the link between the document and the signer from the time of signing ● if need be, confirmation of the origin and destination of the document

to encrypt or decrypt data. One of the keys is kept secret by its holder, the other is freely available. The digital signature is generated by calculating a message digest and encrypting it with the signer's private key. The message digest is a unique number calculated using a hashing algorithm. This is a unique way to represent messages of varying lengths in much smaller format. If only one character of the original message is changed, the message digest will be changed. If the value of the message digest calculated on the message received is identical to the original message, the authentication, non-repudiation and integrity of the message are ensured. However, assurance as to the signer's identity largely depends on the controls implemented to guarantee the security of the signer's private key and on the receiver's confidence that the identity associated with the public key is authentic. A public key infrastructure is a solution that may ensure sound key management and provide assurance as to the signer's identity.

Much progress has been made to legally recognize e-documents and signatures as evidential matter. Ottawa and most provinces have passed e-commerce legislation and have amended evidence acts to recognize e-documents and signatures and establish admissibility criteria for this evidence. However, there is still some legal uncertainty about e-documents. Major ambiguities persist regarding jurisdiction and laws applicable to cyber transactions. Some uncertainty remains about admissibility conditions for e-documents and signatures under Canadian law.

In cases where the admissibility of an e-document is questioned, it is up to the person wanting the document admitted to establish its integrity and authenticity. It is up to the court whether the evidence is admissible. The best way for an entity to mitigate the legal risks associated with the admissibility of e-documents and establish data integrity is to institute and maintain reliable IS and use appropriate technologies. The admissibility of an e-signature is also subject to certain conditions. The technology must allow for the identification of the signer, and the link between the signature and the e-document must be created in such a way that subsequent alterations of the document can be detected. In addition, some legislation sets out standards requiring the use of certain technologies or the application of specific procedures.

Clearly, electronic information raises important issues of interest to management, which needs reliable decision-making information, and auditors, who rely on this information to gather sufficient and appropriate audit evidence to support the content of the audit report.

About the authors

Andrée Lavigne, CA, is a principal in the CICA's Research Studies department.

Caroline Émond, CA, is partner in global risk management services at PricewaterhouseCoopers in Montreal.

The Audit Office of New South Wales: Auditing the implementation of

freedom of information

To comply with the law on Freedom Of Information, agencies need to impose sound standards of information management. But as Stephen Horne explains, there are wider issues to consider, not least of which is whether decisions on information disclosure are taken objectively.



**THE AUDIT OFFICE
OF NEW SOUTH WALES**

What is FOI?

Most democratic societies recognise that Freedom of Information (FOI) is a fundamental element of government accountability. Opening government processes to scrutiny allows the public to question and better evaluate the activities the Government carries out on their behalf.

FOI legislation, introduced in New South Wales (NSW) in 1989¹, gave members of the public the legal right to access most information in most government agencies. They may:

- obtain access to information held as records by State Government Agencies, a Government Minister, local government and other public bodies;
- request amendments to records of a personal nature that are inaccurate; and

The audit aimed to answer some basic questions...

1. Do agencies comply with the spirit of the Act?
2. Do agencies help applicants with their requests?
3. Are fees and charges kept to a minimum?
4. How thoroughly do agencies search for documents?
5. Do agencies provide supporting reasons for their decisions?
6. Do agencies meet the time requirements?
7. Do agencies conduct reviews of decisions?

¹ More details... <http://www.premiers.nsw.gov.au/NSWCommunity/FreedomOfInformation/>

- appeal against a decision not to grant access to information or to amend personal records.

It follows that in order to comply with the Act, departments and agencies need to manage their information in a manner that enables them to trace, recover, and reproduce the information requested within the Act's stipulated period (generally 21 days). Sound information management is therefore essential.

Background

Dealing with FOI requests can be difficult for agencies. They may believe that information they provide could be taken 'out of context' and give an unfair view of their operations. Releasing information about sensitive decisions they have made may be embarrassing. Senior staff may also be well aware that certain information they release could be used in a political context and create difficulties for their Minister.

The FOI Act recognises that agencies might be tempted to avoid these potential difficulties, by using the discretions set out in the Act to limit the information released. This would frustrate the spirit of the Act, so it specifically requires agencies to apply FOI laws in a way that favours disclosure of information. While this audit covered only three agencies, we believe that the issues and recommendations relate to all bodies that handle FOI requests including Ministers, most NSW government agencies, and local government.

Audit scope

Against this background, we reviewed the FOI arrangements within three government agencies²; we also examined 84 FOI requests for non-personal information.

A full copy of the Freedom of Information report, on which this article is based, is available on the Auditor General's web site...

<http://www.audit.nsw.gov.au/repperf.htm>

In order to test key provisions of the Act, we focused on requests in which access to non-personal information was refused, granted in part, or subject to an internal review. We selected FOI requests for non-personal information because they were more likely to involve policy-related information and offer an insight to government decision-making (most of the requests we examined were made by media personnel or Members of Parliament). We did not review the basis of these decisions, but whether the agencies had acted in accordance with the spirit of FOI legislation; in particular, with Section 5(3) the Act, which requires agencies to behave in a manner that furthers its objectives to *...facilitate and encourage, promptly and at the lowest reasonable cost, the disclosure of information* [Section 5(3)(b) of the Act].

We also focused on the agencies' processes for handling requests; for example, for providing assistance to applicants, assessing costs, locating documents, response times and making decisions on access to information.

Audit Findings

During the audit we identified a number of concerns that we subsequently raised with the appropriate departments; these are described in our full report, which is available to download from the Auditor General's web site. I would like to focus on two of them; independence in decision making, which goes to the heart of an equitable FOI process, and the important administrative role of FOI Coordinators.

Independent decision-making

We found that standard practice in the MoT, and in about 25 per cent of the cases we reviewed in the Premier's Department, was to refer proposed determinations to the chief executive (CEO) before they were finalised and sent to the applicant. In DET, the records suggest that two draft determinations were discussed with the then Minister's Office before being finalised.

We have three concerns about the involvement of CEOs or Ministerial staff prior to a determination being made:

- it opens the possibility for perceptions of interference, even though this may not have been intended;
- it may affect an agency's capacity to conduct an unbiased internal review, as it must be undertaken by someone *who did not* "deal with" the original application and *who is not* subordinate to the original decision-maker;
- it presents efficiency issues, as agencies have tight timeframes to meet FOI requirements.

It may be necessary to contact the office of the CEO or the Minister to ascertain the documents that exist and their exemption status. This is not where our concern lies. We also recognise that it is appropriate for CEOs and Ministers to be informed of decisions. However, we believe this is best done when the applicant is advised of the determination. This process issue is an important one in our view, is easily solved, and would resolve all of our concerns on this matter.

² Ministry of Transport (MOT), Premier's Department, Department of Education and Training (DET)

At least half of the officers we interviewed in DET and MoT reported that, at some stage, Ministerial staff or senior departmental officers sought to be involved in the review of determinations or participate in the decision-making process. Sometimes they attributed this to particular individuals who misunderstood or were unaware of the provisions of the Act. Others reported that the situation had improved following a change in managements' attitude or a more centralised FOI process.

In a small number of the cases we examined, involvement of this nature affected the outcome of the determination. The CEO of the former MoT suggested that proposed determinations for two requests be revised or altered. Subsequently, one matter appeared to

have lapsed and no determination was made. The other remained unchanged. In this case, the CEO sought unsuccessfully to release more information than had been proposed. When we discussed these cases with him, he indicated that it was his policy not to interfere. However, he believed there were special circumstances, and his concerns were documented on file to ensure transparency. In DET, agency records suggest that one draft determination was altered following comments from staff of the then Minister.

The Role of FOI staff

FOI Coordinators play an important role in ensuring agencies comply with the spirit of the Act. They manage all the stakeholders in the process - the

applicant, search unit, any third party, and the decision-maker - and monitor time limits. They must also be aware of the Act's requirements, including any new judgments made by the courts or the NSW Ombudsman. We found that FOI Coordinators and their staff supported the Act's objectives. A number of the issues raised above were caused by factors outside their immediate control, for example dealing with uncooperative or uninformed units elsewhere in the agency.

It is important that agencies ensure that all staff, not just those directly involved in processing requests, are aware of the Act's aims and key provisions. FOI Coordinators should be at a relatively senior level in the agency with authority to administer FOI arrangements as required.



freedom of information

Conclusion

Overall, we found that FOI Coordinators and their staff supported the legislation, but the agencies examined can do considerably more to achieve the intentions of the Act.

