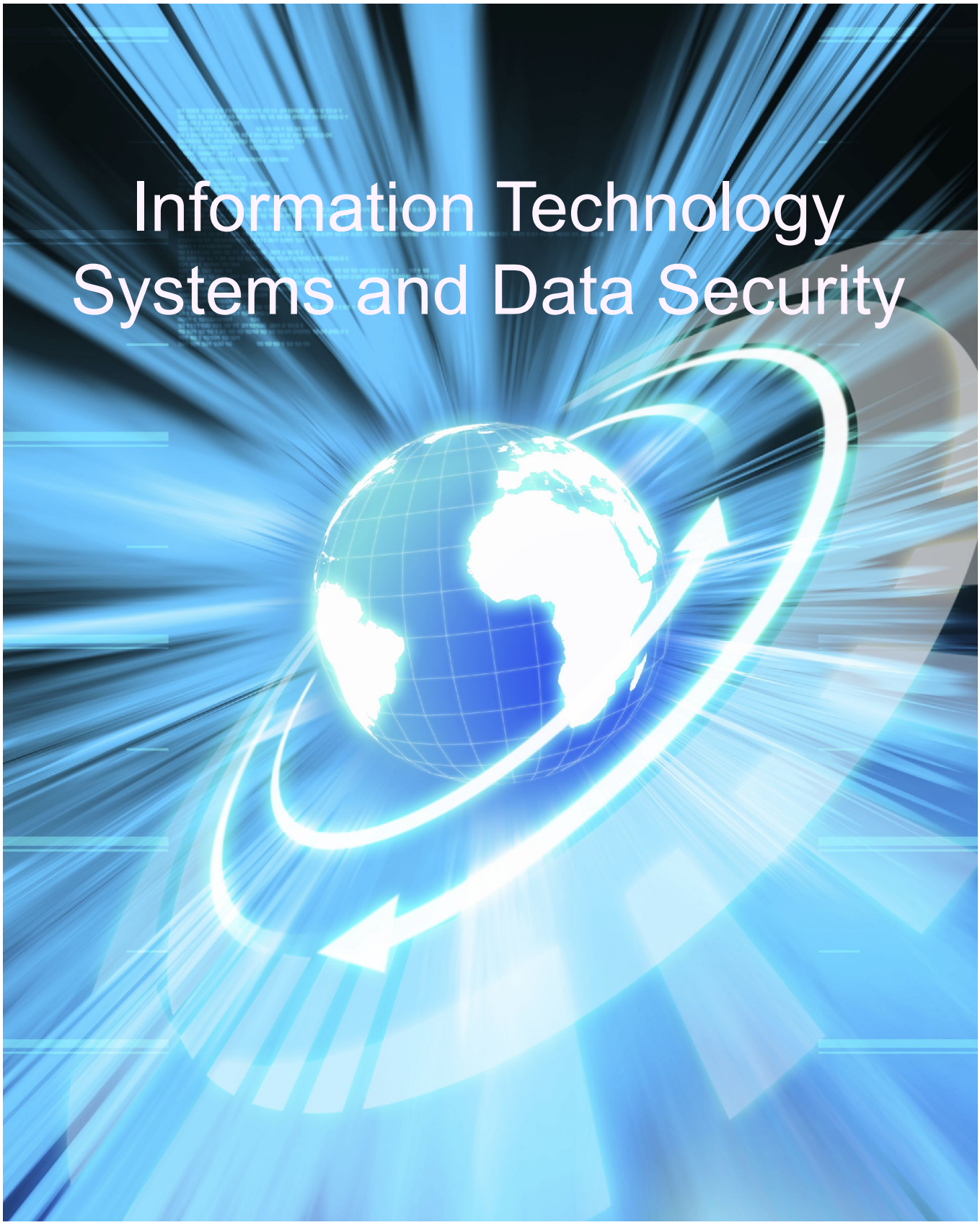
ALLIED
RISK SOLUTIONS

Information Technology Systems and Data Security



ALLIED
RISK SOLUTIONS

Contents

Copyright

Disclaimer

The information presented herein is the view of the author and is for informational purposes only, and may not apply to your situation. Because of the rate at which conditions change, the author reserves the right to update and / or modify his opinion based on the new conditions.

While every attempt has been made to verify the information, the author assumes no responsibility for errors, accuracies or omissions.

If advice concerning legal or related matters is required, the services of a fully qualified professional should be sought. Information provided is subjective and you are advised to keep this in mind when reviewing this e-book.

The author shall not be liable for any loss of profit or any other commericial damages resulting from use of this e-book.

All links are for information purposes only and are not warranted for content, accuracy, or any other implied or explicit purpose.

About the Author(s)

David Niven, B.Sc.(Eng), is an IT specialist having worked in programming, networking, consulting, and communications over the last 30 years.

He has a wealth of experience in large corporate and SMB environments reviewing, installing and maintaining IT systems.

David is now working with AlliedRisk as the program development co-ordinator preparing training programs, consulting services, and professional systems.

This eBook was a collaborative work by the 2 authors incorporating physical security requirements required in businesses today with the additional risks associated with electronic communications which businesses are also heavily reliant upon.

Leighton Cross is the General Manager of PNP Systems and is a business development consultant with Allied Risk Solutions. He has worked in the IT Industry for about 30 years.

Leighton has worked with Rostering and Workforce Management Systems for over 20 years in the Security Industry. He has many security companies that have used his special talents and regularly consults with them about award payments and rostering issues.

Leighton assisted David in the preparation of the security related material for this eBook.

Introduction

As a business you like to have everything safe, robust and secure.

You would also like to have some assurance that things will continue as they were. Unfortunately change is an ever present danger and assurances don't always come easily.

In regards to safety and security, what worked well 20 years ago to protect computer systems and business networks when they made use of large centralised hardware, is very different today.

Computer hardware is smaller, decentralised and much more powerful than its distant relatives.

Business networks are more widespread and more complex than ever. The physical security that restricted access and stopped undesirables from entry and access still needs to be applied today.

Today there are a lot more worrying concerns about Information Technology security than direct physical attacks on hardware.

