Business Computing: the Second 50 Years

The Guildhall conference for business leaders

The Guildhall, London

5 and 6 November 2001

Business Computing

Conference e-workshop report

Security Risks And Precautions

Chairman: DK Matai, CEO, mi2g Ltd

Rapporteur: Edward Wolton, mi2g

LEO

© The LEO Foundation 2001

This paper may be freely reproduced for non-commercial purposes. For other uses please contact Business Computing 50 Conference Committee, LSE Department of Information Systems, Houghton Street, London WC2A 2AE, United Kingom

eWorkshop: Security Risks And Precautions

Chairman: DK Matai, CEO, mi2g Ltd
Rapporteur: Edward Wolton, mi2g

Present: G Allen, LEO and ICL
Chris Baines, mi2g
M Burchall, LEO
Hamish Carmichael, Computer Conservation Society
Patrick Duncan, mi2g
Phil Halliday, Journalist
Ruth Halperin, LSE
Antonio Herrera, LSE
Cameron Lawrence, LSE
Peter Morriss, KPMG
Lord Renwick, EURIM
RT Shaw, LEO
S Shoyinka, LSE
Chris Whelan, DTI

An introduction to Security Risks and Precautions was given by DK Matai:

When LEO became operational in 1951, the world saw computers as unconnected monoliths. Today, computers and the telecom wires that connect them have created a matrix of interconnectivity that is in itself the world's largest distributed computer. The other key aspect of LEO was its emphasis on business right from the beginning. It was built by a business and it had a purpose of helping the Lyons Teashop Company more efficiently in the beginning. With time, many other businesses in the UK and elsewhere benefited from the pioneering architecture, software processes and methodology developed by the LEO team.

As the world has become more networked, Metcalfe's Law has kicked in: *"The power of the network increases exponentially by the number of computers connected to it. Therefore, every computer added to the network both uses it as a resource while adding resources in a spiral of increasing value and choice."* (Bob Metcalfe was the inventor of the ethernet and co-founder of 3Com.) The rider to the Metcalfe Law is that the risk of a networked computing environment also increases as an exponential function as more computers are added to the network.

In this world of networked computing where the internet has made history out of geography and boundaries do not really exist except in our minds, the object of securing information and communication architecture can be broadly described as "information security." Computing security must include all of the following: Physical security, IT policy and IT infrastructure.

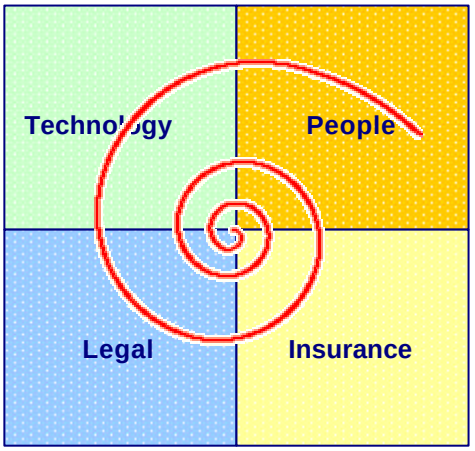
Security risks include threats - both malicious and non-malicious - from either within or outside a company; electronic attack by piracy, surrogacy, denial of service or hazards, performed by disgruntled employees or third parties, perhaps through social engineering. Hackers (software code writers), crackers (malicious code writers) and "script-kiddies"

(using freely available hacking tools from the internet requiring little skill to operate) are all potential electronic threats.

Electronic attack can result in the theft or un-permitted access to electronic money or sensitive data of a commercial organisation, or disrupt operations leading to loss of revenue or even public embarrassment, possibly leading to a loss of confidence and a dramatic fall in market capitalisation. Regarding the public sector, attacks can damage confidence in government, or have a potential effect on military or civil response, or dangerously disrupt services.

Due to an exponential growth in electronic risk in the last five years, it has become necessary to manage it effectively. mi2g demonstrates the management of eRisk using the quadrant matrix below that represents the different aspects covered by Bespoke Security Architecture™.

Any security architecture must not just cover technology but also the legal ramification of security audits, issues surrounding jurisdiction and potential hazards such as breaches in security. It must also take into account the human fallibility element and the security risks inherent to personnel. In addition, insurance should not be left out. Rather the potential results of breaches should be considered and appraised. A loss in market capitalisation is a very real threat and insurance premiums can be based on the quantum of anticipated loss in the case of an eAttack.



© mi2g 2001 All rights reserved worldwide

Discussions

The following is an approximation of the discussions that took place. Note that there are no direct quotes and the following is not precisely attributable to those speakers indicated.

Question: Is security for governments to control or for commercial entities to take control? What are the legal issues?

Chairman: To date, governments and businesses have tackled security differently. The commercial concerns surrounding security are not the same as for government and it is true to say that in the most part, business has lead the field on non-defence related matters. Control of information security products through government agency certification and private sector deployment has in the past been adopted by commercial and government organisations. It is likely that we will see this private-public sector approach continuing until a major sustained electronic attack takes place that will require government intervention and the creation of government funded counter-attack and robust defence capability in the digital space.