On the positive side, each agency had made a number of changes to improve the effectiveness of their processes for handling FOI requests. In most cases, they did not charge processing fees, but if charged the fees were reasonable.

However, we believe that further improvements should be made to address the following issues:

- processing fees being charged in some cases and not others even though a similar amount of work had been undertaken;
- little documented evidence of the extent of searching which had been undertaken to locate documents, making subsequent reviews more difficult;
- supporting reasons for refusing access to information not always being provided to applicants;
- involvement of CEOs or Ministerial staff prior to some determinations being finalised, which opens the possibility for perceptions of interference and may affect an agency's capacity to conduct an unbiased internal review;
- no routine or formal analysis of reviews of decisions to determine whether changes in practice are required;
- timeframes not being achieved.

DET advised us that prior to the audit it had been reviewing its FOI performance and was implementing a number of reforms (developed in consultation with the NSW Ombudsman) to improve the effectiveness of its FOI process. The Premier's Department and the MoT already have, or plan to change various processes to address the issues we raised.

All agencies that handle FOI requests should...

Assist applicants:

- clarify the scope of FOI requests at the earliest opportunity, particularly for large and complex applications;
- provide applicants with information on the FOI process and the status of their request.
- ensure that decisions on access to information are made independent of any undue influence;
- ensure that all staff are aware of the purpose and key provisions of the Act;
- ensure that staff involved in the FOI process have full authority to make decisions as required under the Act.

Fees and charges:

- ensure that fees and charges are applied consistently.

Searching for documents:

- conduct thorough and complete searches for documents;
- document the types of searches undertaken to locate information;
- ensure that adequate records management systems are in place to facilitate document searches.

Making decisions on access:

- document the decision-making process, including all deliberations and viewpoints considered;
- provide supporting reasons for refusing access to information;
- identify all relevant documents to the applicant;
- advise all applicants of their right to appeal.

Independent decision-making:

- inform CEOs of the outcome of decisions in parallel with, rather than prior to, issuing the determination to applicants;

Internal reviews:

- ensure internal reviews are conducted by someone other than, and more senior to, the original decision maker, as required by the Act;
- introduce formal systems for reviewing the outcomes of internal and external reviews of FOI determinations.

FOI laws:

Any review of FOI legislation in NSW should consider:

- the value of *Statements of Affairs* and *Summaries of Affairs*, and whether they serve their intended purpose;
- extending timeframes when consulting the applicant or handling large multi-faceted requests.

Review mechanism:

The Government should consider introducing a review mechanism that routinely oversees FOI arrangements in NSW government agencies.

About the author

Stephen Horne is a Director in the Performance Audit Branch of the Audit Office of New South Wales. He has twenty-five years' experience in a range of organisations in the NSW public sector, and is a recognised authority in the fields of e-government; corporate governance; fraud control strategies; corruption prevention, and performance reporting. Stephen has also contributed widely to public sector improvement in a variety of capacities, including responsibility for over forty major performance audits.

Stephen Horne, B.Bus (Distinction) UTS, FIIA.
E-mail... stephen.horne@audit.nsw.gov.au Website... <http://www.audit.nsw.gov.au>



About Us

The New South Wales Auditor-General...

helps the New South Wales Parliament hold Government accountable for its use of public resources is independent of Government and reports directly to the Parliament operates under the Public Finance and Audit Act 1983.

The Audit Office...

supports the Auditor-General in his work reviews more than 400 New South Wales government agencies to:

- give Parliament reasonable certainty that agencies' financial reports are prepared correctly;
- confirm that agencies adhere to specific laws, regulations and Government directions.

- investigates allegations of serious and substantial waste of public money

determines whether an agency or government activity is achieving what it set out to do, economically, efficiently and according to the law has 205 employees.

Vision...

to be recognised as a centre of excellence in auditing.

Mission...

to assist Parliament to improve the accountability and performance of the State.

Values...

- Independence – work without fear or favour.
- Equity – be fair, just and impartial.
- Integrity – be open, honest and reliable.

Empathy – be understanding of others.
Customer Focus – be courteous, professional and add value.

Continuous Improvement – listen, think, challenge and work smarter.

Clients...

our clients are the Parliament of NSW, the Government and its agencies, and ultimately the public of NSW.

Scissors used to open the Sydney Harbour Bridge in 1932, NSW Parliament House



Sydney Harbour Bridge

Dig the SPACEDIRT

"To fail to plan, is to plan to fail". IEEE 829 is arguably still the most used software testing standard."

"Why standards? The use of standards simplifies communication, promotes consistency and uniformity, and eliminates the need to invent yet another (often different and even incompatible) solution to the same problem. Standards, whether 'official' or merely agreed upon, are especially important when we're talking to customers and suppliers, but it's easy to underestimate their importance when dealing with different departments and disciplines within our own organisation. They also provide vital continuity so that we are not forever reinventing the wheel. They are a way of preserving proven practices above and beyond the inevitable staff changes within organisations." [Ed Kit - Software Testing in the Real World]

That paragraph neatly and (quite) succinctly describes why standards exist. But how does that affect testing practitioners who live, as in the title of Ed Kit's book, in the real world?

Anything that promotes better project communication has to be good for testers. Standards have, therefore, to be effective and produce recognisable (and

measurable?) gains while not adding disproportionate overheads. I once worked for a large organisation that had an internal (and mandatory) standard for almost all documents. It was such that its use transformed a document of 200 real words into 18 pages after all the necessary parts (glossary, 'associated documents', etc) were added. Perhaps this was counterproductive and unnecessary.

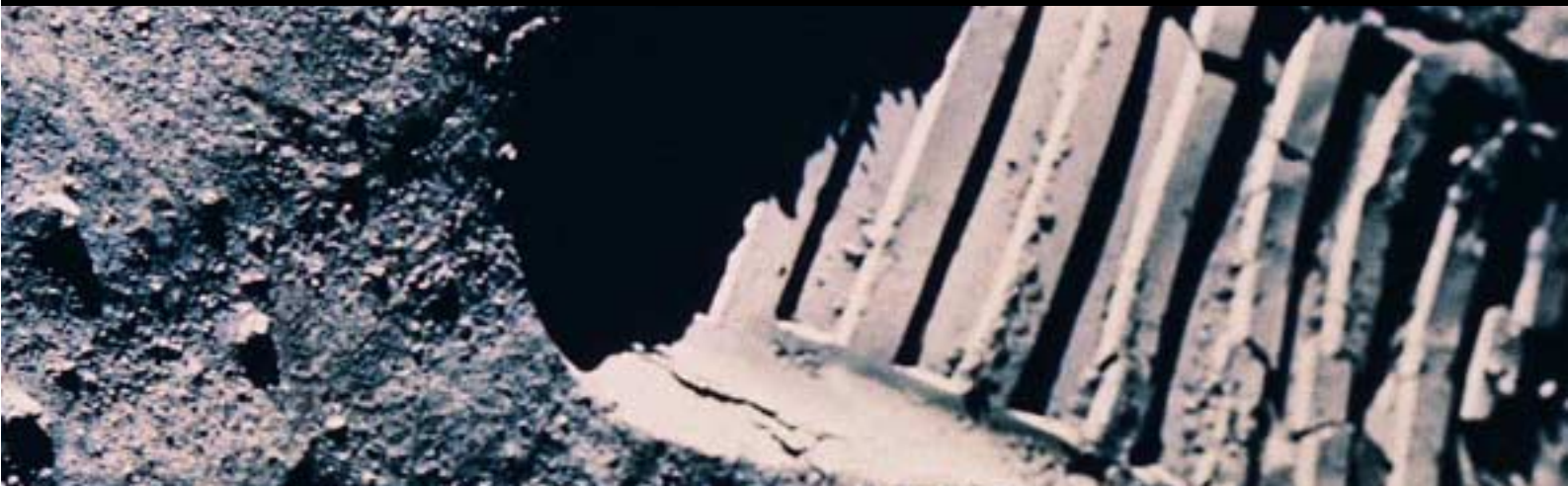
An overview of IEEE 829

There have been diverse document types used in software testing, developed in many cases for the needs of a particular organisation. IEEE 829 (1983) - the **Standard for Software Test Documentation** - was an attempt to pull sources together and present some best practice ideas. The standard was revisited and revised in 1998. Please note that the standard applies to any level of testing that may take place, including acceptance testing, although its application in agile development methodologies may be less obvious. It is usual to have 'a full set' of IEEE 829 documents for each testing stage that is to be undertaken.

