



Introduction to Networks & Computer Security

Year 1 ICA

Harry Schilbach - J9139213
5/8/2010

Contents:

Task 1: A description of the function of two layers from the OSI 7-layer protocol stack . A table naming the major protocols used at this layer - define the characteristics of each protocol and give a brief description of its basic functionality	3
The OSI (Open System Interconnection) model	3
Transport Layer	3
Application Layer	4
Task 2: Prepare a report demonstrating your understanding of the role of networks and security in modern business	6
A discussion about the critical role of Networks in modern business.....	6
Defining what network security is and why it is necessary.	7
A discussion of various Operational Security measures, including Firewalls and Intrusion Detection Systems.	8
The role of policies and procedures in networked environments.....	8
Task 3:	11
Prepare a report identifying current security risks and associated security measures facing modern networked environments	11
Incident response.....	11
Basic principles of Cryptography in network security and a brief description of some cryptographic techniques.....	12
Discuss how a business might try to secure a Wireless LAN	13
Task 4:	15
Prepare a report demonstrating your understanding of the role of Risk assessment in the context of a networked environment.	15
Definition and purpose of Risk Assessment.....	15
How might a modern business go about performing a risk assessment.	16
Bibliography	17

Task 1: A description of the function of two layers from the OSI 7-layer protocol stack . A table naming the major protocols used at this layer - define the characteristics of each protocol and give a brief description of its basic functionality

The OSI (Open System Interconnection) model

The OSI (Open System Interconnection) model is a framework tool for Network Communications between any open networked systems. It provides a common language of communication. This means that they can talk to each and other, exchange data and make sense of the information that they are exchanging.

It allows the exchange of data between a huge variety of systems. This includes laptops you use at home, ATM's, business systems, mobile telephone networks. It does this by breaking down large pieces of information into smaller parts of data and packaging these with instructions explaining where they are going, what they are and how to reassemble these.

This packaged Data is referred to as packets. These packets are then reassembled by the receiving system using the framework of the OSI Model. This means that data (as packets) can be routed along the internet or any network in an efficient manner as possible. It means that these packets can be routed along different paths. Whichever the network feels is the most efficient path for that packet to take to the destination. This provides networked communication with one of its greatest strengths. Resistance.

Transport Layer

The transport layer is central to networked communications. It performs the delivery function between applications; it transports the data and handles delivery errors.

The Transport layer batches up data ready for sending to the Network Layer , this is known as multiplexing, and conversely the layer also receives these batches and sends them to their correct sockets or applications. This is known as demultiplexing.

The transport layer is concerned with delivery of packets direct to the receivers host. It is not concerned with how the network connects those applications.

Transport Layer collects and prepares packets from the application layer. It readies them for the Network Layer. This layer does not have any direct connection with any other hosts – it acts entirely on the machine it is on.

Network routers points along the communication chain do not action any of the information within the transport layer packets. The Transport layer is constricted by the Network Layer. If the Transport Layer requests a service that the Network Layer does not have available, then this service cannot be delivered. Encryption works within the Transport layer *see task 3*. The Transport level is responsible for directing different packets to different sockets that have been specified by the application layer. By the same token the transport layer gathers the information from different application ports and packages then for the network layer.

Table 2: Transport Layer Protocols

Name of Protocol	Characteristics	Functionality
TCP (Transmission Control Protocol)	Provides end to end packet delivery reliability.	Error Detection and correction, so if a receiver doesn't get the packets sent the TCP can resend it. It also reorders the packets of data so that they are in the right order. Creates a 'handshake' with the other host to discuss 'the rules' for transmitting to each other.
UDP (User Datagram Protocol)	Provides a connectionless service to applications, in that it will communicate without setting up special channels of 'handshakes'.	Communicates but does not provide the 'upper-level' services of TCP, such as error detection and ordering of packets which means packets using this service may not turn up, or be out of order. The advantages are that it has a 'light footprint' so is ideal for services such as VOIP where several missing packets won't affect the overall content.

Application Layer

If there was no network applications than there would be no need for networked communications or indeed the OSI model. Applications provide the interface for the user or end host and the trafficked data.