Yet we have come to rely on our notebooks, tablets, and smartphones to give us greater flexibility in running, overseeing and managing our business even with the risks that they represent. You may even rely on remote access to your business systems over the Internet.

As a consequence of this flexibility in this current environment of distributed electronic connectivity, we have the proliferation of viruses, hackers and fraud. They attempt to steal identities, passwords, names and addresses, whatever is left unprotected.

Businesses today need to be aware of the risks and cater for them as best they are able.

This is a brief guide intended to help inform you about the risks to your business notably those unseen dangers that do exist, and how to be best prepared for them.

You can protect your business with physical constraints, intended to safeguard your systems, people and data. Guards, door locks, access control systems and security alarms - all of these can assist in providing a visible presence securing your assets and staff.

But they are no protection for the dangers that lurk on the Internet by criminal gangs seeking financial gain.

Don't be unprepared!

Systems and Data Security Examples

◆ Example of Fraud

Hackers recently took Microsoft for $1.2 million USD by stealing points used in the Xbox Live Marketplace.
Reporter Jesse Emspak j.emspak@IBTimes.com. Mar 2011 [1]

◆ Example of Hacking

PlayStation Network Hacked

Last night Sony confessed that an *"external intrusion"* caused the company to take-down the PlayStation Network and also Sony's Qriocity service in order *"to verify the smooth and secure operation of our network services going forward"*.
By Keir Thomas, PCWorld Apr 23, 2011 7:35 AM

◆ Example of Virus Attacks

2002: Melissa virus author David L. Smith, 33, is sentenced to 20 months in a federal prison.
2002: The "Klez" worm - a bug that sends copies of itself to all of the e-mail addresses in the victim's Microsoft Outlook directory - begins its march across the Web. The worm overwrites files and creates hidden copies of the originals.
2002: A denial-of-service attack hits all 13 of the "root" servers that provide the primary roadmap for almost all Internet communications.
2003: The "Slammer" worm infects hundreds of thousands of computers in less than three hours. The fastest spreading worm ever wreaks havoc on businesses worldwide, knocking cash machines offline and delaying airline flights. [2]

◆ Example of Being Unprepared

A solicitors firm in Sydney had been relying on their backup systems for over 2 years after it was first setup.

Then one day the File Server crashed with a failed hard drive. The backup was checked and many important files were not backed up because they were added after the system was installed, and no-one ever updated or even checked the backup system.

A lot of overtime was necessary to recover from this one event.

◆ Example of Inadequate Knowledge

There was the small business owner who never kept paper accounts, as everything was done online, all transactions were kept on a secure flash drive. Then the accounts
database was corrupted, and the flash drive was examined to fix the problem.

Unfortunately, the flash drive was empty as the backups that had supposedly been going on for years were never backing up to the flash drive.

Fortunately, the location of all the backups was found on the host workstation and recovery was made, with little loss. How embarrassing it was that the manager had no idea that his reliance on a backup process for so long was completely misguided.

◆ Examples of Insider Risks

Types of Internal Risks

- ☑ Fraud
- ☑ Sale of data
- ☑ Modification of data for payment (license records,criminal records, welfare status),
- ☑ Stealing (financial institutions and government)
- ☑ Information Theft (company details or customer information),
- ☑ Sabotage - such as deletion of data, logic bombs, defacement, or extortion
- ☑ Errors such as leaving a system vulnerable and
- ☑ Improper disclosure (such as wikileaks.org).

✓ Enron

The Collapse of Enron in the US became the largest corporate failure in global history and an example of a well-planned and institutionalised corporate fraud.

Technology opened up the Internet and many businesses used it to their advantage.

Enron in January 2000 announced a hugely ambitious plan to build a high-speed broadband telecommunications network and to trade network capacity, or bandwidth, in the same way it traded electricity or natural gas.

In July of 2000 Enron and Blockbuster announced a deal to its customers to provide video on demand throughout the world via high-speed Internet connections. Enron poured hundreds of millions into broadband with very little return, and they were rewarded by Wall Street with massive stock rises.

In August 2000 the company was being regarded by some business publications as one of the most admired and innovative companies in the world.

As a result of its off-balance-sheet debt being reviewed, by 28 November 2000 Enron's share rating dropped to junk status. The company filed for bankruptcy protection on December 2.

Arthur Andersen had the job not only of Enron's external but also its internal audits for Enron. They kept staff on permanent assignment at Enron's offices. Many of Enron's internal accountants, CFOs and controllers were former Andersen executives.

In the end when the bubble burst, Enron's IT accounting systems were totally inadequate to stop the fraud and misrepresentation that had been going on.

Data reporting was misused throughout the organisation in order to justify decisions made.

✓ Greyhound Lines Inc.

Greyhound Lines developed a system called "Trips" a reservation and bus-dispatch system. Greyhound spent at least $6 million in the early 1990s building Trips.

But Trips failed miserably when installed. To avoid using the system, agents wrote tickets by hand while customers waited in line and missed busses.

Sales plunged 12% in one month. Just weeks after rolling Trips out, Greyhound disabled it in some regions while trying to trace problems.

The debacle spurred a $61.4 million USD loss for the first half of 1994.

The CEO and CFO resigned over the IT systems failure. [3]

Physical & Electronic Security versus IT Systems and Data Security

The Visible	The Invisible
Guards, Locks and Barriers	Firewalls and Gateways
Access Control	Passwords and Data encryption
CCTV surveillance	Network Authentication and Log files
Alarm Systems	AntiVirus software, Anti Spyware software, Internet Security Solutions

As you may notice in the table above for each real physical presence there is an equivalent IT item that basically provides similar types of protection.

We are used to seeing the very visible physical barriers that are aimed at keeping out undesirables, or at the very least making it more difficult for the criminals to gain easy access to premises, where the risk of being seen / caught is real.

IT Security is very different from Physical Security as it is generally invisible to many businesses, even to their own staff. IT Security is all about restricting access, documents and applications from threats. This is much more complicated than it used to be with complex inter-related networking (intranets and the Internet) and distributed computing systems proliferating.

