



www.bcs.org/security

INFORMATION SECURITY NOW

Focus: Enterprise Security


Business attribute profiling

Enterprise security architecture

Asset discovery and clarification

Deperimeterization

In conversation:
Phil Cracknell



The Paradox:

Multiple layers of security make life harder for threats.
Multiple layers of security make life harder for you.

The Answer: Proven security.

Anti-Virus & Anti-Spyware
Network Access Control
Intrusion Prevention
Desktop Firewall
E-Mail Security
Anti-Spam

Security threats are mounting in number—and they're evolving in complexity. Your security must evolve as well. This used to mean managing multiple products without integration, which created operational challenges, risk, and increased costs. Not any more. With McAfee® Total Protection for Enterprise, you'll have comprehensive, integrated protection. You'll control everything—from network access control to anti-spyware to anti-virus—all from a single management console. McAfee Total Protection solutions are engineered to provide maximum manageability and deliver total endpoint security without compromise. McAfee, the dedicated security company that blocked or contained 100% of the top attacks in 2005;* delivers proven results backed by more than 15 years of experience. Secure your business advantage. Learn more at www.mcafeeparadox.co.uk/total

McAfee
Proven Security™

*Top list of attacks as reported by Wildlist.org and McAfee Avert Labs. McAfee and/or additional marks herein are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the U.S. and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2006 McAfee, Inc. All rights reserved.

INFORMATION SECURITY NOW is the quarterly magazine of the BCS security forum, incorporating the Information Security Specialist Group. It can also be viewed online at: www.bcs.org/security/isnow

Design: Brian Runciman, Marc Arbuckle
Managing Editor: Brian Runciman

Editorial Advisors (BCS-ISSG Committee): Gareth Niblett, Roger Smith, Alan Woodroffe, Ian Fish, David Alexander, Rodney Clark, Gary Dooley, Francis Evans, Les Fraser, Julia Harris, Norman Jackson, Mark Jones, Mike Madgin, Mike Nash, Phil Phillips, Tony Phipps, James Robson, Charlotte Walker-Osborn.

Registered Charity No 292786
The opinions expressed herein are not necessarily those of BCS or the organizations employing the authors.
© 2006 The British Computer Society.

Copying: Permission to copy for educational purposes only without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage; the BCS copyright notice and the title of the publication and its date appear; and notice is given that copying is by permission of BCS. To copy otherwise, or to republish, requires specific permission from the publications manager at the address below and may require a fee.

Printed in Great Britain by Holywell Press.
ISSN 1752-2390. Volume one, number one.

The British Computer Society
First Floor, Block D, North Star House,
North Star Avenue, Swindon SN2 1FA, UK
tel +44 (0)1793 417 417;
fax +44 (0)1793 417 444; www.bcs.org
Incorporated by Royal Charter 1984.



ISSG Chairman, Gareth Niblett, reviews the infosec scene

Welcome to the first issue of a new BCS magazine – *Information Security Now*. This incorporates the award winning BCS Information Security Specialist Group’s BCS-ISSG Magazine, and is for those in the BCS who are interested in the broad field of information security.

Rather than have the BCS produce multiple security magazines, this new publication is being produced in collaboration with the ISSG and using the BCS-ISSG Committee as its editorial advisors. It is available electronically to all and in print to BCS-ISSG members.



Enterprise security

The main topic of this issue has nothing to do with a star ship, but nonetheless is about a voyage of discovery into the new and unknown. As businesses become more interconnected and mobile, network boundaries erode, providing more ways for attackers to compromise them. Enterprises need to find new ways of understanding, and coping with, this brave new world.

Businesses are now often wholly reliant on electronic processing of information for their existence and financial well-being. It is more critical than ever for enterprises to take the necessary measures to ensure information remains private, accurate and available at the point of need.

This information is now distributed among known critical business systems, other systems, the (often mobile) workforce and third (and fourth) parties. Ensuring appropriate contractual, procedural and technical controls are in, and remain in, place is a skill that all enterprises need to master.

We face a growing and changing landscape of exposure to vulnerabilities which attackers are more eager than ever to exploit, often before there is a direct mitigation. Financial gain is a great motivator – maybe defenders should learn this lesson as well as the attackers.

The enterprise has to realize that the demilitarized zone (DMZ) has been occupied and the concept of a trusted network needs consigning to the history books. Every system must be able to defend itself from its neighbour, because it will often be impossible to identify friend or foe.

Innovate - don't legislate

Over recent years, there has been an increase in legislation and regulation, both national and international, affecting businesses. The coverage has been broad and shows no sign of abating. Technology is no fix in itself and poorly drafted and misapplied rules do little to help, and often hinder.

As we see increased demands for data privacy, protection, interception, retention, breach notifications and computer misuse, some governments are working around their own rules to access or share information in a way that might be incompatible with legal and official procedures.

No one should have the moral or legal authority to both enforce the law and evade it. The spirit is equally, if not more, important than the letter of the law, and governments should remember this when requiring the rest of us to operate within it.

We should engage more in consultations and lobbying related to forthcoming legislation and regulations that may affect us. If bad ideas or drafting reach the statute book, unintended consequences may well impact on us in a way that damages our ability to be effective businesses, and countries.

FURTHER INFORMATION

Information Security Specialist Group: www.bcs-issg.org.uk
Information Risk Management and Audit Specialist Group: www.bcs-irma.org.uk
BCS Security Portal: www.bcs.org/security
Information Security Now online: www.bcs.org/forum/isnow

Prevention cuts down on laborious forensics

Untangling evidence via computer forensics and taking suspects to court is usually a long and expensive task. It is therefore preferable, where possible, to implement security measures to prevent crime, according to speakers at a forensic event organized by the BCS Information Security Specialist Group (ISSG) on 12 July, Helen Boddy reports.