IEEE 829 is often thought of as being the standard for a "High Level Test Plan" or "Master Test Plan" (**HLTP or MTP**). It is more than this, as the standard describes eight documents that can be produced as part of the testing effort. These documents are sometimes distributed between different categories and although there is no consensus on the subdivisions, I find the following partitioning helpful:

- **Test Planning**
 - Test Plan
- **Test Specification**
 - Test design specification
 - Test case specification
 - Test procedure specification
- **Test Reporting**
 - Test Item transmittal report
 - Test log
 - Test incident summary
 - Test summary

Most of these eight document types are well known, but figure 1 (opposite) provides a very brief summary.



Test planning revisited

Test planning is a key activity in any software testing project and for that reason many would associate IEEE 829 *only* with test planning. The standard defines 16 items that should be considered for an MTP, including the key activities of estimation ('schedule' is one of the 16) and risk, both of which are large topics in their own right.

The 16 are given below for completeness together with a well-known mnemonic (SPACEDIRT) for remembering the list; more detail on each can be found in textbooks and on web sites that deal with this subject:

S Scope	test items, what to test, what not to test
P People	training, responsibilities, schedule
A Approach	the approach that will be taken to testing
C Criteria	entry/exit criteria, suspension/resumption criteria
E Environment	test environment needs
D Deliverables	what is being delivered as part of the test process
I Incidentals	introduction, identification (of the document), approval authorities
R Risks	risks and contingencies
T Tasks	the test tasks that are involved in the testing process.

It is worth noting at this point that the standard lists as 'deliverables' the seven other document types that perform part of the standard. Some organisations add to this basic list by including key items such as 'glossary' and 'references' to other documents. I usually keep MTP documents from previous projects and for projects that I worked on for other organisations, so that I can look back and see what specific details were included.

MTP is a LIVING document

This document specifies what is going to be done and how it is going to be done. It needs to be published, to appropriate people, to make others aware of what is - and what is not - going to be tested. However, don't wait for everything to be completed before the document is circulated for comment and/or review. The MTP will change during the life of the project, but this does not mean that

it is unnecessary to obtain individual and departmental sign-off; sign-off is achieved based on what is known at the time. In one organisation, sign-off is achieved by stating that unless this is received by a specified (and realistic) date, it will be assumed. It is remarkable how that concentrates the minds of those concerned!

Two areas that indicate the dynamic nature of the MTP concern schedules and risks. During the testing phase, good news and bad news can act to change priorities. Does this mean that the original MTP was wrong? No; the MTP is what its name suggests, just a plan. At the time, it was based on the best available information, incomplete though this was. Information will improve as testing progresses; for example, what was once a critical risk might now have been addressed (e.g. by third-party security testing). The risk is now answered and will possibly require no further action.

Figure 1 The eight parts

Test Plan	A high level view of how testing will proceed; WHAT is to be tested, by WHOM, HOW, in what TIME frame, to what QUALITY level.
Test Design Spec	Details the test conditions to be exercised, with the expected outcome (in general terms).
Test Case Spec	Specific data requirements to run tests, based upon the test conditions identified.
Test Procedure Spec	Describes how the tester will physically run the test, including set up procedures. The standard defines ten procedure steps that may be applied when running a test.
Test Item Transmittal	The recording of when individual items to be tested have been passed from one stage of testing to another. This includes where to find such items, what is new about them, and is in effect a warranty of 'fit for test'.
Test Log	Details of what tests were run, by whom, and whether individual tests passed or failed.
Test Incident Summary	Details of instances where a test 'failed' for a specific reason.
Test Summary	The Test Summary brings together all pertinent information about the testing, including the number of incidents raised and outstanding, and crucially an assessment about the quality of the system. Also recorded for use in future project planning is details of what was done, and how long it took. This document is important in deciding whether the quality of the system is good enough to allow it to proceed to another stage. This assessment is based upon detailed information that was documented in the Test Plan.



Figure 2 Relationship to other standards

These are some of the other standards that may be referred to when documenting according to IEEE 829:

- IEEE 1008 - Standard for Unit testing
- IEEE 1028 - Standard for Software Reviews
- IEEE 1044 - Standard Classification for Software Anomalies
- IEEE 1044-1 - Guide to Classification for Software Anomalies
- BSS 7925-1 - Vocabulary of Terms in Software Testing
- BSS 7925-2 - Standard for Software Component Testing

Review the document

The MTP needs to be reviewed, with reviews taking place face-to-face. If it is contentious, points of conflict need to be talked through. The MTP is not solely "owned" by the testing team(s); developments groups and users can contribute significantly to its clarification and suggest other items to be added.

What is and what is not to be tested, are two key elements in the MTP. In October 2002, I worked on a project where testing was, as always, pushed for time. The MTP specified that significant testing would concentrate on the retail system with respect to '53-week year' processing (2002 - 2003 was a 53-week year). The development team failed to realise the significance of 53-week years, but the mere insertion of the testing intention resulted in better code (development extended unit test coverage, found some problems and implemented fixes).

It is usual for the detail listed in the MTP to be used as a basis for deciding whether the software under test is suitable for the next stage of testing, deployment to production, etc. Thus, key individuals need to see and agree this detail before the crunch implementation meeting!

Facing Reality

The MTP is one place where testing comes face-to-face with reality.

The MTP is not free-standing, but fits into the overall Test Strategy. In some ways, it is not a prescriptive approach, but a checklist to remind those responsible what should be considered for inclusion in the MTP. Its only pre-

scriptive feature is to use of the 16 point "check-list". It is perfectly OK to exclude one of the 16 points, so long as the reasons for excluding it are listed and agreed by the MTP's reviewers. The MTP also includes risks and assumptions; sometimes the explicit statement of a risk or assumption promotes lively discussion, and even resolution!

Conclusion

As a standard, IEEE 829 is not so much about how to test, but how to document that you have tested, and there is interplay between it and other of the project's standards and documents.

Adherence to IEEE 829 is no guarantee that the testing project will be successful. It should not be used blindly as a standard, but appropriately. Testing is a service that adds nothing to the project team's output; a tester does not make better software (and testers should not be allowed to alter code). We therefore need to slay the myth of "documentation for documentation's sake" and ask ourselves "does the output enable the test and/or development teams to do a better job; or help them to present the information found during testing in a clearer way; or demonstrate to an outside agency (e.g. the auditors) that testing has been properly planned and completed?"

Merely incorporating IEEE 829 will not make a success of a project. It can, however, help to make a success by providing guidelines and pointing the way to better understanding and to better documentation.

Where to learn more

Template - Test Plan Template, based on IEEE 829: Systeme Evolutif web-site: <http://www.evolutif.co.uk/tkb/guidelines/ieee829/>)

also...

http://www.cs.swt.edu/~donshafer/project_documents/test_plan_template.html

Sample - SAMPLE Test Plan, again based on IEEE 829: Systeme Evolutif web-site: <http://www.evolutif.co.uk/tkb/guidelines/ieee829/> and then select Sample MTP

Worked example -

http://www.luckydogarts.com/dm158/docs/System_Test_Plan.doc

See also -

<http://www.google.com> and search for "IEEE 829"

All the web sites above were returned from a 'Google' search. The author has no commercial or other interest in these particular sites.

About the author

Peter Morgan is a senior practitioner with **e-testing Consultancy Ltd**, a UK-based company that specialises in training in software testing and in consultancy. The Company provides entry level training leading to the internationally recognised ISEB Foundation Certificate in Software Testing, details of which can be found at the British Computer Society web site - <http://www1.bcs.org.uk/> under ISEB, Qualifications, Software Testing.

Peter's testing assignments have included large-scale UK government infrastructure projects. He can be contacted by e-mail at PMorgan@etesting.com and further details of the company can be found at <http://www.etesting.com>.

This article first appeared in edition 16 of **Professional Tester** (<http://www.professionaltester.com>) and is reproduced with the Editor's kind permission.

GAO Working with Congress to Improve the Information Technology Acquisition Processes

Without properly functioning hardware and software, the US Army's "Future Combat Systems" will be no more than a bunch of dumb boxes that sit and collect dust on the battlefield. Madhav Panwar and Lisa Pracchia of the General Accounting Office explains why Congress now places heavy emphasis - backed up by legislation - on the process for acquiring high quality computer hardware and software for military use.

Recent military operations around the world demonstrate the superiority of US weapon systems developed by the Department of Defense (DOD). Furthermore, an ever increasing percentage of a weapons system's functionality is provided by ever more sophisticated and complex software. While DOD has risen to the challenge, cost overruns and unsatisfactory performance have led the General Accounting Office (GAO) to designate DOD systems development and modernization efforts a high-risk area.