With the advent of near ubiquitous broadband access (an ONS study said 63% of UK Households were connected to Broadband, with access for 95%), in the amount of network applications has expanded from on demand tv, music streaming websites such as spotify and p2p(peer to peer file sharing). The Application Layer is responsible for providing end-user services such as email, internet, and file transfer.

Table 2: Application Layer Protocols.

Name of Protocol	Characteristics	Functionality
DNS (Domain Name System)	A naming and address translation system.	This assigns an ip address to any network device and then translates that into something more user friendly. E.g. When you type in www.google.co.uk is translates to the actual address of 216.239.59.105
HTTP (Hypertext Transfer Protocol)	A client/server request/response protocol for the internet	http requests the file (typically a web page) from another networked device (typically a webs server) and this responds with a http response usually containing the file. This is initiated with a TCP connection.

SMTP (Simple Mail Transfer Protocol)	An internet standard for email across networks.	Transfers emails from the senders' email server to the receivers email server. Whereas Http is mainly a 'pull protocol' in that it pulls messages SMTP is a 'push protocol' in that it sends files. Requires data to be encoded in 7bit ASCII.
DHCP (Dynamic Host Configuration Protocol)	A protocol that saves IT staff a lot of time! DHCP allows a host to obtain an IP address automatically, instead of having it manually assigned.	A configuration database, set by the administrator on a server with a range of IP addresses, serves the configuration details to a client when asked. This allows efficient use of IP addresses as the client can be given a temporary IP address each time.

Task 2: Prepare a report demonstrating your understanding of the role of networks and security in modern business.

A discussion about the critical role of Networks in modern business.

Almost all aspects of modern society depend on Computer Networks and their Security. From Industry to Research, Education to Defence.

Within the last generation the amount of data an organisation can and does capture has increased exponentially -“Wal-Mart, a retail giant, handles more than 1m customer transactions every hour, feeding databases estimated at more than 2.5 petabytes (Cukier, 2010). Indeed in a recently published study by IDC (IDC, 2010) predicted that for the 2010 the total data held will grow to 1.2 zettabytes, much of this held on business networks.

With this increase in Data comes an increase in Computer Networks to carry the data. The growth of both Data Traffic and Computer Networks are intrinsically linked, they relationship is analogous to a motorway network and the vehicles that travel on such a network. The motorways are the Computer Networks and the data are cars and lorries that travel on such a network , taking this analogy a step forward the higher the quality and capacity of the Network the better the Data or traffic is able to travel around the network.

The advantages of the massive increase in Computer Networks are manifold and space does not allow us to enter into a full discussion here, however for context I'd like to outline a few of the reason:

- Technological – The computer world has been able to witness the trend of Moore's law for several decades now. In overview this states that processing power will double every eighteen months or in effect that their cost will halve over the same period. This has slashed the cost of computing power and the memory to store that data over the past decade. The effect of this is twofold; it removes many of the high costs of entry for people wanting to set up Computer Networks.; It also reduces the cost of storing vast quantities of Data so that the added cost is almost negligible.
- Social - Globalisation brought about by advances in communication technology and the advent of perhaps the greatest Computer Network – the Internet – Has led to both a business and social ability to communicate and conduct business. The above technological advances mean that it is entirely possible to have a designer working for Trek Bikes creating the latest creation on his laptop connected to a Virtual Private Network (VPN) in a coffee shop in California and using a corporate computer network transfer the designs to a factory in Taiwan. 50 years this wasn't possible and more than likely the designers would work right next to the factory. Now all is needed is a connection to a network, be it corporate, public or home. This has transformed business and working practices, allowed corporations to have multiple bases anywhere in the world all connected through networks.

Computer Networks permeate almost every modern business; from a local Bakery running a basic electronic point of sales till to a large multinational server farm providing cloud based 'Software as a Service' facilities. Whilst it is easy to think of computer networks relating just to laptop or PC communication. Networks make life very much easier for everybody. Cash Machines, Traffic Lights, Air Traffic Control and CCTV systems are all based on computer networks. Information being relayed from host to host, and gathering information on databases that makes modern society tick.