Many computer systems today provide services to multiple distributed users and as such require the ability to accurately identify the user making a request.

Traditionally the user's identity is verified by checking a password entered during the login process - the system checks the identity and uses it to determine what operations may be performed.

This process of verifying the identity of the user is called authentication. Password based authentication is no longer suitable for use on computer networks. The reason for this is that passwords sent across the network can be intercepted and subsequently used by eavesdroppers to impersonate the original user.

Entering passwords is a small but essential part of the authentication process involving network protocols. The protocols are integral components of the security systems managing threats and attacks against your business network.

Examples of Network security protocols include ....

- ✓ Kerberos - An Authentication Service
- ✓ SMB
- ✓ IP security – IPSEC
- ✓ Socket and Transport layer security
- ✓ SNMP
- ✓ X.800
- ✓ NFS
- ✓ S/MIME

These networking protocols have been around for many years and have significantly matured, providing a very secure platform for communication. Unfortunately Operating Systems and applications are constantly released with weaknesses that need constant patching to keep them up to date.

Vulnerabilities have been found in every major operating system including Windows, Mac OS, various forms of Unix and Linux, OpenVMS, and others. The only way to reduce the chance of a vulnerability being used against a system is through constant vigilance, including careful system maintenance (e.g. applying software patches), best practices in deployment (e.g. the use of firewalls and access controls) and auditing (both during development and throughout the deployment lifecycle). [4]

Now that we have messaging across iPhones, email communications across the world, and a very real integration of the Internet into our local networks there are a great many threats we are exposed to. These are discussed in the section "Vulnerabilities, Weaknesses, Threats and Attacks". The next section "IT Systems and Data Security Risks" looks at an overview of a Business IT Risk Strategy.

IT Systems and Data Security Risks

Systems are the applications (programs) that manage and arrange the data found in their business.

Data is the information that the business relies on, such as invoices, product details, customer details, correspondence (emails and documents), stored in databases on the computer network or on workstations attached to the network.

Both are essential, and both are at risk. It is no good having all your data and not being able to access it without the programs, and it is no good having the programs with no data to access.

The following items are planning processes that can be implemented by a business to minimise IT systems and data security risks. A Risk Management assessment and planning review would normally include these items as key considerations.

☑ Data and System Redundancy

This is the building of strategies that allow for replacement of key IT components, such as hard disk systems using RAID - an acronym for redundant array of independent disks.
Workstations and / or File Servers operate in a networked environment allowing data and applications to be spread over multiple machines.
Other data redundancy options include data replication (making copies elsewhere), data validation (ensuring the information is accurate and reliable), data verification (verify that data being stored is accurate and within acceptable limits, not erroneous), data synchronisation (updating another location with your current up-to-date data).

☑ Power Problems (Brown outs, surges, earth leakage, voltage differential)

Computers and network components require stable clean power. We can put in line filters, UPS systems, circuit breakers, all to protect our expensive hardware and even more expensive down time, loss of reputation, and business confidence.
A stable and reliable incoming power supply can be somewhat out of your control, but you can minimise the risk using a UPS (Uninterruptible Power Supply) protecting your main system components.

☑ Backup Systems

If corruption or damaged files occur in your business, the consequences can be devastating. The problem can be subtle, not showing up until the damage is extensive and widespread. Resolving it can be straightforward, but incredibly time consuming if you don't have somewhere to start and a process to follow.

How often you backup, what you backup and where you put the backup are all important considerations that not only need careful planning but regular testing to ensure the process continues to work and will work when you really need it.

☑ Disaster Recovery Plan

We plan for fires, emergency evacuations, personal injury but rarely do we plan for system failure or IT Disaster Planning.

Every business faces the possibility of some catastrophic event happening that may prevent it from maintaining normal activity.

This may be something like hail damage, a flood, vandalism, fire, security breach, system breakdown etc.

In Australia we have all of these on a fairly regular basis - for example Queensland floods, Victorian fires, and Sydney hail damage.

How quickly your business recovers and gets back to normal operations is dependent on how well the recovery process is planned beforehand.

Every one would like to get back to business as quickly and smoothly as possible. A well prepared disaster recovery plan can make the process much easier to implement as all the planning has already been done, well before the event.

☑ Contingency Plan

What-if type planning is not hard to do, and it costs little to consider, but what a potential benefit if something really does happen. Preparedness is so important – you cannot predict what may be coming just around the corner.

A contingency plan is a plan for backup procedures, emergency response, and post-disaster recovery.

A Contingency Plan is necessary to ensure the availability of critical resources in the event of a disaster and at the same time to facilitate the continuity of operations in an emergency situation.

It is similar to a Disaster Recovery Plan, but it can also include pre-emptive actions, and post-disaster actions that complement and exceed Disaster Recovery planning.

Some Basic Definitions

☑ **What is a Virus?**

A virus is a program or piece of code that causes an unexpected, usually negative event. Viruses are often disguised as games or images with clever marketing titles to attract your attention.

Viruses can corrupt your Computer - disabling normal operation, attack and disable antivirus programs, and stop applications from working altogether. You do not want a virus on your computer, or inside your business network.

They can be transmitted via flash drives (in the autoplay startup application), as attachments to emails, and in the guise of legitimate applications.

The website http://www.spywareguide.com/ lists over 2,000 viruses, trojan horses, Adware and Spyware products written and distributed over the Internet.

☑ **What is Spyware?**

Spyware is a wide range of unwanted programs that exploit infected computers for commercial gain.

They can deliver unsolicited pop-up advertisements, steal personal information (including financial information such as credit card numbers), monitor web-browsing activity for marketing purposes, or hijack your internet browser (HTTP requests) to advertising sites.

☑ **What is Spam?**

Spam is unsolicited or undesired bulk electronic messages. There is email spam, instant messaging spam, Usenet newsgroup spam, web search-engine spam, spam in blogs, and mobile phone-messaging spam. Spam includes legitimate advertisements, misleading advertisements, and phishing messages designed to trick recipients into giving up personal and financial information.