Significant risk factors include the enormous size and complexity of the software used by these systems. Furthermore, most DOD acquisition organizations (i.e., the program offices tasked with defining, developing and fielding weapons systems) lack both disciplined processes for managing software-intensive system acquisitions, and the contractors who develop the IT systems and software embedded in the weapons. As one Congressional source aptly described the acquisition of US weapons systems, "It's not about bending metal any more, it's about routing electrons."

Software enables a myriad of complex capabilities ranging from massive data fusion across geographically disparate large-scale sensor systems; to decision systems that automatically select the most appropriate weapon and platform to attack a given target; and on to autonomous systems that operate without human intervention to destroy incoming missiles. Software will create the network-centric operation, the cornerstone of DOD's transformation.

Other risk factors include the long-standing "cultural" issues highlighted in earlier GAO reports. Two of these remain relevant; the acquisition community's bias towards hardware and their attention to critical software issues too late in the acquisition process. Typically, program managers do not provide adequate oversight of the software phase of an acquisition, relying instead on contractors to manage themselves. While the Software Engineering Institute (SEI)¹ has provided software developers with various process improvement models, it is generally accepted that if the acquisition organization is at a low process maturity, then the entire program is at risk.



Marine Corp's V-22 -
Software Intensive Weapon System

In a 1998 CrossTalk article, Capers Jones of Software Productivity Research, Inc. defined a major DOD system as having 12.5 million C Statements and a development team numbered in the hundreds. A lack of mature development processes and communications were

known to pose problems on such large development efforts. Configuration control and change management were poorly implemented, and documentation and software rework absorbed the bulk of development costs. Partly as a result of these weaknesses, Jones estimated that the probability of a major software-intensive development project being terminated were as high as 65%.



In contrast, today's jointly-developed large weapons systems, some of which form an integrated set of systems (sometimes called "system of systems"), are even larger, with software distributed among many subsidiary systems.

An example is the Army's *Future Combat Systems (FCS)*², a joint Army/Defense Advanced Research Projects Agency³ program. The Army's vision is for FCS to create an integrated "battlespace", where networked information and communications systems provide a

¹ Carnegie Mellon Software Engineering Institute... <http://www.sei.cmu.edu/>

² For more details see... <http://www.darpa.mil/tto/PROGRAMS/fcs.html>

³ DARPA is at... <http://www.darpa.mil>



competitive edge to soldiers in the field and to commanders in the control room. At this early stage in the definition of requirements, one would be hard pressed to estimate the numbers of FCS developers in a program in which the extended team consists of one prime contractor, eight major subcontractors and 55 other companies under contract. According to Congressional sources, "The FCS is estimated at 32 million total Source Lines Of Code". However, the actual number is likely to be far greater, for past experience with software estimation has shown that we both underestimate size, and add functionality as development progresses.

Fielding FCS successfully will require a highly mature acquisition organization, and more mature development and testing approaches than those used in the past on the development of smaller systems. In particular, greater effort will need to be spent on improving processes for managing changes to requirements and for ensuring that information is shared among all stakeholders. Furthermore, program managers will need to exert far greater influence on IT-related issues and obtain more objective "Earned Value" data from contractors. Without properly functioning hardware and software, FCS will be no more than a bunch of "dumb boxes" that sit and collect dust on the battlefield.

Mature processes are essential for ensuring that (a) the requirements are objectively defined, (b) the right management discipline is applied to contract management, and (c) that the software development environment is equally transparent to developer and customer. Other tools, such as Earned Value analysis, will need to be used to ensure that the system functions as intended, and that major problems and errors are caught well in advance of operational testing.

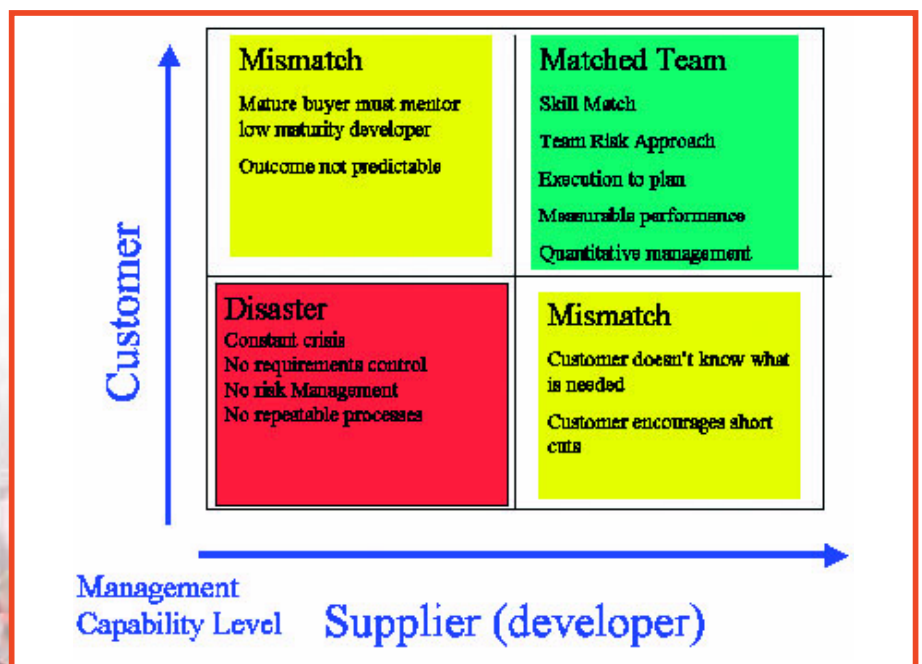
The History

Software Development Process Improvement

In the late 1980s, software developers began to invest in process improvement by adopting best practice models. Many public and private organizations based their improvement programs on the SEI's "Software Capability Maturity Model" (SW-CMM)⁴. Adoption was slow at first, but by the mid-90s, companies with improvement programs were showing results. For example, SEI reported that a major defense contractor who implemented a process improvement program in 1988 had, by

1995, reduced rework costs from about 40 percent to about 10 percent of total project cost, increased staff productivity by 170 percent and reduced defects by about 75 percent. SEI also reported that over an eight year period, a software development contractor had reduced average estimated schedule deviation from 112 percent to 5 percent, and estimated cost deviation from 87 percent to minus 4 percent.

By 2001, software development units within DOD were also showing results from their improvement programs. According to one GAO report, each DOD unit with a software process improvement (SPI) program reported positive results on software/systems quality. For example, the Defense Finance and Accounting Service reported that its SPI program had reduced the overall cost to deliver software by about one-third over comparable organizations; a Navy software activity reported reduced costs and improved product quality, and achieved a 7:1 return on its SPI investment; and an Army activity reported that improvements derived from its SPI program had enabled it to almost double its productivity in writing software for new systems.



⁴ For SW CMM see . . . <http://www.sei.cmu.edu/cmm/>

Software Acquisition Process Improvement

Many defense and civilian contractors who develop software-intensive systems have made performance gains through SPI, but those who acquire the same systems have lagged behind.

Problems occur in situations where low process-maturity acquirers contract for software from high process-maturity developers. Matt Fischer, one of the authors of the SA-CMM, uses this chart to explain why acquirers must also improve their process for managing software contracts.

For example, acquirers may try to circumvent development and management processes because they feel that following them adversely affects their ability to meet their goal. "Process avoidance" by the acquirer can result in rework, additional delays, and unexcusable cost and schedule quotes; had it been followed, this is exactly what the process was designed to avoid.

Other problems can occur at the end of the development process. Where cost and delivery schedules become more important to the acquirer than the developer's obligation to meet their exit criteria for delivering a quality product, the result can be software that contains avoidable defects. GAO reviews of major weapons systems have uncovered consistent problems - such as cost increases, schedule delays and performance shortfalls - for which the underlying causes include pressure on program managers to promise more than they can deliver.

The GAO have recommended⁵ establishing and implementing a DOD-wide SPI program based on accepted best practice improvement models. In response, DOD tasked two working groups within the Office of the Secretary of Defense to develop a plan for implementing DOD-wide SPI and to establish a means of sharing SPI lessons and best practice knowledge throughout DOD. DOD also pointed to a recent revision of their regulation 5000.2-R as

containing the necessary policy guidance. The author believes that subsequent DOD inaction in response to GAO-01-116 played a pivotal role in Congress legislating for software acquisition process improvement.

On 2 December 2002, Section 804 of Defense Authorization Act of Fiscal Year 2003 (or simply "Section 804") was enacted. The report accompanying their version of the Defense Authorization for Fiscal Year 2003 spelled out clearly the Senate's concern about the negative impact of longstanding software problems on major defense acquisition programs. The Senate stated that Section 804 is designed to implement the recommendations set out in GAO 01-116.