Defining what network security is and why it is necessary.

It is because these networks are so crucial to modern society that they have to be defended. These networks face the same dangers that 'physical' world does; Criminal and malicious individuals and organisations wish to steal this data travelling on networks. Be it credit card details, the blueprints for that latest bike designed in California, the contents of your private e-mail , or a terrorist accessing the air traffic network .

The need to secure these networks is fundamental, but what do we mean when we talk about Network or Computer Security?

To break this down Martin R Smith (Smith, 1989) quotes his 5 year old sons' answer to the question of what security is – "Keeping me safe, and keeping people out". This simple answer can be built upon to develop our working definition of what Computer and Network Security is. There are generally said to be three intentions of Network Security; confidentiality; integrity and availability;

- Confidentiality ensures making the information held on and transmitted by a network is either unintelligible or unavailable to anyone who does not have legitimate access
- Integrity means that the data hasn't been changed by accident or intention by unauthorised people or computers. Again this applies to a static storage facility or transmission over a network where it is amount that a computer on a network can confirm what was received was what was sent.
- Availability allows people and computers to access the information an organisation holds on its network. Availability is perhaps the goal that complicates Network Security the most. It would be very easy to have two computers in the vault of a bank containing customer accounts details networked only to each other. The network, information and computer would be classed as being 'very secure', but would be next to useless on an availability scale if customers and staff had to go to one of those computers to access their accounts.

Over the last twenty years a whole online economy has been created whose revenue is purely generated on computer networks (e.g. the internet). An unreferenced survey in Commonsense Computer Security (Smith, 1989) states that two out of three companies said that their business would be 'seriously affected' after just a few days without their computers. Fast forward twenty years and our reliance on computer networks has grown that very few business could go a day without their computers and indeed loss of networks for only a few minutes could result in massive potential losses of revenue. On the 6th June 2008 Amazon.com was unavailable to its North American customers for approximately 120 minutes; in its analysis Cnet.com (Shankland, 2008) stated that if this outage was extrapolated to a global Amazon.com outage it would cost the company around \$31 000 a minute or \$3 720 000 for the entirety of the outage. Whilst this outage

was not the result of a lack of network security it demonstrates the potential impact that a compromise in security or lack of availability can have upon an organisation.

A discussion of various Operational Security measures, including Firewalls and Intrusion Detection Systems.

How do we as individuals and businesses' protect our networks from these vulnerabilities. There are several software solutions that protect computer networks. Security precautions revolve mainly around two categories. Intrusion Detection Systems (IDS) and Firewalls. Let's explore these security solutions in more details:

- Firewalls are akin to a medieval wall around a city. They provide protection around a network and allow only authorised access and egress through a gateway. They inspect the header information of data packets of data entering a network. They look for suspicious destination/sources of packets, checking them against a list or filter of suspicious sources and if necessary block these packets from entering the network. As well as looking for suspicious information rules can be set on the firewall to stop outside computers connecting to individual computers, via FTP connections for instance which would allow a outside source control of an internal host. Firewalls can also act as proxy hosts, acting as a go between with an internal host requesting information from the internet and the request information, This stops the 'outside world' from both discovering the identity of the requesting host and connecting directly to it. Firewalls are a very flexible solution for businesses as they are customisable and can monitor a large amount of hosts and data traffic.
- Intrusion Detection Systems (IDS) or Applications are concerned with similar tasks as a firewall and indeed work with it, an IDS can update the firewalls list of filters and suspicious source addresses. An IDS looks for suspicious patterns, such as attempts to open multiple FTP's, unexpected volume of HTTP requests that could trigger a DOS (Denial of Service) attack. It's worth noting that an IDS also monitors outgoing traffic, as this can provide information on a successful attack sending outgoing traffic back to the malicious host.
- Demilitarised Zones known as DMZ involves creating a sub-net that has a lower level of security than your main network. Typically this may be a network that has contact with outside networks such as the internet, an organisation may put their public web servers there, or a another organisation, for instance a company could create a DMZ for a client to have access to certain information whilst not allowing access to their own local area network (LAN). The effect of this is that it adds another barrier, normally protected with IDS controls to your LAN whilst allowing you to communicate with the outside world, customers, partners, or suppliers.