☑ **What is Phishing?**

Phishing is a form of criminal activity using social engineering techniques through email or instant messaging. Phishers attempt to fraudulently acquire other people's personal information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication.

☑ **What is Adware?**

Adware is a legitimate, non-replicating program designed to display ads to the computer user, often based on monitoring of browsing habits, and often in exchange for the right to use a program without paying for it (a take on the shareware concept).

An example of Adware is Bonzi Buddy (shown here). The program when installed was interactive, friendly and very appealing.

He walks, talks, sings, browses and searches the Internet with you. The Bonzi Buddy website went out of business in 2005. It was hard to remove, and was very much an adaware product sending your browser history to its designer. It has however been recently relaunched.

☑ **What is a Trojan Horse?**

A Trojan horse program is a malicious program that pretends to be a benign application.

A Trojan horse program purposefully does something the user does not expect.

Trojans are not viruses since they do not replicate, but Trojan horse programs can be just as destructive.

☑ **What is a Worm?**

Computer Worms are viruses that reside in the active memory of a computer and duplicate themselves. They may send copies of themselves to other computers, such as through email or Internet Relay Chat (IRC).

☑ **What is Malware?**

Malware is a generic term used to describe malicious software such as viruses, Trojan horses, spyware, and malicious active content.

☑ **What is a Virus Hoax?**

Virus hoaxes are not viruses, but are usually emails warning people about a virus or other malicious software program. Some hoaxes cause as much trouble as viruses by causing massive amounts of unnecessary email.

Most hoaxes contain one or more of the following characteristics:

- ✓ Warnings about alleged new viruses and their damaging consequences
- ✓ Demands that the reader forward the warning to as many people as possible
- ✓ Pseudo-technical “information” describing the virus
- ✓ Bogus comments from officials: FBI, software companies, news agencies, etc.

If you receive an email message about a virus, check with a reputable source to ensure the warning is real before you do anything you may regret.

Sometimes hoaxes start out as viruses and some viruses start as hoaxes, so both viruses and virus hoaxes should be considered a threat.

Hoaxes have been sent out warning of dangerous files that should be removed, that in fact are quite safe Operating System files.

☑ **What is a Hacker?**

A hacker is a person who creates and modifies computer software and hardware, including computer programming, administration, and security-related items.

This can be done for either negative or positive reasons.

Criminal hackers create malware in order to commit crimes.

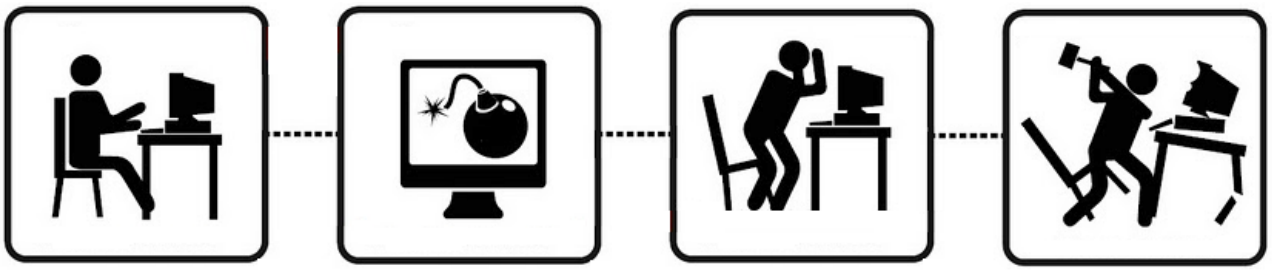
We now look at weaknesses and potential failure points that can be present in a business network that could result in attacks.

Not good Password Management

Vulnerabilities, Weaknesses, Threats and Attacks

The key aspects of security are confidentiality, integrity, and availablity. We need to make sure that these are always maintained in our business IT Systems and Data, otherwise we may not always have an operating Business.

To protect a Business from various security threats, we need to be aware of the Vulnerabilities in the current system, any weaknesses that have the potential to be exploited and what exposure we have to threats from outside and also within the business.



Vulnerability

It is a characteristic of the system that permits attackers to mount a successful attack. Sometimes also called a “security hole”. An information security “vulnerability” is a mistake in software that can be directly used by a hacker to gain access to a system or network. [5]

A vulnerability can allow an attacker to compromise the availability, confidentiality, or integrity of a computer system. Vulnerabilities may be the result of a programming error or a flaw in the design that will affect security. Vulnerabilities can affect both software and hardware. It is important to stay abreast of new vulnerabilities being identified in the threat landscape because early detection and patching will minimize the chances of being exploited.

A vulnerability is a state in a computing system (or set of systems) that can

- ✓ allow an attacker to execute commands as another user
- ✓ allow an attacker to access data that is contrary to the specified access restrictions for that data
- ✓ allow an attacker to pose as another entity
- ✓ allow an attacker to conduct a denial of service attack on the business

Examples of vulnerabilities include:

- ✓ phf (remote command execution as user “nobody”)
- ✓ rpc.ttdbserverd (remote command execution as root)
- ✓ world-writeable password file (modification of system-critical data)
- ✓ default password (remote command execution or other access)
- ✓ denial of service problems that allow an attacker to cause a Blue Screen of Death
- ✓ smurf (denial of service by flooding a network)

Weakness

A weakness in a system is a potential vulnerability, whose risk is not clear. Sometimes several weaknesses might combine to yield a full-fledged vulnerability.

Threat

A threat is a circumstance or scenario with the potential to exploit a vulnerability, and cause harm to a system.

Symantec Intelligence Quarterly Report: July - September 2011 [6]
Highlights from the SARC 2011 Quarterly Report on Threat Activity in the World

Approximately 155 million unique malicious code threats were observed over the quarter.

Additionally, around 1 billion attacks were blocked during the third quarter of 2011.

The compromise of a popular e-commerce shopping cart software package affected 6 million websites.

Noteworthy scams were observed during the quarter featuring Hurricane Irene, the death of Amy Winehouse, and the potential release of the iPhone 5.

