

Security? What Security? An Ounce Of Prevention.....

By John Handley – Senior Technical Consultant - Comms-Online

Imagine you get up each morning and leave your house, safe in the comfort of knowing that when you get home after an arduous days work your house will be there in the condition you left it!

So you get home...put the key in the door, and then...some of the lights will come on, the TV will not, your favourite chair is missing a pillow, the toilet occasionally flushes, the kitchen door has a mark on the lock. There's a note on the table in handwriting you don't recognise.

Well what's your first reaction? Shock? What's your second reaction? Embarrassment? Maybe call the Police? "Should I have listened to Chubb and had an alarm installed? Keep that picture in mind and let's turn to your IT network.

Just like your house your network has windows (forgive the pun), doors and ways in/out that you may or may not be aware of. One fundamental thing in common between the two is you! Or people! So now we have to use the 'S' word – 'Security' aka Infosec. These words can create feelings of confusion and intimidation.

Security begins at home! Just think about my earlier diatribe!

It is not essential to possess a deep technical knowledge of the tcp-ip stack to appreciate security (I can think of at least ten people out there right now who have started writing an email in reply). What I feel is essential is a calm, methodical approach to understanding yours and your peers attitude to information security or Infosec.

Infosec needs to be addressed in the same way it needs to be applied, in a layered approach. It starts at the top of your organisation. Upper management need to develop and buy into a high level statement on security policy. Once upper management support the policy it is a lot easier to implement and maintain. Without this support, the good ship Infosec will founder on the rocks as opposed to being applied to points of ingress/egress on your network.

So, now we have a piece of paper entitled Security Policy, what next? Well, that's up to you as IT or Infosec manager and how you see your organisation. You need to develop this document on an ongoing basis in line with



your needs. Education of your workforce, technical and non-technical is paramount to any successful IT policy. Most people have heard at this stage that eighty percent of IT security issues emanate from within your network. We have seen huge percentages of IT budgets being consumed on WAN links, Internet connections and their associated security products to secure them.

Mike Galvin – Country Manager of Cisco comments "Security issues were highlighted in a very strong way after the events of 9/11. After an initial furore however, the current economic environment and the legacy of the technology bubble burst has left a number of customers in a technology truce in terms of investment. Security solutions and services have not escaped this effect and a number of specialist security companies in the Irish market have been adversely affected. Customers want to understand their return on investment on security technology and also want to understand how they can build an end-end security policy covering the desktop, core infrastructure, access solutions (e.g. teleworking, GPRS etc) and server technologies".

How much of that IT budget do we allocate to inside your network? Our colleagues across the Atlantic now have a due diligence and care directive when dealing with information security. There are standards now developed for the ways we deal with and secure

information. In America they have the Health Insurance Accountability and Profitability Act (HIPAA). In the U.K. there is a British Standard, "Information security management. Code of practice for information security management" BS7799. There is an ISO Information Security standard ISO17799 which is quite detailed.

So, where do you start looking? I prefer to start with non-vendor specific guidelines. One site I regularly visit is the SysAdmin, Audit Network, Security website www.sans.org which has everything from the top ten common vulnerabilities, sample IT policies, security webcasts and intrusion detection to name but a few. Others such as www.isc2.org, www.securityfocus.com, www.cosac.net, www.humanfirewall.com, and www.iso-17799-security-world.co.uk come to mind. There are copious globally recognised, industry standard certifications, which you may choose to pursue. One word of warning! Do not think Security is an over night success story, it takes many, many hours, days, weeks, even years of hard work and it never stops!

Coming back to web seminars or webinars, if you look you will find at least one webinar a week that may deepen your understanding of Infosec. I find these a great source of reference, which can usually be viewed in your own time!

Regarding the security product vendors I could fill ten pages with their web sites. Precious care must also be taken when assigning security related tasks to people with no security training. It is fair to say that industry standard certification for Security Products will demonstrate a level of competence with that product. Look at it this way, what is the potential loss to your organisation compared to your IT security budget?

Get out there and talk to your peers about security concerns, go to the security user groups and discuss your fears! Security with obscurity is not necessarily the way to go.

Bring in the security consultants by all means. Remember that you need to listen to them and cascade all the lessons learned throughout your organisation and management structure. You can develop a security awareness program but you need to maintain it and regularly review it as security trends develop. Empower your people with some level of security responsibility irrespective of its size. No more

post it's on the screen with passwords, for example! Maintain a healthy level of security consciousness or paranoia, just like with your house!