There are various programs on the market that will help clean and bleach traces of illicit activities on a computer. It is even possible to buy software that will check that cleaning has been effective.

Yet even when a suspect has been particularly thorough in cleaning and bleaching a computer's disk, it is usually possible to find some evidence that can be pieced into a case to present in court, as Professor Tony Sammes of Cranfield University explained

He argued against publishing details of a suspect's actions so that clues are not inadvertently given to other criminals on covering their tracks.

Useful sources for gathering evidence are records of internet activity, according to Jim Bates, both a prosecution and defence expert in computer forensics. Recent investigations have shown how easy it is for 'invisible' pictures

to be sent via email, recoverable by forensic methods but unknown to the user.

Evidence needs to be handled with care. Edward Wilding, computer forensics expert and well known author, claimed it is easy to alter computer evidence, for example, by starting up a windows-based PC.

If handling evidence in a business fraud case, a chain of evidence must be maintained, according to Noel Bonczoszek, an IT crime investigator, and notes made at the time, as they are more likely to be accepted by a court rather than a witness who is relying on memory of an event long ago.

Edward Wilding suggested some key rules when handling forensic investigations:

- quantify the risk;
- obtain expert legal advice;
- maintain operational security;
- establish the chain of command;
- gather your evidence covertly;
- use appropriate experts so that their evidence stands up in court;
- lock down all boxes and dial-in ports; and
- don't discuss investigations by email.

New spam in old Word

Marshal's Threat Research and Content Engineering (TRACE) Team claims a new form of spam is hidden in Word documents. It combines obfuscation and social engineering to bypass anti-spam software and spam-savvy email users.

This latest version of spam looks like a typical business email containing a Word document attachment. The email subject line and file name are also business related, so that recipients are more likely to open it. The message body contains little or no text but the Word document contains the spam message. Users open the document expecting to find an invoice or purchase order and instead find a spam message.

The TRACE team has identified over 100 examples of the new Word spam since it first appeared in August 2006. According to the TRACE team, the new strain is being sent out from a number of different countries, indicating the spam is likely being distributed from zombie PCs.



Businesses blind to pornography threat

New laws making possession of hardcore pornography a criminal offence are a big wake-up call to businesses. Many company directors are unaware what employees may be downloading onto company owned networks, computers, laptops and servers hardcore pornography and violent imagery. Companies also have a duty of care to ensure no pornography is held on their technology and directors could face a three year prison term if violent or child related pornography is found.

Monitoring solutions provider Chronicle Solutions is warning UK organizations that not knowing what material is being downloaded by employees is no excuse and will not protect them from potential financial loss, reputation damage and, increasingly, criminal proceedings.

CEO, Nick Kingsbury, explains: 'Just as Barings Bank was liable for the actions of Nick Leeson, so businesses are liable for the illegal downloading and storing of hardcore pornography. Having corporate policies in place is not enough. The only way businesses can protect themselves is by ensuring they can monitor, identify and prevent such activities.'

Behind the headlines

Legal news behind the Infosec headlines from Struan Robertson of law firm, Pinsent Masons.

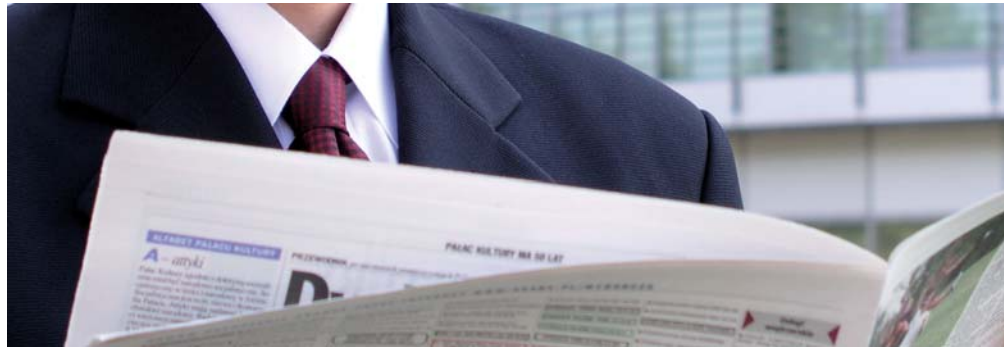
Spamhaus rejects \$11m US judgment

Anti-spam group Spamhaus has ignored a ruling from an Illinois court granting an \$11 million claim against it. The London-based group says it will only answer to a UK court judgment.

Spamhaus is a not-for-profit organization which maintains 'blacklists' of domain names and companies it suspects of sending spam. Those who choose to can have all emails from those companies or domains blocked.

It was sued by US company, e360insight, and its chief executive, David Linhardt. The Illinois court judgment orders Spamhaus to stop taking any action to block or delay email sent by e360 unless it can show that the company has violated US law.

'Spamhaus does not block anyone from sending email,' said Spamhaus chief executive, Steve Linford, in a



statement. 'Spamhaus operates a mail filter advisory system which allows only Spamhaus users to reject incoming email at the point of ingress into their private networks from email senders which Spamhaus advises do not fully comply with Spamhaus's policy for acceptance of inbound email. Mr. Linhardt can send as much email as he likes to anyone on the internet, just not to Spamhaus users.'

Microsoft sues spammer for hotmail breach

Microsoft has won what it described as the largest reported civil award against a spammer in Europe. The software giant says it won a court order requiring spammer Paul Fox to pay £45,000. Rather than pursue a case under Britain's limited anti-spam laws,

Microsoft filed a complaint that Fox had breached the terms and conditions of its hotmail service.