Section 804: The Law

Section 804 mandates the improvement of DOD's software acquisition processes. This legislation directly instructs the secretaries of each military department and the heads of relevant defense agencies to establish software acquisition process improvement programs - an apparent message of frustration with the way software improvement has been handled in the past.

Software acquisition process improvement program requirements include:

- A documented process for software acquisition planning; requirements development and management; project management and oversight; and risk management.
- Efforts to develop appropriate metrics for performance measurement and continual process improvement.
- A process to ensure that key program personnel have an appropriate level of experience or training in software acquisition.
- A process to ensure that each military department and defense agency implements and adheres to

established software acquisition processes and requirements.

Section 804 also requires the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (in consultation with the Under Secretary of Defense for Acquisition, Technology, and Logistics) to:

- Provide applicable improvement program administration and compliance guidance, and to ensure that secretaries of the departments and agencies comply with that guidance.
- Assist departments and agencies with their respective improvement programs by ensuring that they use applicable source selection criteria and also have access to a clearinghouse for best practice information on software development and acquisition in both the public and private sectors.

Congressional Intent

"Anyone looking at the past Congressional actions and listening to the frustration expressed in Congressional Hearings will find the fundamental improvements mandated in Section 804 come as no surprise. The only surprise is that Congress has been as patient as they have been. Now, Congressional patience seems to be turning to impatience; an impatience to see significant improvement in fixing our perennial problems with cost, schedule, and performance - and in addressing the underlying drivers that are causing these problems."⁶

Congressional sources affirm that "DOD is going to have to pay attention from the ground up, in other words, at the program manager level, or programs will continue to get tanked. Congress will remain interested and we're not going to let this go until DOD significantly improves how it acquires software-intensive systems. The only way it's going to get fixed is by people on the inside - it simply makes no sense on any level to continue ignoring it."

⁵ See report GAO-01-116 (DOD Information Technology: Software and Systems Process Improvement Programs Vary in Use of Best Practices), published in March 2001.

⁶ Norm Brown, Founder and Former Director of the Software Program Managers Network, and Navy Department Member of the 2000 Defense Science Board Task Force on Defense Software.

DOD Response and Implementation Guideline

On 21 March 2003, DOD issued a memorandum to provide the uniform implementation guidance that Section 804 requires. This memorandum identifies applicability, delineated organizational roles and responsibilities for overseeing implementation, and clarifies initial expectations for DOD Component process improvement programs. It also instructed military departments and those defense agencies that manage major defense acquisition programs to establish software acquisition process improvement programs. Requirements for these programs included defining and applying measures; following applicable methods based on some structured approach that includes an appraisal method; and determining and reporting the status of process adherence and performance effectiveness.

The DOD memorandum also gives the Office of the Secretary of Defense Software Intensive Systems Steering Group the role of leading a DOD-wide effort to improve software acquisition processes. This role entails providing program guidance; identifying best practices; establishing a clearinghouse of information regarding best practices and lessons learned in software development and acquisition; and providing guidance for documenting, performing, and continuously improving a minimum of eight specific software acquisition processes.

Conclusions

Section 804's mandate for DOD software acquisition process improvement programs is here to stay. It is not one-time legislation with little or no follow-up, but the result of a consistent, well documented and growing need. Congressional sources are already considering actively identifying certain key programs for greater scrutiny to see if they have adequately implemented the legislation's requirements. According to GAO sources, *"the outcome is what's important, and not which best practice*

Highlights of Recent GAO Reports Relating to Acquisition Process Improvement

GAO report GAO-01-116 (<http://www.gao.gov/new.items/d01116.pdf>):

- Compared and contrasted DOD software and systems engineering practices with leading best practices.
- Recommended issuing a DOD-wide policy implementing SPI for software-intensive systems based on SEI best practice improvement models; developing a program to gauge compliance to that policy; and developing a means of sharing SPI lessons learned throughout the DOD.

GAO report GAO-02-9 (<http://www.gao.gov/new.items/d029.pdf>):

- Reviewed the quality of the Defense Logistics Agency's processes, its application of best practices and opportunities to improve.
- Recommended issuing a DLA-wide policy requiring software-intensive acquisition projects - both the acquirers and contract developers - to achieve a specific level of process maturity based on a combination of SEI improvement models; and to establish/sustain a software process improvement program.

GAO report GAO-02-701 (<http://www.gao.gov/new.items/d02701.pdf>):

- Assessed the impact of design and manufacturing knowledge on DOD program outcomes, compared best practices to those used by DOD, and analyzed current weapons system acquisition guidance for application of best practices to obtain better program outcomes.
- Recommended taking steps to close the gaps between the current DOD acquisition environment and best practices; ensuring that its acquisition processes capture specific design and manufacturing knowledge at key junctures; and providing incentives to use knowledge-based processes.

GAO report GAO-03-476 (<http://www.gao.gov/new.items/d03476.pdf>):

- Provided an independent, knowledge-based assessment of 26 major defense acquisition programs to gauge projected attainment of program goals relative to best practices.
- Observed that when programs proceed with less knowledge than suggested by best practices, cost, schedule and performance problems often result; to varying degrees all programs assessed proceeded with inadequate knowledge at key junctures and suffered negative consequences.

improvement model is used as a road map to achieve the mandated requirements." Given that the GAO and Congress both feel that the acquisition of systems with major software components needs to be

improved, it is imperative that DOD program managers understand that their efforts will be measured against Section 804 requirements.

Madhav S. Panwar and Lisa Pracchia

A chilling thought!

"There was of course no way of knowing whether you were being watched at any given moment."

George Orwell, "1984"

Author and wit Quentin Crisp described euphemisms as "*unpleasant truths wearing diplomatic cologne*"; and on matters concerning cologne, Quentin was a force to be reckoned with.

My daughter's social security number recently dropped through our letterbox, a gentle reminder from the State that time had come to commence a lifetime's toil. Although several years of study lie ahead, the college vacations now offer the opportunity - so Jean informed us - to supplement the pittance paid her by her miserly parents. This was excellent news indeed, for my daughter has developed a remarkable talent for outlay and it was heartening to see her become immersed in the *Situations Vacant* columns of our local rag. Having learned not to play with fire I didn't enquire too closely about her intentions, but it came as quite a surprise when,

some days later, Jean announced that she was to start work as a "console operator".

Console operator? Perhaps I've been around IT for too long, for the vision that flashed through my mind on hearing this news was one of watchful technicians confronting a bank of message-laden screens on the operations bridge of some Big Blue installation. Alas, not so. Just as the Head Programmer of old has transformed into the service provider's Chief Software Architect; Learning Solution Consultants have displaced Trainers; and Public Relations Officers now style themselves Media Outreach Coordinators, I guess that I shouldn't be surprised to find our local supermarket's checkout girls also wearing a discrete splash of diplomatic cologne. After all, when properly considered, "console operator" isn't an entirely misleading description of their role, for what are the innocuous looking point-of-sales terminals they attend but consoles, optimised to pour an endless stream of purchase data (yes, even my one-horse town has 24 x 7 shopping) into the company's ever-churning accounting, supply chain and data mining systems?

Supermarket retailing has moved a world apart from the high street grocery stores of my youth. Refrigeration and sleek vacuum packaging have put paid to the suspended sides of ham and bacon, the whole cheeses, and the sacks and

casks of various comestibles that together gave rise to the characteristic and unforgettable grocery store aroma¹. Gone is the marble-topped counter resplendent with bacon slicer, coffee grinder and brass weighing scales, crowned by a cash register exhibiting similar architectural lines to the Bank of England. Gone also is the apron-clad proprietor who, much to my dismay, always had time to update my mother on all the local gossip, and in full and complete detail! These changes owe much to Piggly Wiggly.²



Piggly Wiggly®

Piggly Wiggly was the creation of Clarence Saunders, an American, who to the grocery trade was what Charles Babbage was to computing, a creative genius with ambition. Whereas Babbage's mission was to enhance the quality of mathematical tables, Saunders' strove to improve shopping for customer and grocer alike. Despite his

The bar code...

...a method of automatic identification that allows information to be captured quickly and accurately by a computer. A bar code symbol consists of a series of bars and spaces of various thicknesses. These are broken down into groups of bar/space patterns that represent human readable characters.

¹ Visitors to London can still sample that aroma in the Food Hall at Harrods. Well worth a visit.