In terms of the legal issues surrounding information security, there is much coverage at present of data protection, and the difference in data protection law between Europe and the US. Whereas European Directives give blanket coverage to data protection,

American Acts of Congress point to specific instances or industries and lack the comprehensive consumer protection we have in Europe.

Question: Does the British government have the capability to withstand electronic attack and does it have the ability to electronically counter-attack?

Chairman: With the vast quantities of data in global conduits it is impossible for any one intelligence agency to comprehensively monitor the ether or the airwaves. In the UK, the agencies responsible for detection and interception of electronic activity would not be capable of withstanding a concerted and sustained electronic attack, for example upon the entire UK critical national infrastructure. However, they may be able to predict that attack was about to begin or was underway. HM Government defence policy is based on physical response; whether by air, sea, land or in space. To the best of our knowledge there is no mass counter-attack capability deployed by HM Government in cyberspace.

Question: What are the electronic parallels between US and European data protection, specifically with regard to encryption and investigatory powers?

Chairman: The new Act of Congress, the "Uniting and Strengthening America Act" passed into law in the US in October 2001. The Regulation of Investigatory Powers (RIP) Act received Royal assent in the UK in July 2000. The European Directives on Data Protection for EU member countries became the Data Protection Act 1998 in the UK and came into effect in March 2000. In all cases, encryption is still within the control of national governments.

Panel: Surely the problems of security are self-inflicted wounds. Companies have built insecure systems and ignored the warnings. If companies choose to implement security from the start of development they would avoid many of the subsequent headaches we have seen in some notable software applications. More guard dogs are needed on a house whose windows are fragile but no amount of dogs will compensate for the fact that there should not have been any windows on the ground floor.

Question: What are the personal, private concerns of consumers? How do we protect ourselves? Is Linux more secure than Windows?

Chairman: We began getting involved in the world of information security in a serious way in 1997 when a series of online communities – our lounges – were hacked continuously. The lounges were originally running on Microsoft's Internet Information Server (IIS) and as a direct result of those attacks they were migrated to Linux with Apache. We were able to customise or bespoke the code to our stringent security requirements.

Question: Are the majority of hacking attacks performed on Windows?

Chairman: From our own database going back five years to when the internet as we now know it was in its infancy, the numbers of attacks by operating system work out at approximately 57% for Windows and 18% for Linux. However, Linux is also growing as an overall percentage of all hacking attacks on web servers.

Panel: Security needs to be holistic.

Chairman: Any security solution must begin with an assessment of the status quo and to note the objectives of the eRisk management. An examination must be made of any existing network and the systems administration must be assessed to see what, if any, security patches have been applied to the software. The results of an exhaustive security study and the application of a layered security architecture will assure a very high level of security, however this needs to be addressed constantly to ensure that the maximum protection is always applied. The threat changes with time.

Question: What of the arguments on authentication? Will webcams assist in this?

Chairman: As we move forward into an age where authentication is the key to successful commercial relationships, we will make more and more use of digital notaries and electronic passports that cover all areas of electronic authentication. The important elements that need to be stressed are:

- What somebody is (eg biometric authentication via iris or fingerprint recognition)
- What somebody knows (eg a password)
- What somebody possesses or has (eg a smart ID card)

Panel: Biometrics is not the answer to all our fears. It is an exclusive technology. For example, blind or partially sighted people cannot use iris recognition or retinal scans. Fingerprint recognition does not work on people with skin disorders that affect the fingertip (a significant percentage of the world population). Biometrics can only be used in conjunction with other methods of authentication.

Panel: In the past we relied on Electronic Data Interchange (EDI), which was fixed point to point. That seems to have been changed by the internet.

Panel: There can never be a 100% guarantee of security in a networked system. Therefore the key to successful security is comprehensive risk management, including authentication. At present, there is a mental block in consumers and businesses alike to transact business online, a security hurdle that the industry must demonstrably overcome.

Panel: It is important to keep policy development separate from technology.

Panel: It is important to mention here that the government is acting and will be acting in the future as a procurer of information security and not just as a policy setter.

Question: What do people perceive the technology to be? What of vulnerabilities, either electronic or physical? As an example, women frequently do not admit that they are women when online. I have recently suffered immense inconvenience due to wanting to change the password on an online system due to a cumbersome authentication procedure.

Chairman: We are seeing a dramatic rise in identity theft as criminals impersonate people for financial gain; either by the fraudulent use of credit cards or by electronic identity piracy.

Panel: Perhaps the most important issue here is how to authenticate in the modern era. In the old days it was easy and paper based but now trust is more difficult to establish.

Chairman: The key word here is trust. Is he who he says he is?

Question: How can people be trained to be more security conscious?

Chairman: Technology can help in training personnel and assisting them in online security matters. However technology is not the answer to everything.

Question: What are the key issues for dissemination?

Chairman: One of the key issues overlooked by many organisations is that of a sound personnel policy in the event of a crisis. A strong personnel policy that is properly communicated can mitigate risk considerably.

Panel: There is a resistance to the implementation of comprehensive security solutions. For example, the increased security at airports has travellers grumbling loudly though they know it is for their benefit. Personnel policy is the kiss of death for many companies – there is an innate distrust of personnel by technical staff.

The Chairman then rounded up the discussion and closed the session having thanked all the participants.