A Microsoft spokesperson said, 'Under a court order, breach of which would be contempt of court and a criminal offence, Mr Fox agreed not to repeat his spamming against Microsoft or any ISP and to pay £45k by way of damages and as a contribution to Microsoft's legal costs.'

Europe may require data breach notification

The European Commission has published proposals for a law change that could force telecoms firms to notify regulators and customers of all breaches of their data security. A similar law in California has resulted in a stream of data breaches being made public.

RFID update

Charlotte Walker-Osborn, Associate Solicitor, Technology Group, Eversheds LLP.

Many will be aware of potential legislation suggested in relation to the use of Radio Frequency Identification (RFID) technology.

To prevent the possibility of a fragmented approach to RFID in Europe, the European Commission has set out an ambitious timeline for the adoption of a policy environment that stimulates the use of RFID technology while providing safeguards for personal data.

Phase one

In a first phase, from March to June 2006, the Commission held five workshops to assess the

potential of RFID for business and society but also addressed concerns about personal privacy and security.

These workshops attracted wide interest from all stakeholders and gained recognition around the world. The final workshops report has now been published.

Phase two

Four months into the initiative, the launch of the online public consultation, on 3 July 2006, marked the second phase of the open and interactive debate.

Your Voice in Europe website provided an opportunity for industry stakeholders and the public to have their say on the all aspects of RFID's development.

The Commission expects this to produce a wide consensus on whether Europe needs a conducive and stable policy environment, encouraging all types of companies to invest in RFID technology and harmonizing technology

standards, while at safeguarding individuals' privacy and security.

The deadline for responses to the online public consultation was extended to 30 September 2006. The results of the consultation can be viewed on the RFID consultation website at: www.rfidconsultation.eu/

Final phase

The final stage in the process of consultation is (at the time of writing) the EU RFID Public Conference on 16 October 2006 in Brussels.

On the basis of these results, the European Commission intend to prepare a Communication to European Parliament and Council.

© Copyright 2006 Eversheds.

This is for general information purposes only and not to be relied upon as a detailed legal source.

Measuring performance and ROI in information security

John Sherwood CEng FBCS CITP considers how to assess return on investment in security in the first of a series of articles.

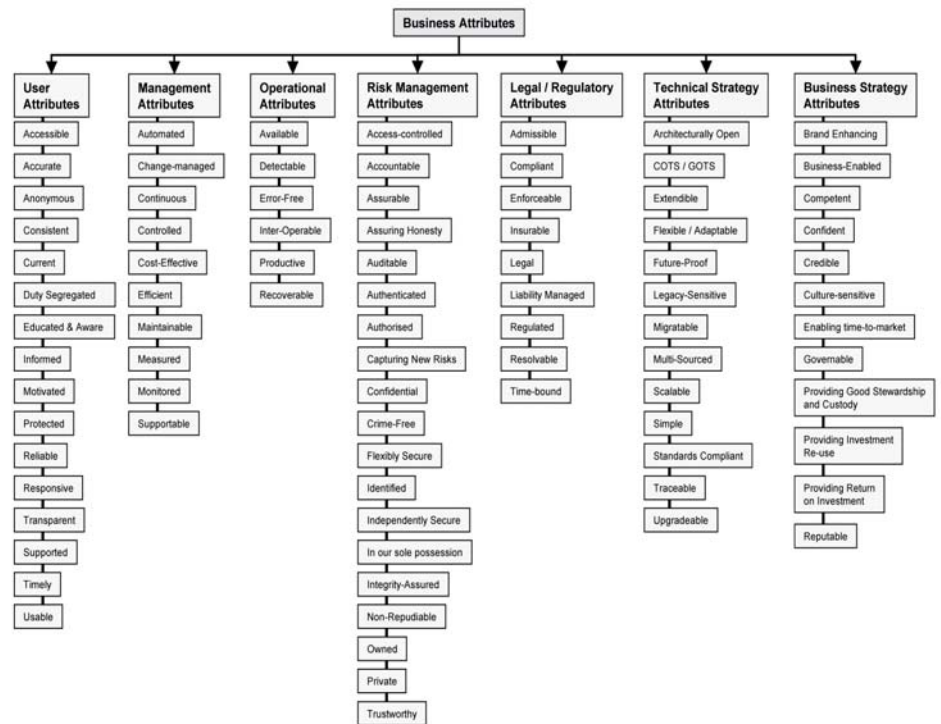
Many famous commentators from many ages of history have pointed out the need to be able to measure the results of our endeavours so as to be able to judge whether or not we are being successful in meeting our objectives.

Among them are counted Galileo, Lord Kelvin and Peter Drucker, all from different eras but all asserting the same thing: if you cannot measure the results you cannot manage the activity effectively. Galileo goes a step further: 'Measure that which is measurable and render measurable that which is not yet measurable.'

The challenge is in the second part of this advice – that if measurement seems to be difficult to achieve, we just need to be innovative and creative in finding new methods that will yield the measurements that we require. This series of articles describes such an innovation for measuring information security performance.

In the early 21st century, when management wisdom is focused on the need to measure business performance in all areas, one of the key challenges facing chief information officers, security architects and information security managers is how to measure security and therefore how to measure the return on investments in security improvements. The topic is raised many times in professional conferences and informal discussions, often with the result that the participants agree that there is a crying need for useful measurements but that there is a lack of suitable methods available.

The key word here is 'useful', because there are lots of things that can easily be measured (such as the number of security incidents in a given period) but they are not always helpful.



Taxonomy of business attributes

The trouble with security is that if it were to be perfect nothing would happen and reporting to management that: 'nothing is happening Boss' is not generally seen as helpful. Indeed it can be seen as a reason to dismiss the entire security team, scrap the improvement projects and save the budget.