² Piggly Wiggly... <http://www.pigglywiggly.com/>

later attempts at automation being, like those of Babbage, for another age, Saunders introduced many successful and startlingly simple innovations, including that which underpins the supermarket concept, "self-service".

In grocery stores of the time, shoppers presented their orders over the counter to sales assistants, who then gathered the groceries from the store's shelves. Saunders' idea was that the customer would do this by walking around the store with a basket (the supermarket trolley was a much later innovation). And the payoff? Customers received the benefits of greater variety, lower prices and quicker shopping, but gone forever was the old high street grocery store with its characteristic aroma, furnishings and personal service.

Saunders opened his first Piggly Wiggly store in Memphis in 1916 and it quickly became popular. Customers entered through turnstiles and with no assistants to shop for them selected their groceries from open shelves, paying for them at a "checkout". Piggly Wiggly went on to become a group of independent franchises, which by 1929 was the second largest grocery group in the US and its creator a millionaire. Then came the Wall Street Crash followed by a legal dispute with the New York Stock Exchange that drove Saunders into bankruptcy. Although Piggly Wiggly survived - and remains alive and well - Saunders had no further connection with the business.

Not a man deterred by setbacks, Clarence Saunders went on to experiment with automated self-service shopping. In his *Kedoozle* store - a name derived from the phrase "key does all" - the merchandise was displayed as single units each within a glass cabinet under which was a keyhole. Customers entering the store were handed a small pistol-like key that they placed in the keyhole below the goods they wished to buy, the quantity being determined by the number of times they pulled the key's trigger. This action, recorded on punched tape, activated back office machinery to assemble the order, which was then despatched to the checkout on a conveyor belt. On reaching the

checkout, the customer's tape was run through a reader to produce the bill, their groceries being assembled, boxed and waiting for collection. No need for shopping trolleys while there were savings in space, in the labour needed to stock the shelves and in the time customers spent queuing at the checkout. Alas, the machinery proved unreliable, particularly at busy times and the resulting delays coupled with a heavy maintenance bill killed Keydoozle.

Saunders never fulfilled his dream of truly automated shopping. At the time of his death in 1953, he was planning another automatic store based on a system he named "Foodelectric". And Piggly Wiggly? Saunders' reason for choosing this intriguing name remains a mystery. A story has it that it suggested itself when he saw several little pigs struggling to get under a fence from the window of a passing train. When asked why he chose such an unusual name Saunders' reply was, "So people will ask that very question". One can't argue with that!

An icon for today

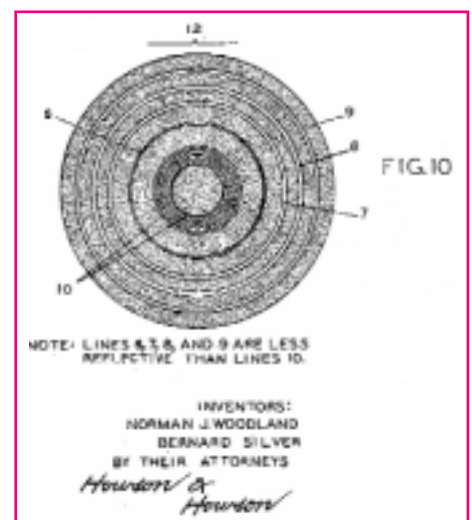
Visitors to the Smithsonian Institution's National Museum of American History will not be surprised to find a pack of Wrigley's chewing gum displayed among other icons of American culture. But this particular pack of gum is more than that; on 26th June, 1974, it became the first bar coded product to be lifted from a supermarket trolley by a long-forgotten customer, and scanned at a checkout.

Looking around me I see several items branded in this way; the case of the CD I'm listening to, a book, a couple of magazines, the covers of some document folders lying on my desk beneath a can of Coke, all bear prominent bar codes. If I looked in our refrigerator, I'd find more. Back at the office, our electrical and IT equipment is bar coded to streamline identification during inventory. Conference delegates are sometimes asked to wear a bar coded ID badge, as are hospital patients; airline passengers' luggage, packages sent through the mail, and just about everything sold in a supermarket are bar

coded to aid identification and tracking. NASA relies on bar codes to monitor the thousands of heat tiles that need replacing after every space shuttle trip. Researchers have even placed tiny bar codes on individual bees to track their mating habits. The ubiquitous bar code is truly an icon for today.

The story began in 1948. A student at the Drexel Institute of Technology in Philadelphia overheard the chief executive of a local supermarket chain asking one of the deans to undertake research into a system that would automatically read product information at the checkout. The dean wasn't interested, but Bernard Silver told his friend Joe Woodland about the request and they began working on a solution.

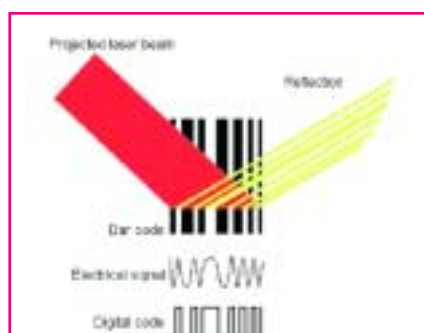
Their first device used patterns of ink that glowed under ultraviolet light. It worked, but the patterns were expensive to print and there were problems with ink stability. Despite the drawbacks, the pair remained convinced they had a workable idea, Woodland even giving up teaching to devote more time to developing a practical system. And the outcome? An application to patent an invention relating "to the art of article classification ...through the medium of identifying patterns". The patent was issued on 7th October 1952.³



In their patent ("Fig 10" is an extract), Woodland and Silver described their bar code as a symbol made up of concentric circles to enable reading from any

³ US patent 2,612,994 can be viewed online at... <http://patft.uspto.gov/netahtml/srchnum.htm> (you may need to install a Tiff image viewer to display it... <http://www.alternatiff.com/>)

direction, but they also described their "symbology" as a pattern of four straight white lines on a dark background, the first being a datum line from which the positions of the other three were fixed. Information was encoded by the presence or absence of one or more of the lines, thus allowing up to seven different article classifications (excluding the datum line, binary 111). However, the inventors noted that by adding more lines it would be possible to encode more classifications (e.g. 10 data lines enables 1023 classifications). A movie soundtrack player served as a bar code reader, but it was bulky and expensive to install while use of a high power



Bar code readers contain a light source, photo detector and signal processing circuitry. The light source shines light onto the bar code, is reflected back into the scanner and focused onto the photo detector, which converts the optical information into an electrical signal. The signal is then "cleaned up" with further circuitry and converted to a signal format that will be recognised by the device to which the bar code reader is connected.

filament lamp made its operation somewhat hazardous. A further problem was that the computers needed to process the information captured by the reader were not readily available in the 1950s.

Bar coding was a sound concept, but it was to be almost 20 years before microchip and laser scanning technologies were sufficiently mature to make it a practical proposition. By then, Bernard Silver was dead - he died in 1962, at the age of thirty-eight - and RCA had acquired the rights to Woodland and Silver's patent. Although Woodland went

on to develop bar coding further for IBM, work recognised in 1992 by the award of the National Medal of Technology by President Bush, he didn't grow rich from an idea that spawned a billion dollar business.

The problem with labelling

New technologies occasionally converge with emerging business demands to bring about a step-change change in the way that things are done. This was to be the case with bar coding.

By the early 1970s, laser scanners and a new generation of intelligent cash register - the electronic point-of-sales (EPOS) terminal - had arrived. These developments coincided with growing competition between the US



Equivalent UPC-A & UPC-E bar codes. UPC-E is a smaller seven-digit UPC symbology often used for small retail items. UPC-E compresses a normal 12-digit UPC-A number into a six-digit code by "suppressing" the number system digit, trailing zeros in the manufacturer's code and leading zeros in the product identification part of the bar code message. A seventh check digit is encoded into a parity pattern for the six main digits. UPC-E can thus be uncompressed back into a standard UPC-A 12-digit number.

supermarket chains that increased pressure on their already tight trading margins. The search was on to cut costs and the most obvious target was the checkout, where the EPOS terminal offered promising possibilities providing that each grocery product could be identified uniquely, automatically and, of course, cheaply.

When a bar coded product is scanned at the checkout, the bar code reader captures the product's unique reference number, which the EPOS terminal then uses as a key to enter a central database to obtain the product's price and description. By this means, it becomes

possible to price any item in the store simply by modifying its entry in the central database. Data captured at the checkout can also be used to track stock levels; to support automatic product re-ordering when stock falls below predetermined levels (a job for electronic data interchange - EDI); to identify fast and slow moving product lines; and, by using historical data, to predict seasonal fluctuations in demand. Furthermore, by cajoling customers into using personal loyalty cards, sales data can be linked to individual customer profiles to determine their purchasing habits (and so into the world of "data mining"). The big drawback is that to devise a labelling scheme for every supermarket chain is not just expensive; it also hinders supply chain integration due to manufacturers having to recognise different supermarket numbering schemes. Product labelling is only cost-effective when supermarket chains work cooperatively with each other and with their suppliers.