Threat Activity Trends

During the final quarter of 2011, the United States had the most overall malicious activity, with 19 percent of the total - down slightly from 20 percent in 2009, when it also ranked first.

The United States was the top country for originating network attacks in 2010.

In 2010, the healthcare sector had the highest percentage of data breaches that could lead to identity theft.

The financial sector was the top sector in 2010 for identities exposed in data breaches.

The leading cause of data breaches that could lead to identity theft in 2010 was the theft or loss of a computer or other data-storage device.

Hacking was the leading source of reported identities exposed in 2010.

The most exposed type of data in deliberate breaches (hacking, insider breaches, or fraud) was customer-related information.

The United States was the most targeted county by denial-of- service attacks.

Source: Symantec Corp., Internet Security Threat Report, Vol. 16. [7]

Attack

An attack is a deliberate attempt to breach a system's security.

Attacks are usually classified into two types:

(1) **Passive attack** refers to attack that does not result in a change to the system, and attempts to break the system solely based upon observed data.

(2) **Active attack** on the other hand involves modifying, replaying, inserting, deleting, or blocking data.

Types of Attacks can include ...

Attacks against confidentiality
- – eavesdropping
- – traffic flow analysis

Attacks against integrity
- – IP spoof
- – Sequence number attack
- – Man-in-the-middle attack

Attacks against availability
- – Denial of Service attack
- – Traffic redirection

Precursor to attack
- – Port scan

Specific Types of Attacks

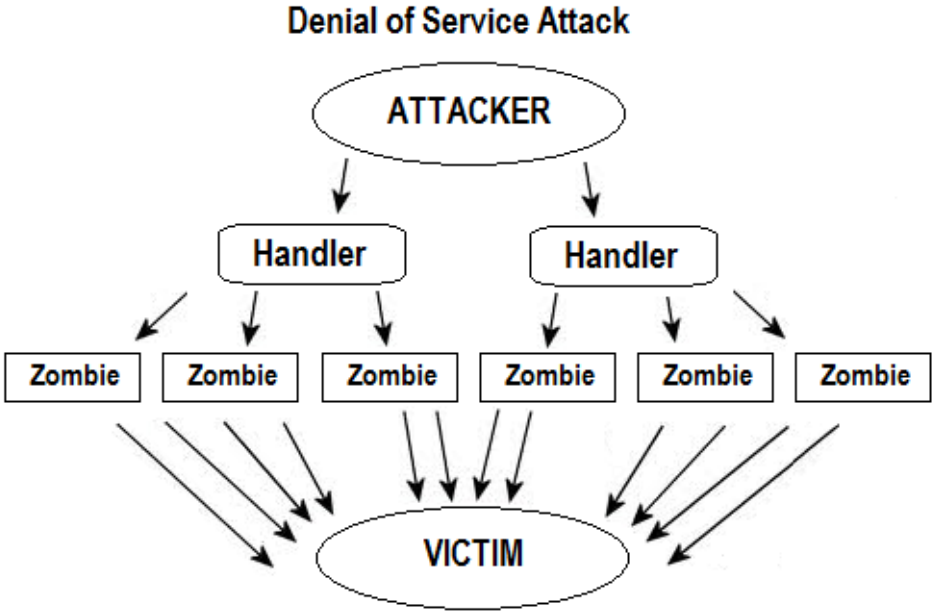
1. **Denial of Service Attacks**
US National Cyber Alert System - Cyber Security Tip ST04-015 (archive) [8]

Understanding Denial-of-Service Attacks
You may have heard of denial-of-service attacks launched against websites, but you can also be a victim of these attacks. Denial-of-service attacks can be difficult to distinguish from common network activity, but there are some indications that an attack is in progress.

What is a denial-of-service (DoS) attack?

In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.

The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. When you type a URL for a particular website into your browser, you are sending a request to that site's computer server to view the page. The server can



only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process your request. This is a "denial of service" because you can't access that site.

An attacker can use spam email messages to launch a similar attack on your email account. Whether you have an email account supplied by your employer or one available through a free service such as Yahoo or Hotmail, you are assigned a specific quota, which limits the amount of data you can have in your account at any given time. By sending many, or large, email messages to the account, an attacker can consume your quota, preventing you from receiving legitimate messages.

What is a distributed denial-of-service (DDoS) attack?
In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses (the affected PC is termed a "Zombie" acting under the influence of the attacker). The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.

How do you avoid being part of the problem?

Unfortunately, there are no effective ways to prevent being the victim of a DoS or DDoS attack, but there are steps you can take to reduce the likelihood that an attacker will use your computer to attack other computers:

Install and maintain suitable anti-virus software.

Install a firewall, and configure it to restrict traffic coming into and leaving your computer.

Follow good security practices for distributing your email address. Applying email filters may help you manage unwanted traffic.

Author: Mindi McDowell Copyright 2004 Carnegie Mellon University.

2. Phishing
US National Cyber Alert System - Cyber Security Tip ST04-014 (archive) [9]

Avoiding Social Engineering and Phishing Attacks
Do not give sensitive information to anyone unless you are sure that they are indeed who they claim to be and that they should have access to the information.

What is a social engineering attack?

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

What is a phishing attack?

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Phishing attacks may also appear to come from other types of organizations, such as charities.

Attackers often take advantage of current events and certain times of the year, such as

- ✓ natural disasters (e.g., Hurricane Katrina, Indonesian tsunami)
- ✓ epidemics and health scares (e.g., H1N1, SARS, Bird Flu pandemic)
- ✓ economic concerns (e.g., Taxation Office or IRS scams)
- ✓ major political elections
- ✓ holidays

How do you avoid being a victim?

Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

Don't send sensitive information over the Internet before checking a website's security. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g. .com vs. .net).

If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request - instead, check previous statements for contact information.

Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.

What do you do if you think you are a victim?

If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.

If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account. Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.

Author: Mindi McDowell Copyright 2004, 2009 Carnegie Mellon University.

Prevention and Protection

IT Systems and Data Security is better handled in a pre-emptive manner, rather than after the event. Of course that cannot always be the case as new types of attacks are constantly appearing.

Preventing problems from occuring is much better than having to spend a lot of time and resources looking at ...