The role of policies and procedures in networked environments.

Networked environments should be governed by a strict set of policies to ensure good governance, legislative adherence and consistency within an organisation.

Large organisations will have a Chief Information Officer (CIO) whose responsible for all aspects of IT. However every organisation is duty bound by legislation, such as the Data Protection Act (1998) and the Freedom of Information Act (2000), to ensure that the data an organisation is secure, correct

and that the data can be ordered for access. Policies and procedures can help an organisation to ensure that it remains on the right side of the Law and that every person within the organisation knows their responsibilities when it comes to network security.

Some policies that could help include:

- Acceptable IT User policy - This could be a document that outlines what is an acceptable use of an organisations IT resources and networks. It could include acceptable email and internet policy. Restrictions on the use of non-standard or authorised software and hardware. Also security of passwords and IT facilities. IT policies can engage the user and alert them both to the threat that a network can be under and also guide them in how to minimise the threat. It is common industry practice to create, promote and police a acceptable IT user policy for all users that come into contact with a business' computer Network. This could be a training document or a contractual requirement
- Security Policy - An organisation may want to restrict how data stored on their LAN is accessed by their Users. This could include giving different users different levels of access or access to different areas of the LAN. Users could be restricted from downloading executable files from the internet to stop viruses or unauthorised software. Physical restrictions could include the banning of removable storage media so downloaded data is managed correctly and not done ad-hoc by unauthorised users. A headline grabbing incident happened when the DWP lost personal data for 25 million on a mailed CD (Discs loss 'entirely avoidable', 2008).

Having policies in place demonstrates internally and externally that as an organisation you are serious about Network security

Task 3:

Prepare a report identifying current security risks and associated security measures facing modern networked environments

Incident response.

Security risks in a digital and networked world mirror risks in the physical world “...if real banks are robbed than digital banks will be robbed.” (Schneier, 2004). A Networks’ primary function is to Communicate; this communication provides opportunity for malicious or criminal behaviour. Malware, an amalgam of the words malicious and software, is a major threat to modern networked environments.

Incident response is about having a structured way of addressing a computer or network security incident, Garfinkel and Spafford suggest two overarching responses to be “Rule 1: Don’t Panic! ...Rule 2: Document!” (Garfinkel & Spafford, 1996). To this I would add that ‘Rule3: The response should be dynamic’ in that it should be reviewed, practised, updated and improved upon.

Whilst ‘Rule 1’ may seem obvious but there can be times when a response can cause greater damage than the initial security threat, for instance turning off a web server may cut off revenue for an online shop whilst the attack was just a amateur phishing attempt. Rule 2 is just as important, whether in a large organisation or small business it’s vital to document in real time what is happening. This could involve something as simple as a timeline noting observed effects such as large amounts of e-mail being generated or websites and servers’ becoming unavailable. Ideally documentation will be in place before a computer or security incident occurs. This will allow an organisation to take a predetermined thorough approach to Incident Response and allow Network Administrators to abide by Rule 2. Such a document should include the following:

- **Threat Assessment** – a decision matrix to help the administrator dealing with the incident to accurately assess the threat and the necessary response. Questions to ask could include; “Has an attacker succeeded in getting into your system?”; “Is the attack currently in progress?” (Zwicky, Cooper, & Chapman, 2000); Is this an actual incident or a false positive? e.g. is maintenance being done on your network. The answers to these could lead to different levels or avenues of response.
- **Communication of an Incident** - Documentation could include a list of people within an organisation to notify of an incident. This could not only include people who can help with the security incident (such as a anti-virus software companies), but also people who are affected by the incident, for instance a loss of service to a customer may require you to notify a Helpdesk, who may be fielding calls from customers asking about loss of service.
- **Evidence Gathering** – one back-up, witnessed and not re-writable and secured. It could involve screenshots, or server logs showing a compromised network or machine or even creating a “snapshot of each compromised system...by doing a full backup to tape...” (Zwicky, Cooper, & Chapman, 2000). This will not only allow later analysis of the security

incident but also help identification of processes that will reduce the risk of a similar incident and can help with legal proceedings.