Back in 1970, this problem soon became apparent. The outcome was an industry committee, set up to formulate guidelines on barcode development and to devise a standard approach.

Some basic principles were to lie at the heart of the Committee's guidelines:

- to make life easier for the cashier, thereby reducing queues at the checkout, bar codes needed to be readable from almost any angle and at a wide range of distances;
- the labels, which would be reproduced by the millions, needed to be cheap and easy to print; and to be affordable...
- automated checkout systems needed to pay for themselves in two and a half years.

The last goal turned out to be quite plausible. Business consultants McKinley predicted that by adopting a universal labelling system the industry would save \$150 million a year at 1970 prices.

The Universal Product Code (UPC) was to emerge from these deliberations and from development undertaken by IBM (who recalled having Joe Woodland on their payroll).



MaxiCode is a 2D symbology that can encode about 100 characters of data in an area of one square inch. Within this small space are two MaxiCode components: black and white hexagons that pack information in two directions, and a target-like central pattern that allows the symbol to be easily located at high speeds.

The Universal Product Code

Introduced in 1973, UPC was the first bar code symbology to be widely adopted for product marking, in this case by the American grocery industry. Some 250,000 companies in 25 major industries now use the codes to reduce supply chain costs and improve business efficiency.

To obtain a company identifier code, a manufacturer registers with the Uniform Code Council⁴ and then registers each product, thereby ensuring that every package scanned at the checkout bears a unique product reference number. The code comprises two groups of six coded digits (the numbers below a bar code are translations for human use only). The first digit in the first group

indicates the type of product - zero for a national brand; 2 for variable weight, such as meat; 4 for price reductions; and a few other special items. The next five are the manufacturer's code, such as "30000" for the Quaker Oats Company. In the second group, the first five digits form the unique product code while the sixth digit is to verify that all the preceding digits are scanned properly. Thus the scanner will read "30000 06110" as a pound of Quaker's "Cap'n Crunch" cereal, or "30000 01020" as an 18-ounce package of "Old Fashioned Quaker Oats". To enable scanning in either direction, hidden cues in the code's structure tell the scanner which end is which, while printing the bar coded reference numbers on product wrappers during manufacture relieves stores from the expensive overhead of having to label every item they stock.

UPC is not the only bar code symbology now in use, there are many others designed for different industries, including the European Article Numbering system (EAN⁵ - also developed by Joe Woodland), which includes an extra pair of digits and is on its way to becoming the world's most widely used system. The United States Department of Defense adopted "Code 39" for marking all products sold to the US military. POSTNET is the standard bar code used in the United States for ZIP codes in bulk mailing.

An extension to the single dimensional bar code concept are two-dimensional (2D) bar codes that use two axes to enable information about an item to be encoded in addition to its identifying code. Some 2D codes, such as the hexagon-based Maxicode⁶, do not use bars at all.

An icon for tomorrow?

Although UPC symbols form the backbone of all things inventory in the grocery trade, the new Radio Frequency ID (or **RFID**) tag has superseded optical scanning. RFID offers the potential for 'smarter' more flexible supply chain management. It enables products to be identified, counted and tracked automatically, resulting - so its promoters claim - in "near-perfect stock and supply chain visibility".

Products are implanted with RFID tags during manufacture. Each tag contains a microchip on which is stored a unique Electronic Product Code (**EPC**) and a tiny radio antenna. At 400 microns square - a micron (μm) is one thousandth of a millimeter - a tag is smaller than a grain of sand.

As a palette of goods leaves the manufacturer, it passes through a beam of radio waves transmitted by an RFID reader. This causes the tags to "wake up" and begin broadcasting their individual EPCs. Depending on the radio frequency used, RFID systems give a range of up to 30 metres, thus removing the line-of-sight restrictions that apply to bar code scanning.

A local application linked to the readers then queries an Object Name Service database over the Internet. Acting like a reverse telephone directory, the ONS server matches the EPC to the address of a server that holds extensive information on the product; this links to and augments similar systems around the world to form a global database. Because the reader that sent the query is in a known location, the 'system' can identify which manufacturer produced the product, hence, should a product defect or tampering incidents arise, the source of the problem is easily located.

Back at the supermarket, deliveries update the store's retail systems automatically. What's more, because the supermarket's shelves are equipped with integrated readers, they "understand" what stock is being placed on them. When a customer removes an item, the



The EPC is made up of a header and three sets of data. The header

identifies the EPC's version number to allow for different lengths or types of EPC later on. The second part of the number identifies the EPC Manager; most likely the manufacturer of the product the EPC is attached to, for example 'The Coca-Cola Company'. The third, called object class, refers to the exact type of product, most often the Stock Keeping Unit; for example 'Diet Coke 330 ml can, US version'. The fourth is the item's unique serial number that describes exactly which 330 ml can of Diet Coke is referred to. This makes it possible, for example, to quickly find products that might be nearing their expiry date.

⁴ The Uniform Code Council... <http://www.uc-council.org>

⁵ EAN International... <http://www.ean-ucc.org/>

⁶ Example of 2D bar coding: Maxicode... <http://www.maxicode.com/>

diminished shelf immediately routes a message to the automated replenishment system, which if necessary orders further stock. And customer benefits? A reader built into the store's exit recognises each item in the shopper's trolley by their individual EPCs; a quick swipe of the debit or credit card and the customer's on their way. Gone is the checkout with its "console operator", while in another place, Clive Saunders beams with satisfaction.⁷ Perhaps 'RFID' will become tomorrow's icon?

And to conclude, a little science fiction - or is it?

Contrary to George Orwell's grim prediction⁸, 1984 passed free (overall) from his bleak vision of omnipresent state security. Nevertheless, one might reflect on events in the aftermath of 9/11 and on their implications for the future. For instance, it might concern us to learn that the role of the US Information Awareness Office⁹ is to *"imagine, develop, apply, integrate, demonstrate, and transition information technologies, components, and prototype closed-loop information systems that will counter asymmetric threats by achieving total information awareness that is useful for pre-emption, national security warning, and national security decision making."* Buried deep in this bucketful of gobbledegook, *'total information awareness'* sounds uncannily similar to an objective touched on earlier in this piece, *'near-perfect stock and supply chain visibility'*.

In the eyes of some, 9/11 nurtured the business case for tighter state security, while the technology necessary to deliver *'near-perfect stock and supply chain visibility'* is now available. Might business case and enabling technology again combine to bring about another step change, not in the way we identify and track groceries, but people and their possessions? Might the time come when, in place of a letter informing us of our social security number, we're implanted¹⁰ with an Electronic Person Code (EPC) tag at birth? Might a government department exist - Orwell named it "Ministry of Love", *Miniluv* for

An RFID system typically includes:

- a tag or label embedded with a single chip computer and an antenna;
- a radio (much like a wireless LAN radio) that communicates with the tag.

Unlike bar code-based tracking systems, an RFID system can read the information on a tag without requiring line of sight or a particular orientation. The tag can be programmed to hold information such as an item's serial number, color, size, manufacture date and current price, as well as a list of all distribution points the item touched before reaching the store.

short - to keep an outwardly benevolent eye on us, its inner role suitably shrouded in diplomatic cologne by its media outreach coordinators?

Consider a few of the advantages. We always know where our children are or can find out. Gone are the interminable queues at airport check-ins, security and immigration desks; embedded RFID tags ensure that, on arrival, we and our possessions are automatically scanned, identified and verified by reference to a global (and, naturally, error-free) Object Name Service database. What about a 'less-crime', if not a crime-free society? It's a big disincentive to commit crime when the authorities know where everyone and their possessions are at any given moment.

RFID delivers such capabilities on a plate; but there's a question to be asked. Where does state security start and finish and the violation of personal privacy and civil liberty begin? State security ruled OK in Orwell's starkly painted world. As he described it, *"there was of course no way of knowing whether you were being watched at any given moment"*. Might the application of RFID move us in that direction?

A chilling thought!

See diagram overleaf.