- ✓ What has been compromised on your network - both Data and Applications
- ✓ Options for Data and Application recovery - which backup and how much to recover
- ✓ Detecting where the intrusion occurred and how best to address it - patching vulnerabilities after the event
- ✓ Rebuilding workstation(s) or Server(s) that may have been compromised
- ✓ Checking all storage devices, flash drives, backup systems, notebooks, tablets for signs of attack - notably data corruption and infected files.

Reputation and Customer base can be severely impacted by business downtime.

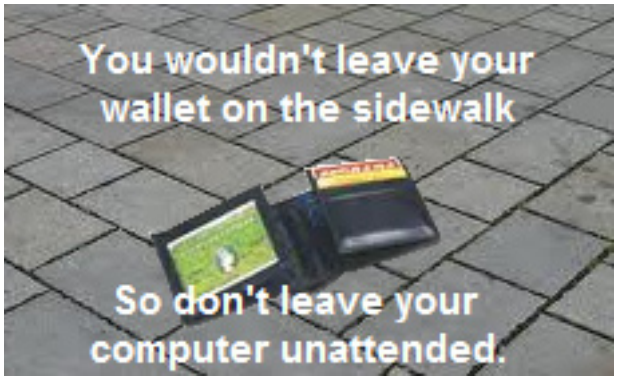
Consider the following suggestions as steps in preventing attacks and giving you some reasonable protection.

☑ **Secure What you Throw Away**

Take the situation of storage and disposal of important documents (client details, personal information, passwords or even essential business documentation).

You wouldn't give a copy of your key to the office to a complete stranger, but that's what can happen if you dispose of old equipment without a proper clean up.

Hard disks can still store information after being reformatted and disposed of. In Africa, some salvage experts were discovering files, emails and photos on old computers thrown out by businesses after an upgrade. They were able to recover deleted files and information stored on the old drives.



Paper documents disposed of by a business should always be shredded if they contain sensitive information like names, addresses or account details. So also hard disk drives should be properly wiped of any sensitive or confidential data. This can easily be fixed and should never happen.

There are plenty of wipe programs that can be used to completely erase a hard disk.

☑ Beware of the Dangers of Social Networking

Social Networking in its essence encourages people to interact online. It has a very serious downside in that once material is placed on the Internet it has a habit of staying on the Internet and proliferating. You can prevent problems by taking sensible steps to limit your exposure and risk online.

Never put confidential or private information up on the Internet - no compromising photos, criticism of fellow-workers, anything that might come back and haunt you.
Never accept invitation offers of a new friend.
Just because they may know someone you know, doesn't mean they are your friend. There have been many cases where people are tricked into accepting a friend, who then use that new access to target all your friends and associates using your name as a reference, all the while they are criminals getting any information they can glean, for identity profiles sold on the black market.

Never enter credit card details, medicare, banking account details, or other personal information online, unless you are on a secure website that you are familiar with and use a secure transaction (https).

☑ Use Secure Transactions (HTTPS)

Hyper Text Transfer Protocol Secure (HTTPS) is a secure version of the normal Hyper Text Transfer Protocol (http). HTTPS allows secure ecommerce transactions, such as online banking by encrypting the information sent between you and the server. Web browsers such as Internet Explorer and Firefox display a padlock icon to indicate that the website is secure.

When a user connects to a website via HTTPS, the website encrypts the session with a digital certificate. A user can tell if they are connected to a secure website if the website URL begins with https:// instead of http://.

☑ Use Antivirus and Internet Security software

On the Internet today, you must use antivirus software. Businesses can get group licenses that cover all their workstations at a reasonable cost. The bigger software developers produce very secure and reliable systems that really do protect you from many of the dangers we have spoken about. These are some of the more well known and trusted developers - McAfee, Norton, Avast, Bitdefender, Kaspersky, Panda, F-Secure, AVG, Avast, BullGuard, Avira, and ESET NOD32.

They usually have one or 2 year subscription offers covering all updates to their virus definitions and program updates.

Some even have free antivirus software for home users, that is almost as good as the professional paid versions. So you really don't have any excuse for not getting some antivirus protection.

Strongly consider using a software package that not only includes the ability to scan for viruses,
but also protects your computer from keyloggers & other spyware, and that also uses real-time detection for any unauthorized attempts to gain access to your computer. There are plenty of reliable reviews of the latest antivirus software releases. Compare them for levels of protection, reliability, ease of use and price.

☑ **Keep your antivirus definitions & security software up-to-date**

New viruses, worms, phishing scams and Trojans are developed all the time. It's no good having excellent protection that is never kept up to date. All good antivirus software companies allow you to download updates for antivirus definitions (this is what tells the antivirus software what viruses to look for) as well as the core security software itself for free, or for a small subscription fee.

You should let your software update itself regularly (daily) to ensure that you are always protected from the latest threats.

☑ **Use a Firewall**

A "firewall" can be a software application or a hardware device that acts as a buffer between your computer(s) and the rest of the Internet. Firewalls can be setup to only allow certain types of information to be transmitted between your computer and the Internet. Firewalls are a great way to reduce the risk of attacks from hackers, keyloggers, worms and other malicious attacks on your computers. Many Internet security software packages include a firewall application. Most ADSL 2+ modems also include Firewall protection to stop traffic before it hits your business network.

Setting up a Firewall is not for the faint hearted and can be complicated, so get the right person to review and configure Firewall protection on your Business network.

☑ **Run a thorough virus scan regularly**

Many antivirus programs can automatically run in the background (real time scanning) to watch for new bugs before they have a chance to cause any damage. If you do a lot of work on the Internet, and receive a lot of correspondence by email, it's worth scanning your workstation regularly, let it run overnight or set up a schedule so that it cuts in early in the morning for a full scan.

Better to be safe than sorry.

☑ **Be Careful of Suspicious Emails**

Be wary of e-mails asking you to confirm personal information or account details, especially if there is an urgent tone to the message. Also be wary of special offers - if it sounds hard to believe then it more than likely is. If you are ever uncertain about an email, then directly contact the company before doing anything.