What is the ISO global standard for information security management?

ISO 17799, also known as BS7799, provides best practice recommendations for information security management. It helps identify, manage and minimize the range of threats to which information is regularly subjected.

The Security Management Index is organized into 10 sections based on ISO 17799/BS 7799 Standards

1. Security policy - This provides management direction and support for information security
2. Organization of assets and resources - To help you manage information security within the organization
3. Asset classification and control - To help you identify your assets and appropriately protect them
4. Personnel security - To reduce the risks of human error, theft, fraud or misuse of facilities
5. Physical and environmental security - To prevent unauthorized access, damage and interference to business premises and information
6. Communications and operations management - To ensure the correct and secure operation of information processing facilities
7. Access control - To control access to information
8. Systems development and maintenance - To ensure that security is built into information systems
9. Business continuity management - To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters
10. Compliance - To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations, and any security requirement An organization using BS 7799 as the basis for its ISMS, can become registered by BSI, thus demonstrating to stakeholders that the ISMS meets the requirements of the standard.

LAYERED IT SECURITY

I will try to give you my take on this, I'm sure most of you have your own ideas and time and experience will mould this for sure. I am trying to piece together an awareness here of network traffic and concerns from inside and outside your network.



Mike Galvin – Country Manager of Cisco Systems

Externally facing routers (with a public IP address) for example can be configured with an access list to allow only telnet connections from particular networks or router interfaces. It's rather unsettling to audit a site and then attempt to telnet to the sites externally facing router from the internet only to get a login prompt! Do you maintain a backup copy of your router configurations?

After the internet facing router we may for example have another router or a firewall. In the case of the router we need to pay careful attention once again to access lists. In the case of the firewall it is worth researching the vendor's product for vulnerability alerts. Is there a banner that states Unauthorised Access IS Prohibited? One case in the US last year hung on the point that a would be intruder got a welcome message to a router. At all times it is essential to maintain a detailed IP address schema and network topology map. Versions of router software, firewall software and patches revisions should be managed within a strict configuration management and change control regime.

Some sites make use of an Intrusion Detection System at this point in the network. There are a lot of products out there available with various ways of detecting would be network intrusions. False positives (or false alarms) can be quite misleading and a trained intrusion detection analyst is quite a rare commodity!

If there are requirements for online credit card based transaction processing, there may be necessity access to an enterprise database sitting within your LAN. This can involve more administrative complexity, which must be

documented and tested rigorously. Certain small to medium enterprises may for example have the same person who looks after all email, routers and firewalls. It may become necessary to maintain a skill matrix purely for your security personnel and organise skill transfer regularly.

Viruses and malware are now a consideration it would be fool hardy to ignore even partially. Because of the close integration of some of the more common email solutions with operating systems it has become much easier for virus writers to take advantage of this interoperability and connectivity. Similarly what were once warnings like SQL injection (for example it is possible to use the dialog boxes in a web page to manipulate databases) and cross site scripting (for example embedding html in a login or password box on a web page) issues are more prevalent. The same issues may manifest on desktops as well as servers.

If you have a Proxy server, this may be another layer, what services are advertised at your network interface card?

Protection from email Spam, email borne viruses and worms, java, active-x need to be addressed in step with your organisations IT policy. I have visited sites that filter any type of active web content, much to the frustration of the user base.

Regarding backups, do you regularly do test restores? What is your procedure for failed backups?

What password policy is in place? Some sites use a password policy with a minimum of six alphanumeric characters to include at least one number and one capital. Signing on to multiple systems such as NT Domains, AS400, and UNIX can be problematic to manage when usernames and password policies differ. Kerberos is a Single Sign on Solution (SSO) which may be considered, Windows 2000 for example uses a variant of this.

Telephone access and usage should also be considered, call forwarding to external numbers from desk phones can be an issue. Similarly modems in PC's that are on the LAN are an instant compromise, which can only lead to disaster. I read of one company that used a war-dialler (a piece of software that will sequentially dial all the numbers in a range and detect a fax, modem etc) for all their telephone numbers to audit for undocumented modems.

Where do you stop? Only you can answer that question! I once attended a project management course and the opening question from the instructor was "How do you eat an elephant?" The answer of course was "In very small pieces". This is how I approach Information Security or Infosec.