Having spent the past 15 years working as information security consultants to a wide variety of clients in many countries and in many industry sectors, we have been able to observe the common themes that recur again and again across this broad cross-section of organizations.

The main themes are that: (1) information security must always be driven by protecting business interests, it could have no other function, and (2) information security is a response to the perceived risks to those business interests.

So, any measurement method must begin by being business focused and

risk focused. Within these high-level themes there are also observable sub-themes that we have collected, analysed and codified into a taxonomy of business attributes organized under seven headings (see diagram above).

This is non-definitive list that often increases with every new client assignment completed. Why are there so many? Because almost every possible attribute of a system or process has some bearing on the fitness of a security solution for the purpose it is intended. In the second of this series articles we shall explain how to use this taxonomy to build a business attributes profile that can be used as the basis of a security performance measurement method.

For more information refer to: [Enterprise Security Architecture: A Business Driven Approach](#) ISBN 1-57820-318-X

www.sabsa-institute.com

Security architecture: what is it and how does it work?

David Lynas FBCS CITP explains that security architecture is often not taken sufficiently seriously.

One of the great privileges that come from advising clients internationally is that I see some impressive local constructions and buildings.

Unfortunately, when it comes to enterprise security architecture my experience is rather different. A recent call from an international financial institution illustrates: 'Please describe the benefits of our security architecture to our management team. To help, here is a diagram of our firewalls and perimeter defence mechanisms.' What they are showing me and their stakeholders is not architecture, it is in fact plumbing.

From the perspective of towns and cities, architecture is more than buildings: it is the set of rules and processes by which we create buildings that serve the functional and aesthetic purposes for which we intend them. The multiplicity and complex interaction of our various needs must be supported and so architecture is based on an understanding of the needs that it must fulfil.

First challenge

So the first challenge facing the security architect is to articulate the business needs for security. Imagine constructing the Golden Gate Bridge before understanding definitively how much weight it must support, how it will resist the effects of salt, or how much it must flex in a high wind or earthquake. Such a design process would be unthinkable and yet that is exactly what the bank did when it implemented an architecture using various exciting technologies and tools: it was technically impressive but no-one was quite sure what it had achieved or why. Resolution requires a common 'requirements engineering' framework and language, meaningful at all levels.

In a field where overall strength is

considered to be that of the weakest link, many security architects are unable even to list the full set of components, never mind define how they actually fit together. This is caused by an approach to security that consists of a multitude of disconnected tactical point solutions, components and operational processes.

Second challenge

The second challenge is to ensure the proposed solution can adapt and remain strategically valuable after go-live.

Consider the contrast provided by Michael Schumacher's Ferrari: every component and process is strategically designed, procured and constructed to work with every other component and process, and the system is engineered to cope with alarming rates of change after deployment. That is truly an architected system and the approach provides a framework within which complexity can be managed successfully.

Just as in traditional architecture where the artisans create their component architectures within an overarching design framework, security architecture must be created as though all components were part of a single project.

Role of security architecture

The role of security architecture is to provide the framework that breaks down complexity into apparent simplicity. This is achieved by layering techniques and there are six such architectural layers: the business view of risks and success factors expressed as control objectives; the architect's view of the strategy for meeting the objectives; the designer's view of the set of logical security services required to deliver appropriate control; the builder's view of the technology model required to deliver the security services; the specialist tradesman's view of specific security products, standards and tools; and the facilities management, or service



management, view of the processes and procedures required to operate and support security services and to secure operational services.

This layering enables the architect to provide traceable evidence that the defined needs are met fully and that the residual risk is acceptable to stakeholders.

In conclusion, whether we discuss architecture of buildings or information security, its role is the same – knowing the difference between architecture and plumbing is a great place to start.

Directories, inventories and the power of triangulation

Phil Venables, chief information risk officer for a leading US-based Investment Bank, explains the importance of asset discovery in assessing information security.

Management of information security is typically predicated on the existence of reliable asset inventories. These enable the assessment of criticality, analysis of risk and prioritization of control enforcement. Most security methodologies start with the statement



'first, find all your assets,' but, how to sustain an asset record is rarely discussed.

Assets can be regarded as items of value in the information space, e.g. servers, applications, databases, information, services, components and people. It is of little value to assess assets once only, a sustained approach is needed for true asset discovery, tracking and naming. This is where directories, inventories, tools and the like are relevant, such as:

- Service provider/vendor directory – to provide a view of service providers. This can either be authoritative in its own right through a registration process, or aggregated from contracts.
- People directory – the key issue is that it represents accurately who is an employee and who is a client as authoritatively as possible, e.g. by linking to the HR and CRM systems.
- Role and hierarchy directory – in simple organizations, this will probably be a series of attributes in the people directory. However, for many organizations people may have multiple roles and exist in multiple approver hierarchies.
- Systems inventory – to provide a precise record of what is where on the network. This can usually be fed from configuration management systems, which may be the inventory itself, or through a process of 'sonar-like' discovery on the network.
- Application directory – to provide a view of the business applications related to the systems on which the application runs. An application directory should maintain information about the purpose and criticality of an application, and, in many cases, the risk and control of that application, i.e. is it a 'privacy critical' application because of the information it manages or the services it provides?
- Data control directory – to resemble a data dictionary but not necessarily with the schematic features associated with it, in other words a record of the macro data types in an enterprise.
- Applications can only be migrated to production if they are in the application directory.
- Payments cannot be made to vendors unless they are in the service provider directory.