Ian Peticrew



⁷ Store of the future movie...

http://www.future-store.org/servlet/PB/menu/1000373_12/1073996191443.html

⁸ George Orwell - "1984" online edition... <http://www.online-literature.com/orwell/1984/>

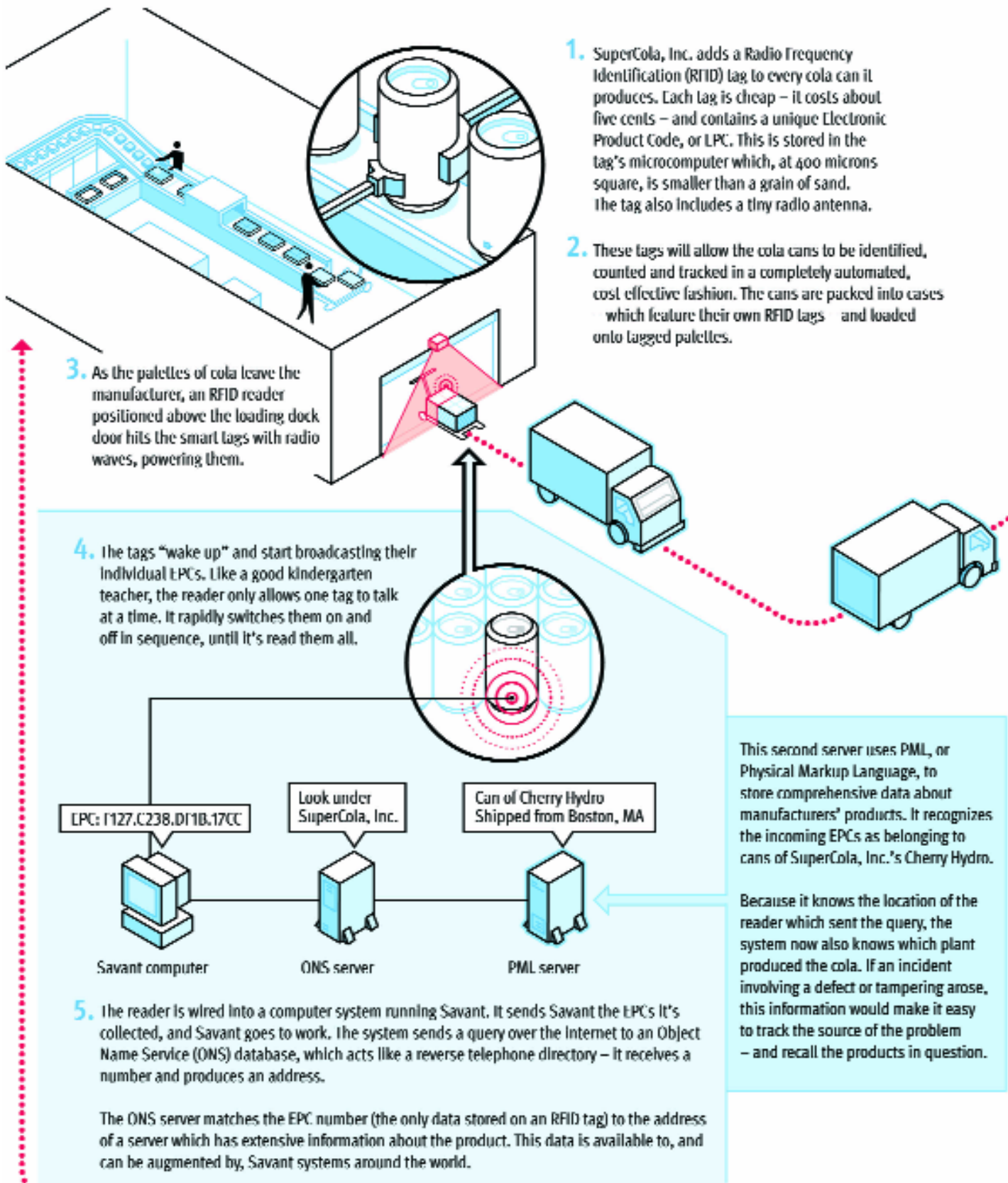
⁹ The IAO web site has been withdrawn, but see...

http://en.wikipedia.org/wiki/Information_Awareness_Office

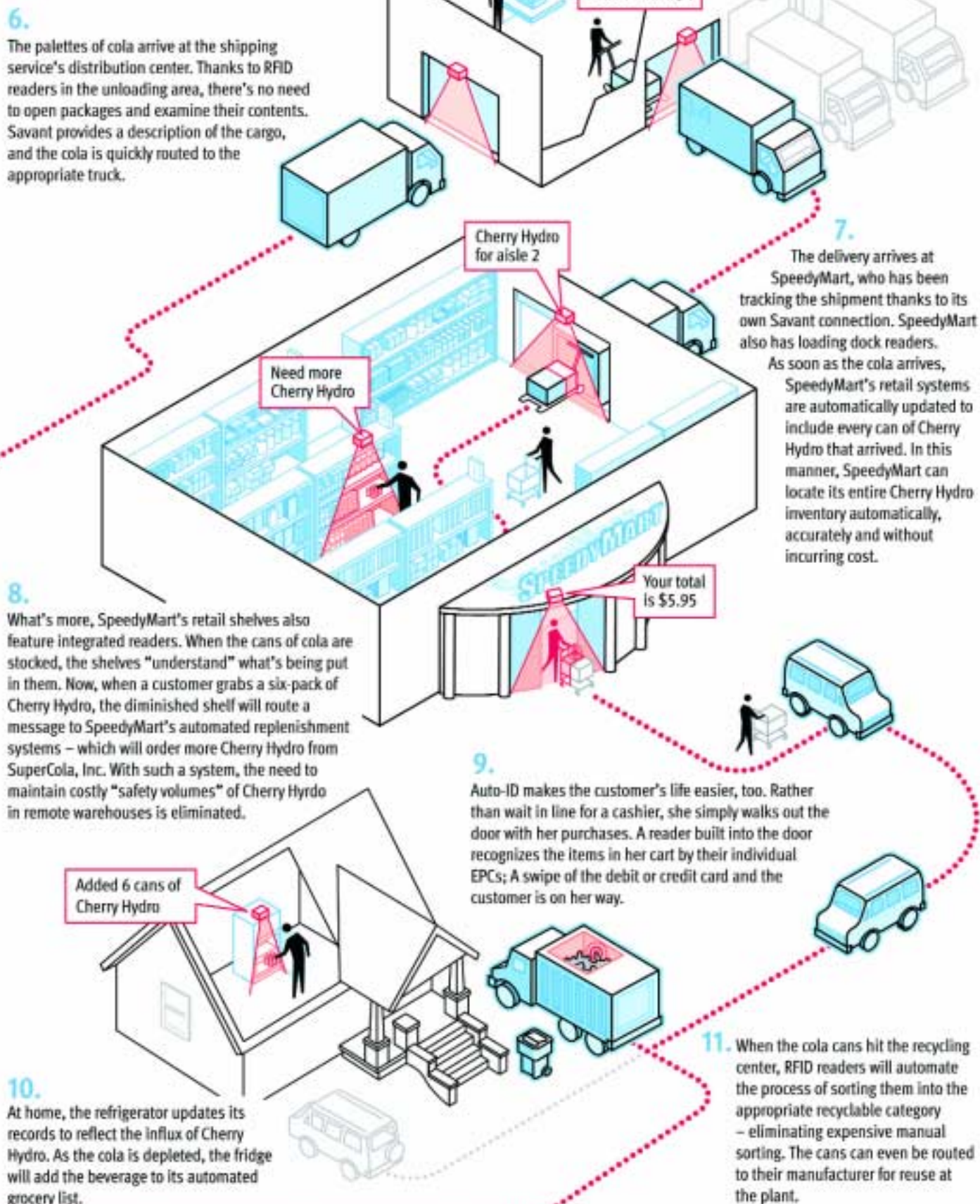
¹⁰ It's quite feasible! See Kevin Warwick, Professor of Cybernetics... <http://www.kevinwarwick.com/>

HOW THE AUTO-ID SYSTEM WILL AUTOMATE THE SUPPLY CHAIN

With Auto-ID technology, physical objects will have embedded intelligence that will allow them to communicate with each other and with businesses and consumers. Auto-ID technology offers an automated, numeric system of smart objects that revolutionizes the way we manufacture, sell, and buy products. Here's how it works:



XPLANATIONS™ by XPLANE®



into IT
THE INTOSAI IT JOURNAL

Layout and Production by NAO Information Centre | Printed by SLSPrint | DG Ref: 3316RD
Printed on **Greencoat** paper. Greencoat is produced using 80% recycled fibre and 20% virgin TCF pulp from sustainable forests.