Phishing scams are very good at making an e-mail or other social media message appear to come from a reputable company or service that you deal with. In some cases, the e-mail may contain links that look like they are from the company's website (notably banks or finance groups), but actually link to a malicious site that is run by hackers or identity thieves.

Here are some more detailed tips of what to watch out for to avoid being the victim of a phishing scam:

- ✓ Don't use the links or phone numbers in any suspicious e-mails to contact the company.
- ✓ Instead, go to the company's website directly by typing in their address, or call the company at a known phone number and ask about the message.

Even though a link may look legitimate, hackers may have masked the actual web address that you will go to when clicking on the link.

☑ **Never fill out any forms in an e-mail sent to you**

If the e-mail itself contains fields asking you to enter personal information, don't do it.

Banks particularly would **never** ask you to do this. If uncertain go directly to the company's website and attempt to locate the form there. If it's a legitimate request, you'll be able to find what you need on the company's website.

☑ **Enable your web browser's anti-phishing detection service**

Most popular web browsers today (including Internet Explorer 7 & higher, Firefox, Safari and Google Chrome) include the option to check websites you visit to ensure they are not known phishing sites. Most antivirus programs also now have pre-emptive checking on websites, checking for malicious attacks.

When enabled, if you visit a website that is known to be part of a phishing scam, the web browser will display a warning (such as turning the address bar red, or displaying a message that the website you are visiting is unsafe) indicating that you should not continue to the website.

☑ **Scan all e-mail attachments before you send or receive them**

Most antivirus programs operate with e-mail software to automatically scan all incoming and outgoing mail for you. If your antivirus program does not have this option, use your antivirus program to scan any attachments you receive in an e-mail before you open them.

It is also a good idea to scan attachments before you send them to ensure that you aren't unknowingly spreading a virus. Scan any files you receive through a file-sharing service, Chat or Instant Messaging program.

Virus distributors extensively use file-sharing, Chat and Instant Messaging services to distribute their work. Scan all files you receive through these services, and be especially careful if you do not know the person you are receiving the files from!

☑ **Configure your e-mail program to not automatically open new messages**

Many viruses sent through e-mail take advantage of the fact that some e-mail programs will automatically try to preview or open a new message. Disabling this option will allow you to delete a suspicious e-mail before displaying it, reducing the potential for a virus or other malicious program to be released on your computer.

☑ **Scan any removable media (like Flash drives or external hard disks) before opening files on the disk**

This is especially true if you have been given a disk by someone who you don't know, and just as important for someone you do know (friends can easily spread a virus to all their associates because they are a little more trusting of them). It's worth waiting a little while to ensure the drives are clean before exposing your system to an uncertain risk.

☑ **Watch out for unexpected macros in Microsoft Office documents**

While macros in Microsoft Office documents are typically safe, they can also be used to trigger viruses. If you open a Microsoft Office document from someone you are not familiar with and it contains a macro, do not allow the macro to run. You should also not run a macro if a document says it has a macro and you know it should not. The latest versions of Microsoft Word and Excel automatically disable macro features when first installed, due to this threat.

☑ **Keep your operating system, web browser and other key applications up-to-date**

Many security threats can be easily avoided by checking for software updates regularly. Microsoft offers two update services - Windows Update and Office Update that will automatically check for all critical security updates as well as other recommended updates for Windows, Internet Explorer, and Microsoft Office applications.

☑ **Backup Often**

Backing up regularly and keeping copies of your backup separate from your computer is a great way to protect against losing data. This is not only good protection against virus attacks but also because of hardware failure as hard disks can fail over time and use.

By keeping regular backups, you'll always be able to restore your files should they become infected, deleted or damaged. Once the backup is complete, remove the device from the computer. This will prevent the backup device from being infected as well, should your system get a virus. Labeling your backup devices with the date of the backup will help you identify which disk(s) to restore from so that you restore a "clean" version of your files. Backup devices can include external hard disks, flash drives, writeable DVD or tape backup units.

☑ **Check your Credit Reports monthly**

A great way to monitor your identity and make sure you haven't been the victim of electronic identity theft is to check your credit reports every month. Look for any unrecognised transactions. If unsure check with your bank.

☑ **Seriously Consider a Replacement Schedule**

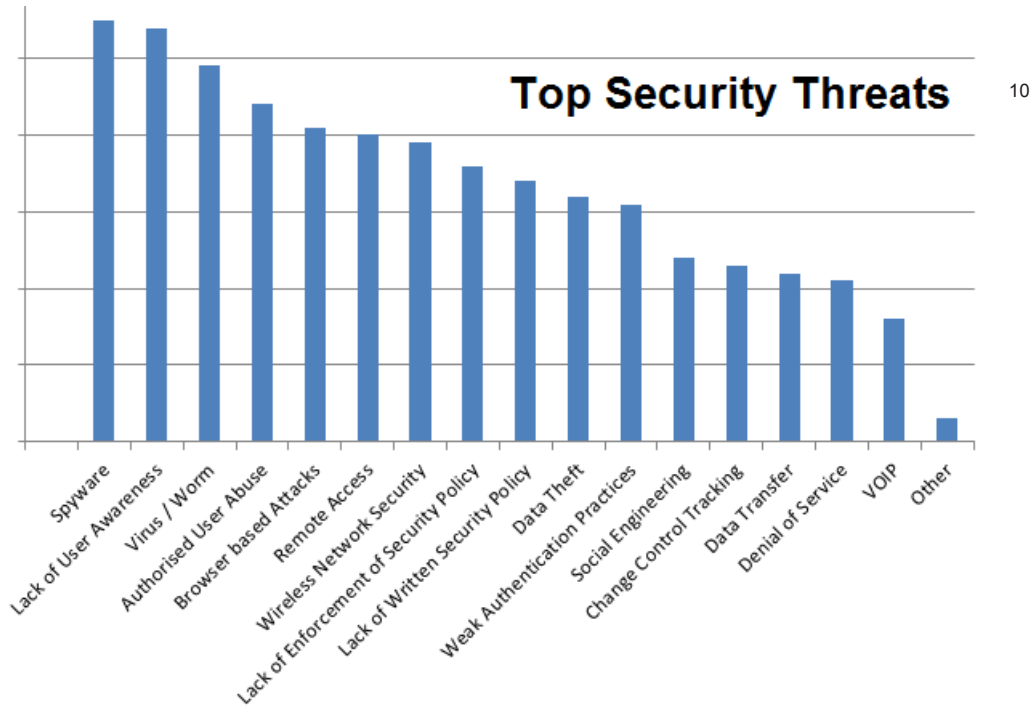
You expect to trade in your vehicle after some years of use, in order to reduce maintenance, maintain a minimum reliability and get a better trade in value. Computers and other hardware devices (printers, modems, switches etc) are no different. They also have parts that wear out, based on use and time.