These rules are invaluable in helping assure the accuracy of the directory/inventories because their use is embedded in a critical process about which people care. However, the real power comes from more advanced rules that interlink multiple directories around a rule, for example:

- Privacy data only goes to service providers assured at a high level and only from applications designated as privacy critical;
- All employees have their business certifications assessed by a direct manager before access is approved to critical applications;
- Employees in one business division do not have access to applications in another business division unless they are acting as finance managers;
- Applications only run on known registered servers;
- Resilience-critical applications are not dependent on a single service provider or single system.

These represent links between multiple directories, and if there is an actual or attempted violation of these rules, something needs addressing, even if it is only the data in the directory.

In this way, the power of triangulation rules between directories yields wide-scale benefits in terms of control, and provides the feedback loop to sustain accuracy and drive enrichment on those directories. This, in turn, leads to more trust in each directory and to use for other purposes possibly bringing greater immediate financial returns.

Phil Venables can be reached by email at: pip@ieee.org
www.linkedin.com/in/philvenables

Deperimeterization what, why, how?

Raúl Siles, SANS certified instructor, explains the importance of deperimeterization as an enterprise security strategy.

The evolution of enterprise computer networks and enterprise network security during the last ten years helped Jon Measham to coin the deperimeterization term in 2001.

Definition

Deperimeterization is a security strategy designed to protect an organization's IT infrastructure and information assets by applying defence in depth, namely, multiple layers of redundant protection to mitigate the risk of one defence being circumvented.

This reflects the maturity of networks from the castle model to the open model. In the castle model, assets are protected from external threats by a strong perimeter, a well-defined single entry point usually safeguarded by firewalls. In today's IT environments, the perimeter has moved from outer network security to the data centre, to individual computers - such as back-end servers and end-users' data.

Flexibility, agility, mobility and always-on capability demands new technologies, such as remote VPN connectivity or wireless networks. Intruders and security breaches are both internal and external threats so security experts have had to implement new robust security solutions.

Deperimeterization applies network segmentation, strict access controls, secure protocols and systems, authentication and encryption at multiple levels.

Why is it still cutting-edge? The concept is not being applied at enterprise level to its ultimate extent. The main reason is its complexity. Moving from a single protection gateway to the

protection of each resource as if directly exposed to internet, increases the complexity of the model exponentially.

Phase one

In order to manage this borderless world, an organization needs to follow a simplified two-phase methodology approach to deperimeterization. The design phase analyses and identifies an organization's resources or entities. Entities are any IT asset or information, depending on the level of granularity desired. Typically, entities are sections of the network, groups of users or servers, individual systems or applications, or even specific data, such as payroll data.

This phase establishes communication requirements between entities. It provides a security policy defining the list of entities and the links and relationships between them, that is, who can access what or talk to whom, and how.

This methodology should use a 'divide and conquer' iterative approach in order to deal with the complexity. Deperimeterization starts at a higher-level and focuses on the most critical environments, based on a risk analysis. Once the strategy has been applied to sensitive assets, it must be extended in two directions: towards the whole organization, and towards increasing the granularity used to identify new identities.

Phase two

The second phase defines network architecture and security technologies that enforce the policies, helping to implement secure network segmentation. There are hundreds of security solutions to protect and segregate all the entities, at the network, system, application and end-user levels.

At network level, secure internal network topology is required. Most commonly, firewalls compartmentalize

network segments at the network-transport (TCP/IP) or even at application, level. There are other network-based technologies to help isolate resources with a higher granularisation, such as, VLANs, VLAN and port ACLs, private VLANs, or internal IPSec-based VPNs.

At system and OS level, protection is enforced by personal firewalls, anti-virus and anti-spyware software, patching, IDS/IPS, host integrity tools, server-based ACLs, or advanced mandatory access control (MAC) solutions enforcing low-level system security policies. This mechanism manages the 'perimeter' and relationships between basic entities within an IT infrastructure, that is, the system processes, devices, communication end-points, files and users.

All categories of end-users should authenticate and present required authorization credentials to access specific resources within the organization's infrastructure. Access controls should be applied at network level, using the 802.1X protocol, and at system and application levels, using secure protocols (IPsec or SSL-based), PKI, two-factor authentication and network admission controls (NAC), focused on validating the security of computers before granting access to the network.

The strategy must consider the protection of data. All data on, or stored within, the organization's network should be encrypted.

Finally, not only technologies, but security services and processes must be involved in the process. This extends from audit and review of security policies, to system hardening, end-user security awareness, training, periodic security assessments and penetration tests.

www.raulsiles.com
www.sans.org

In conversation

Phil Cracknell, director – technology assurance and advisory at Deloitte, identifies some key issues in enterprise security in discussion with Rupert Kendrick.

Although he probably wouldn't wish to admit it, by his experience alone, Phil Cracknell is something of a veteran in the IT security industry. His recent appointment, as head of Deloitte's security team led by Mike Maddison, speaks volumes for the breadth and depth of his expertise.

'I've been working in information security for over 20 years now,' he enthuses. 'I've worked in a large city bank and consulted for a leading information security consultancy advising heavily influential bodies on security issues.' At one time or another, he always seems to have been associated with some of the most influential organizations, including Sun Microsystems and Checkpoint Technologies. He's just left as director of the security practice at Capgemini. Working for his own company, Phil has had several years offering consultancy services at the highest level.

Ask Phil Cracknell about enterprise security and he'll speak fluently on any issue with a clarity that even a layman can understand. With enterprise security uppermost on the minds of boardrooms these days, he began by evaluating the effectiveness of penetration testing.

'Of course, back in 1996, when it was first identified as white-hot technology, it was, frankly, unfashionable. In the early days, there were, what were known as, "tiger teams" – an American expression – which were teams of individuals hired to break into a system at all costs to test its vulnerability. It originated with the US Defense department (DoD) and at that point there was a real concern that commercial "tiger teams" could be breaking the law.'