- **Recovery Plan** – to allow quick resumption of service it is important that as part of the incident response plan includes regular timetabled back-ups of all data and applications. These should be multiple (both in quantity and back-up dates points) and keep secure in several places
- **Security Incident Report** – this could be a template for completion after the security incident. It would detail the nature and type of incident or attack, the methods employed, the scope and impact of the incident and any lessons learnt from the attack and the way the organisation dealt with it to increase understanding and reduce the risk for future.

Basic principles of Cryptography in network security and a brief description of some cryptographic techniques.

Cryptography is one of the main tools engaged in networked environments. It allows privacy, trust and secrecy. Cryptography is concerned with encryption and decryption in essence it is concerned with keeping things secret be they your email message or your credit card details.. It takes messages and encodes them in a way that stops others from reading them, allowing only the intended recipient to decode and access these messages. In network security packets of data are encrypted with a special key or algorithm that scrambles the message. To access the data you must have key that allows the message to be put back together. Let's look at these algorithm's in a little more detail:

- **Symmetric or Secret Key Cryptography** – this algorithm involves one private key that performs both the encryption and decryption. So the sender and receiver of the message both use the same, hence symmetric, key. Another attempting to intercept the message needs this key. Advantages of this are that they are generally faster to execute on the receiver. Disadvantages include the need for great security when initially exchanging keys over a network as an eavesdropper could use these to decode future messages.
- **Asymmetric or Public Key Cryptography** – replaces Symmetric models one key with two; a public key and a private key. The public key is available to everyone for encryption of the message, however the receiver uses his private key to decrypt the message.

Some programs use a mixture of these to make the encryption even more secure. An example of this would be PGP (Pretty Good Privacy) program that uses a combination of the above mixed with another cryptographic method known as Hashing.

Discuss security relating to Transport Layer and Network Layer Security

The majority of security occurs at the Transport Layer and Network Layer within the Protocol Stack.

The Transport Layer host protocols that are directly related to secure end to end communications. TLS (Transport Layer Security) and it's precursor SSL (Secure Socket Layer) are two such protocols

that use TCP (Transmission Control Protocol). These provide server and client authentication, data confidentiality and integrity. Some its services are as follows:

- Fragmentation – It takes data from the application layer and divides it into smaller blocks
- Integrity – to notify the receiver that the message is as it left the sender TSL/SSL creates a unique identifier known as a MAC
- Confidentiality – Data and identifier are encrypted using private key cryptography.

IPSec (Internet Protocol Security) works at the network layer. It firstly establishes a host to host session. Some of its services are as follows.

- Cryptographic Agreement – Ensures that both hosts use the same algorithms, *see section above*
- Encryption of IP Packet Data – This encryption can only be decoded by the receiving hosts IPSec.
- Data Integrity – Ensures that the header fields were not altered in transportation.
- Origin authentication – Ensures that the details of the source are the actual source, this is done through a trusted key.

Discuss how a business might try to secure a Wireless LAN

Most businesses now use a WLAN (wireless local area network). This a cheap convenient solution to establishing a network in an work area. It allows users to work where they wish an is cheaper than network cabling a whole work area.

Wireless network routers come with a lot of settings that can increase their security. Let's look at how we can secure a network:

- **Use the highest level of security** – currently WPA2, more secure than the previous WEP. This means that users' wishing to join the wireless network must have a key. Encryption is 256 bit instead of the lower 128 bit of WEP.
- **Change default login name and Password of Routers** – If someone has access to your network they can lock you out of the router.
- **Location of wireless router** – If this is kept in the middles of the work space the range will be limited to malicious users.
- **Turn off** – when not in use the router can be switched off, this means no one can attack outside working hours.
- **Mac Addresses** – Specify which devices, via their MAC addresses, can access the router.

This would suffice for a small office network.