Time moved on and essentially the same function is now known by the

much more genteel name of penetration testing or ethical hacking. 'The idea's the same,' he explains, 'it's a purely electronic exercise to expose the weakness of a system and to enable a demonstration to show how vulnerabilities can be remedied.'

But, he points out, it raises almost as many questions as it solves. 'There are tremendous pitfalls for the unwary. Any organization embarking on a penetration testing strategy needs to ask itself some serious questions at the outset – and when it decides the answers to those questions, it needs to be sure that it stays within the perimeters of those answers.'

With fluency and perceptiveness, he proceeds to reel off a series of critical issues which simply may not occur to many organizations.

'For instance, what are the credentials and reputation of the organization performing the testing process? Do any issues of confidentiality, privacy and information assurance arise? Remember that this organization may be investigating the operation of both internal and external networks both of which are likely to reveal highly confidential information and data.'

There's also the question of the scope of the 'attack'. 'Should it be a full scale attack, or should it be limited or partial in scope? Remember, a full scale "attack" runs the risk of bringing

Many organizations don't have a structured or methodical process or plan for conducting penetration testing.



down the whole system and then there's the issue of the resiliency of the system and having to restore it to normal continuity.'

Another issue surrounds the timing of the 'attack'. 'An organization has to decide the best time for a test to be performed. Should it announce it in advance, so possibly enabling something to be concealed from the tester, and, perhaps, compromising the reality of the response because of the advance notice? Or should it be conducted at random, when the quality of the response might be less than desirable?'

Many organizations, he claims, don't have a structured or methodical process or plan for conducting penetration testing. But he points out a recent development that might now make this less necessary.

'Some security solution providers are realizing that the future of penetration testing lies in commoditizing the service. At times and intervals agreed with the client, testing can be conducted remotely and at regular periods – and, of course, more frequently, because the personal attendance of the tester becomes unnecessary.'

It's recommended that penetration testing should be performed after any time there has been a significant change in an organization's network, or if there's a major change in its Internet use, but 'as such changes take place on almost a daily basis, it's difficult to see how that could be sustained' he says. 'Most organizations are tested at least once a year, some prefer once a quarter or even fortnightly, it just depends on

Gone, I think, are the days of the FUD (fear, uncertainty and doubt) factor on the back of which much consultancy has been sold in the past.

the convenience and resources of the organization.'

He points to the growing prevalence of penetration testing as sign that organizations are certainly becoming more security-aware. 'Virtually all organizations employing critical systems – and let's face it – that involves almost every organization. For instance, financial services organizations undergo penetration testing as a matter of course. Certainly all government departments do so and are checked regularly by CESG.

The other side of the coin is the reaction of an organization once it is faced with the reality of the report. 'Vulnerability management is quite another matter,' he says. 'The reactions

of organizations vary enormously. Some effectively do nothing for a while. Or if the solutions are relatively straightforward, they'll make the necessary changes.

'Others take a few weeks or sometimes don't bother at all – in which case they will have simply obtained a report for a report's sake. I think it boils down to the commitment of senior management, but one has to question that commitment if a report is obtained but the requisite action doesn't follow.'

As to effectiveness of penetration-testing, he says this is largely in the hands of the organization. 'Just as life is what you make it, so are the results of the testing. If they don't act on the recommendations of the report, they can't complain if a calamity occurs further down the line.'

Nor should cost be an issue. He claims that the facility shouldn't be expensive. Of course, there's the time of the individual tester. But here organizations can help themselves, although, they often don't.

'At the outset an organization should decide whether a system and network should be explained to the tester before testing gets underway. If no guidance or explanation is offered, the tester has to spend time finding out for himself how the network operates, and that can be time-consuming. In effect, the organization has to decide whether there is to be zero knowledge or full disclosure.'

We move to the related question of wireless networks. He sees this as a 'protocol that has yet to be adopted as mainstream technology for most organizations. It's leading edge and so experimental for most organizations at the moment.'

But, he claims, it's moving in leaps and bounds and will soon surpass wired networks in some organizations. 'One point to bear in mind is that most internal networks are rarely, if ever, encrypted – yet wireless communications are heavily encrypted. But the driver of the technology is undoubtedly that it is inexpensive and so convenient to use.'

He claims more standards are needed to give wireless networks 'more credibility. But some solution providers,

Boardrooms tend not to like technical security issues. If the issues are strategic, they tend to be more interested.

such as Cisco, are now offering dynamic encryption which is extremely difficult to crack.'

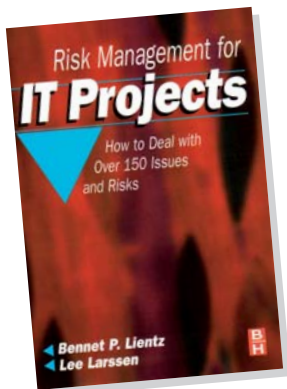
Talking of return on investment in information security, we end on the issue of security consultancy. Phil Cracknell is extremely bullish about the future of consultancy services in this area.

'Gone, I think, are the days of the FUD (fear uncertainty and doubt) factor on the back of which much consultancy has been sold in the past. The attitude has changed noticeably in recent times.

'Most boardrooms now recognize that, even if they have internal resources, they are probably better served in the long run by securing an external – and independent – appraisal of their situation. It's the independence of the evaluation that's important.'

But the reaction of boardrooms to consultants' findings is variable. 'Sometimes they act on recommendations, sometimes not. If the issues are technical, most often they are delegated to the IT department for attention. Boardrooms tend not to like technical security issues. If the issues are strategic, they tend to be more interested, especially if there are real strategic or risk management issues at stake.'