However if you business is larger or you network serves outside clients if would wise to invest in a larger more secure set-up, as in *Figure 1*, This involves Intrusion detection devices that actively look for threats or attacks, firewalls to protect the whole network, a Demilitarised sub-network too service traffic from outside whilst protecting your internal network, and a proxy server to ensure that individual IP address within your workspace are not discovered.

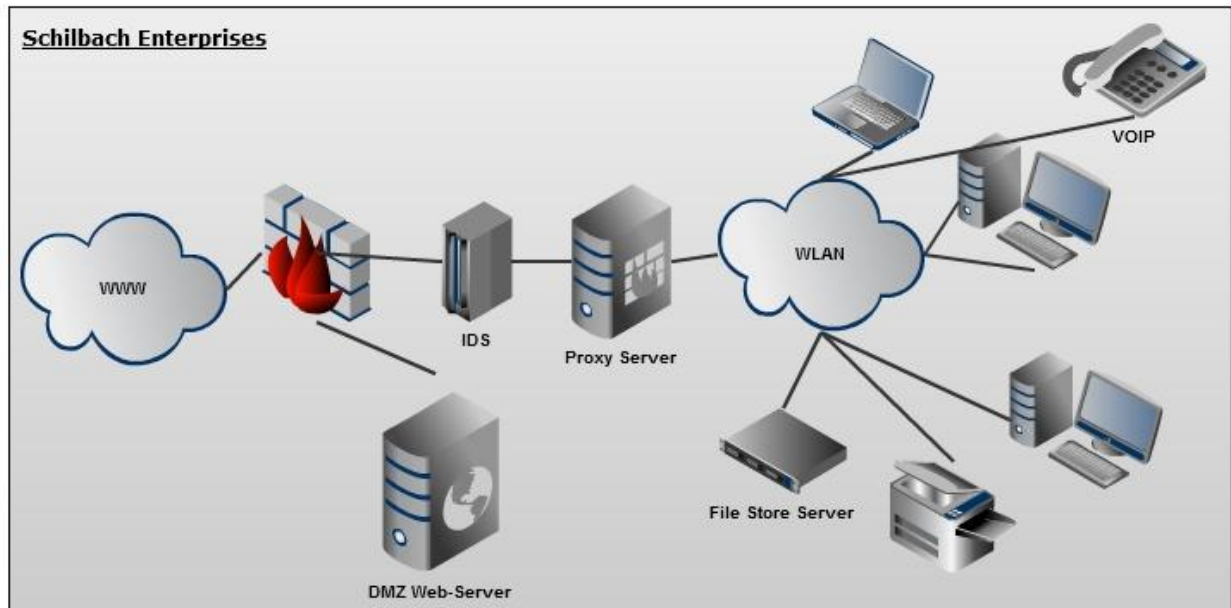


Figure 1: Creating a Secure Network

Task 4:

Prepare a report demonstrating your understanding of the role of Risk assessment in the context of a networked environment.

Definition and purpose of Risk Assessment.

Risk assessment is first and foremost concerned with identifying all possible vulnerabilities to a networked environment. In an ideal world an organisation would be able to mitigate all risks identified immediately, however finite resources normally dictate how many of the risks can be 'plugged', therefore attaching a priority allows the highest threat risks to be dealt with sooner. When attaching a priority you need to analyse the risk of occurrence as well as the potential impact and cost of remedy.

Risk assessment within a networked environment involves taking an objective view of the current situation with regards to security vulnerabilities. There are two broad viewpoints that you can take:

- **External View** – How do people outside your organisation have access to your network.
- **Internal View** – Looks at people within your organisation and how they access your network.

Before we look at the above in more detail, let's look at some absolute basics of risk assessment. A walk around any modern office can usually reveal passwords on 'post-it' notes stuck to the edge of monitors, unlocked workstations and wireless routers with the WEP passwords written on them for 'convenient' access to visitors.

What sort of passwords are the users accessing the system with. Are user accounts, network routers and firewalls username/passwords set to the manufacturers or suppliers default? Will using 'Admin' and 'password1' or 'admin1' allow anyone to access and change security settings and effectively shut you out from your own network tools. No malicious software or Janus attacks needed. Technical skill required: Zero.