But what drives the information security consultancy now is the pressing issue of standards, legislation and regulation. 'After Sarbanes-Oxley, compliance is uppermost on the agenda of most boardrooms,' he explains. 'With that as a driver, many organizations do not need much persuasion that security issues need regular expert attention.'



Risk Management for IT Projects

Bennet Lientz and Lee Larssen
 Butterworth-Heinemann
 (Elsevier)
 Price: £29.99
 ISBN 10:0-7506-6231-0

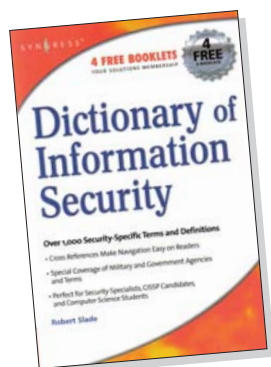
The basis for this book is that the rate of failure of IT projects has remained little changed in the past 15-20 years –

estimated as being 40-50 per cent.

The book points out that this has taken place against the backdrop of new IT, innovative methods and tools and different management approaches.

The authors show how to identify and track the various issues that recur in developing and managing IT projects and offer sensible and practical recommendations on: issues that arise and their frequency; their impacts; detection of specific issues; and strategies for resolving them.

The book is divided into four parts; issues and risk management; internal issues and risk; external issues and risk; and specific IT risks. It will be invaluable for organizations wary of embarking on IT projects because of their variable success.



Dictionary of Information Security

Robert Slade
 Syngress Publishing
 Price £19.99
 ISBN 1-59749-115-2

This book suggests that what has been lacking in the world of information security is a single-source glossary of terms, with preferred definitions for each term, as used throughout the world by information security experts

The author claims to have developed several courses that have addressed topics in the common body of knowledge in the security field and has struggled continuously to find universally acceptable definitions in

'infosec' terminology.

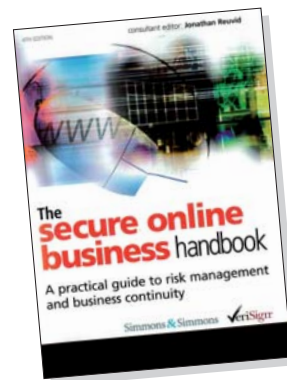
This book therefore is a solution to his dilemma. It is a comprehensive collection of words, terms and phrases, both familiar and not so familiar, which encompass all aspects of information security.

In fact, it is so comprehensive that, at times, its content is arguably superfluous. For instance, is it really necessary to define the words 'asset' or 'fault'?

On the other hand, many definitions of terminology are undoubtedly within the province of only the most experienced of information security practitioners and, in that respect, the book will be an invaluable resource.

Further, the definitions are clear, accurate, authoritative and well cross-referenced – and, like any dictionary, it will invariably be necessary to have to hand.

Whether 30 pages of foreword and introduction are needed is questionable, but this is not a serious point of criticism of a book which will undoubtedly prove invaluable to almost every information security professional.



The Secure Online Business Handbook

General Editor: Jonathan Reuvid
 Kogan Page
 Price £35.00
 ISBN 0-7494-4642-0

The internet is an exciting but unstable place in which to do business. While the rewards are high, the effective management of the security risks involved is a formidable task for senior management. It is this issue that this book tries to address.

The author has compiled contributions from some 'heavyweight' resources, including Simmons & Simmons, the Business Continuity Institute; the Cybercrime Working Group, and Verisign.

The content is wide-ranging and authoritative. Beginning with part one - information and systems at risk; it moves to part two - exposure and vulnerability; part three - software and identity protection; part four - operational management and good practice; ending with part five – contingency planning and disaster recovery. Helpful contact details appear at the end of the book. For a book of relatively few pages, it contains a significant volume of information.

Specific topics addressed include; attack trends, 'phishing' and 'pharming'; web security; online privacy; safe online trading; information security training; software protection; management systems; outsourcing solutions and data recovery.

Some readers might prefer to learn in more depth of the contribution that adoption of relevant BSI Standards can make to online security, but, taken as a whole, this book is as comprehensive a review of information security issues as is likely to be possible within a relatively restricted length for such a complex subject.

Trainspotting

John Mitchell, editor of BCS IRMA's award winning journal and managing director of LHS Business Control, stumbles finds some curious security anomalies in the security of the national rail infrastructure.

The recent fire at Kings Cross which stopped north/south trains into London led me to query the resilience of our national rail infrastructure.

Service availability is a security issue. It was not the fire that stopped trains running, but the need to evacuate a nearby signal box. If you needed to evacuate your data centre, the powers that be would be pretty upset if your business continuity programme (BCP) could not deliver an adequate service.

This is exactly what happened with Network Rail. It was only an interruption but it brought travel chaos. What would have happened if the signal box itself had been destroyed?

No answer

First, I approached the National Infrastructure Security Co-ordination Centre (NISCC) whose deputy director informed me that it is not their bailiwick. 'No, we deal with electronic security, not hardware.'

'But surely the signalling stuff is electronic.'

'Sorry, ask the department of transport.'

I emailed the secretary of state for transport. Neither The Right Honourable Douglas Alexander MP nor his minions cared to respond.

After several failed attempts to attract his attention, I emailed Tony Blair to his email address at the No. 10 website with a query as to what I have to do to obtain a response from the secretary of state?

I received 'snail mail' from the department of transport stating that the signalling failure is a Network Rail problem. I agree the lack of a viable BCP is a Network Rail problem, but the department for transport should be asking why Network Rail performed so



abysmally. Surely, everyone knows about single points of failure in their service provision?

Auditing

As an IT auditor, it is my task to provide assurance, or otherwise, that my clients' systems have good availability; especially those providing a web-based service.