How did we get into that office? Were we challenged? Did we have to show a pass? Does the office have access controls? If the answer was 'no' then all it would need is a smartly dressed confident person to walk in and be accessing the organisations data within minutes, no fancy hacking tools or hours spent with dictionary or brute force attacks on a network. Technical skill required: Zero.

These are all security risks that allow unauthorised access to networks and data. All the above do not require any special 'hacker' knowledge and equipment no more sophisticated than a wireless enabled Smartphone or Net book.

How might a modern business go about performing a risk assessment.

The result of a risk assessment should be a risk assessment report which gives us a qualified overview of the risks facing a networked organisation and how to address those risks. Industry standards have been laid out by the government (National Institute of Standards and Technology, 2002). Below is detailed the structure that they recommend with some commentary:

- **Define the Risk Assessment** – This includes looking at the scope and purpose of the assessment and creating a methodology. Who is going to be involved, time periods involved, reporting hierarchies. What software and hardware is to be used (e.g. Event Logs, Packet Sniffers)
- **Perform System Analysis** – the ‘meat’ of the project, collection of data from web-server logs, packet sniffing software, looking at previous security breaches, performing integrity checks on systems and at the extreme even employing someone to attempt to find the vulnerabilities of your network known as penetration testers or ‘white hats’. The purpose of this assessment requirement, identification of present or potential threats and vulnerabilities.
- **Create Risk Ratings** - Once these have been identified the next step is to put a qualitative or quantitative assessment of the impact of the detailed risk. E.g. If one web server fails it will mean that x customers can't access their account page. Once the impact of the risk has been evaluated you can attach a priority to it.
- **Develop Recommendations** – Using priorities identified create mitigation plans for vulnerability. How are you going to fix this or stop it happening? This should involve cost/benefit analysis and detail the reduction in risk your plans will have. A lot of vulnerabilities may be reduced but eradicated without an impact on business, e.g. again shutting down web servers.
- **Document Results** – the final stage, present findings to all stakeholders – not just IT staff - with a detailed plan and costing. This should initiate the beginning of a project to reduce those identified vulnerabilities.

It's worth concluding that once the above has been completed it is essential that this process is repeated periodically. Threats and vulnerabilities evolve and a ‘secure’ system today will not be a secure system tomorrow.

Bibliography

Cukier, K. (2010, February). Data, Data Everywhere. *The Economist* .

Discs loss 'entirely avoidable'. (2008, June 25). Retrieved May 05, 2010, from BBC :
http://news.bbc.co.uk/1/hi/uk_politics/7472814.stm

Ebay. (2003). *Ebay Archived Annual Reports*. Retrieved April 9th, 2010, from Ebay:
<http://files.shareholder.com/downloads/ebay/887965641x0x43781/1BC47297-275F-4312-8778-CC60AEFA0114/eBay2003Annual.pdf>

Ferguson, N., & Schneier, B. (2003). *Practical Cryptography*. Wiley Publishing Inc.

Ferguson, N., & Schneier, B. (2003). *Practical Cryptography*. Wiley Publishing Inc.

Garfinkel, S., & Spafford, G. (1996). *Practical Unix & Internet Security*. O'Reilly.

IDC. (2010). *The Digital Universe Decade – Are You Ready?* <http://idcdocserv.com/925>.

National Institute of Standards and Technology. (2002). *Risk Management Guide for Information Technology Systems*. Department of Commerce US government .

Schneier, B. (2004). *Secrets & Lies*. Wiley Computer Publishing.

Shankland, S. (2008, June 6). *Amazon suffers US outage on Friday*. Retrieved March 31, 2010, from cnet: http://news.cnet.com/8301-10784_3-9962010-7.html

Smith, M. R. (1989). *Commonsense Computer Security*. McGraw-Hill Book Company.

Zwicky, E. D., Cooper, S., & Chapman, D. B. (2000). *Building Internet Firewalls*. O'Reilly.