I always ask the single point of failure question. No reputable enterprise would host its key service on a single server without a mirrored back-up, but it seems that this is what Network Rail is doing with its Kings Cross signal box.

Judging by the response from NISCC, there is doubt as to whether a signal box comprises part of our national electronic infrastructure. It's a debatable point, but as almost all our national infrastructure, from traffic lights through to sewer plants, depends on computers, we cannot afford finger-pointing between departments in the way hardware and software suppliers sometimes do.

System totality

Any system is the totality of its components and each component is just as important as the next. NASA's space shuttle uses three computers with

majority voting in the case of a disagreement. It is the only part of that very complex system which is triplicated. We need to move away from thinking that computer security applies only to data processing.

When my niece programmed my video recorder without my permission, I pointed out that she was in breach of both the unauthorized access and unauthorized modification clauses of the Computer Misuse Act 1990.

My wife wondered if she would ever be able to level the same charge against me with regard to programming the washing machine. No chance.

I know the law and I have no intention for going down due to unauthorized programming of a washing machine. However, this may be a way for the authorities to detain suspected terrorists: 'I am arresting you under the Computer Misuse Act 1990 for the unauthorized programming of a video recorder/washing machine/teasmade, or whatever.'

I kid you not. It's a crazy world in which I don't have to make things like this up.

John Mitchell can be contacted on 01707 851454, john@lhscontrol.com
www.lhscontrol.com

Forthcoming events



Public events

17-18 October 2006
Information, Retention, Management and Disclosure, London
 IQPC - 020 7368 9301

This event addresses the critical rules, decisions and best practice, multi-jurisdictional compliance and privacy and data protection obligations and will be addressed by leading UK and international speakers in their fields.

18-19 October 2006
Documation UK, London
 Reed Exhibitions
www.documation-uk.com

This event focuses on all aspects of document management and includes information and content management issues. It will showcase a wide range of new technologies and services covering web content, email and fax management, document and records management, information capture, scanning, imaging and business processes.

18-19 October 2006
Storage Expo Global 2006, London
 Reed Exhibitions 0870 429 4338

This event is the UK's only dedicated data storage event and presents a comprehensive range of data storage solutions from the leading suppliers. It is supported by a full seminar and training programme.

18-20 October 2006
Biometrics 2006, London
 Elsevier 01367 718 500

This event spans three days and addresses technological developments, reviewing all the major biometric technology solutions; applications including the latest trials and tests on the use of biometric technology; and new case studies and implementation experiences from government, financial services, immigration, law enforcement and commerce.

30 October - 2 November 2006
Data Management and Information Quality Conference
 IRM UK 020 8866 8366

This event addresses all aspects of information management and quality control and will comprise even conference tracks (54 sessions), 14 pre-conference tutorials and five post-conference tutorials. Case studies will be featured from a wide range of global corporates in seminars addressed by leading experts in their field.

28-30 November 2006
Information Management Solutions 2006, London
 VNU Exhibitions 020 7316 9660

This event comprises an exhibition including leading suppliers of solutions to address content management; electronic document management; enterprise search solutions; information continuity, storage, security and compliance; collaboration, and knowledge management.

ISSG events

1 November 2006
Measuring Information Security
 Sheffield Hallam University,
 Sheffield

This seminar, co-sponsored by the Faculty of Arts, Computing, Engineering and Sciences at Sheffield Hallam University, will address the 'now' issues that organizations face when trying to measure the effectiveness and efficiency of their information security management systems and associated controls. The event brings together experienced practitioners and researchers, who will identify current best practice in both technical and management aspects of information security measurement, whilst at the same time turning their attention to future directions.

24 January 2007
Annual Legal Day
 RAF Club, Piccadilly, London

Led by the Group's own legal expert, committee member Charlotte Walker-Osborn, and with speakers drawn from various areas of industry and related regulatory bodies, this seminar is likely to cover new laws around data protection, information security, IT and more.

22-23 March 2007
ISSG Annual Conference:
 Theme - Resilience
 Milton Hill Conference Centre,
 Oxfordshire

16 May 2007
ISSG Annual General Meeting
 QinetiQ, Malvern

11 July 2007
Privacy Matters
 BCS London
 Details to be confirmed


For updated details, see:
www.bcs-issg.org.uk/events.html

IRMA events

21 November 2006
Project control: the auditor's role in IS projects and systems development - joint meeting with ICAEW

For updated details, see:
www.bcs-irma.org/events.htm





DR. HANS VOLKMANN
FRCS, FRCP, MB

BIG TOE
CONSULTANT

Sometimes you need a specialist

And if you're looking for Managed Hosting, you need a Managed Hosting specialist.

Rackspace doesn't build websites or sell servers, and we definitely can't help you out with that ingrowing toenail. But if it involves Managed Hosting, we will do more than help. We'll give you guaranteed 100% uptime, a guaranteed one-hour hardware fix and, of course, our legendary Fanatical Support™, 24 hours a day, 365 days a year.

We can do all this - because it's all we do.



Dedication. Obsession. Commitment. Fanatical Support.™ It's a way of life.

Please call **0800 634 0030** or visit us at www.rackspace.co.uk/specialist.



WE TARGET



MALWARE

MICROSOFT.COM/UK/SECURITY/IT

Microsoft

Tools to help secure your network, where and when you need them.

The Microsoft® Malicious Software Removal Tool—over 16 million instances of malware removed and counting. Read the white paper, based on data collected by this effective tool. It arms you with a clear view of the security landscape, including the latest trends, threats, and countermeasures. Find it now at microsoft.com/uk/security/IT

© 2006 Microsoft Corporation. All rights reserved. Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries.

Microsoft®