Expect replacements of the following items after the indicated time frame.

DVD Writer	2 years
Power Supply	2 years
Hard Disk drive	3 years
Video Card	2 years
Motherboard	6 years
RAM	3 years

Some of these items can be easily replaced (like the Power Supply, RAM, Hard Disk drives, and DVD writers), but over time some cannot. New motherboards are released every 6 months, so getting a similar type after 6 years is almost impossible.

Video cards are constantly changing models and types - take for example motherboard connection types (Bus interface) for video cards (from 1981 to the present), they include ISA XT, ISA AT, MCA, NUBUS, EISA, VESA, PCI, AGP 1x, AGP 2x, AGP 4x, AGP 8x, PCIe x1, PCIe x4, PCIe x8, PCIe x16, PCIe x16 2.0. This represents a new type every 2 years - each incompatible with the previous model. You may find you cannot replace that card if it fails.



What To Do?

We have already touched on many of the steps you should take in the section on “Prevention and Protection”. But there are a few more strategic actions that could be considered, mentioned in the section “IT Systems and Data Security Risks”.

Awareness, Planning and Action

It is first necesary to to be fully aware of the risks. Awareness is part and parcel of training, education and consultation. Read, consult and discuss these issues with suitable advisors so that you are better informed.

After being made aware of the risks, you need to determine what actions to take next, if any to address these issues.

You can prepare an Action Plan, which may or may not include a Disasater Recovery Plan or Contingency Plan.

An action plan determines

- ✓ who is involved in the planning and decision processes
- ✓ who is accountable for each process
- ✓ who is to document the processes and
- ✓ who is to train staff on their requirements and responsibilities

The Action plan may recommend Risk Management Assessment and / or Planning be undertaken to determine the potential risks and exposure to attacks from within or outside the business; the consequences of downtime; vulnerabilities, threats and weaknesses of the existing business systems; and the cost benefit of undertaking such a process.

The Action plan may take up the form of

- ✓ A statement of Purpose (how it integrates into the Business Mission statement),
- ✓ Detailing Objectives Required,
- ✓ Identifying Target Audience (Stakeholders),
- ✓ Considering impacts to related Groups or Services and
- ✓ Preparing a Guide or handout for all concerned as to how it wil operate and function.

Forms

Consider preparing and distributing standard forms in regard to IT Systems and Data security, such as

- ✓ Reports of Attacks (Incident Reports) including resolution of the problem (sample shown below)
- ✓ General Awareness of Risks (see sample on next page - IT Security Awareness Questionnaire)

The advantage of forms is to

- ✓ make staff aware of the possible risks,
- ✓ make staff aware that management is concerned about these matters, and
- ✓ encourage involvement so that everyone has an opportunity to provide an input to the process.

Submitting forms should be properly prepared so that everyone gets access to one in a timely manner, and feedback is also provided in a suitable timeframe.

Otherwise it may be seen as a waste of time and resources.

INCIDENT REPORT

Entered by: _____
Date: __/__/____
Location: _____
Staff Involved: _____
Contact Details: _____
E-mail: _____
Department: _____
Phone: _____
Description of the event: _____
_____
Circumstances surrounding the event (before and after activity):
_____
_____
Problem Resolution:
_____
_____
Office Use
Report No. _____
Discussed with Supervisor: (Name and Date)
_____
Completed: _____

IT SECURITY AWARENESS QUESTIONNAIRE

We are conducting a study to help determine ways of educating our staff about information security issues. We would appreciate if you could spare 10 minutes to answer a few brief questions regarding information security.

1. How do you currently access the Internet at work?
a. [ ] A dial-up connection
b. [ ] ADSL (broadband) connection
c. [ ] Company Internet

2. Where do you use your computer (check all that apply)?
a. [ ] Home
b. [ ] Office
c. [ ] Public-access location (school, library, community centre)
d. [ ] Internet café
e. [ ] Internet/phone centre
f. [ ] Other (please indicate where)_____

3. Many people define safety as protection from adverse effects. With this in mind, on a scale of one to five, with one being very concerned, and five being the least concerned, how concerned are you about the safety of your information technology assets (computer, peripherals, electronic data, etc.)?

1 2 3 4 5
Very Somewhat Least

4. Which of the following do you think poses the greatest threat to your information technology? Select any that apply to you:
a. [ ] Viruses and worms
b. [ ] Spam and other unsolicited e-mails
c. [ ] Hackers
d. [ ] Fraudulent schemes
e. [ ] Malicious software (e.g. spyware)
f. [ ] Faulty computer hardware
[ ] Other_____

5. Are you aware that head office will be evaluating the potential threats to the businesses' information technology systems, and that the information you provide could help design a plan to protect you from potential threats?
[ ] Yes, I am aware of this
[ ] No, I am not aware of this

6. On a scale of one to five, with one being very knowledgeable and five being the least knowledgeable, please rank your knowledge of the steps that can be taken to protect your information technology assets:
1 2 3 4 5
Very Somewhat Least

7. Do you have any of the following in place to protect your computer and electronic data?
Please indicate all that apply.
a. [ ] Anti-virus software that is updated regularly
b. [ ] Firewall
c. [ ] Anti-spam filter
d. [ ] Good password practices
e. [ ] Process of regular back-up of data
f. [ ] Up-to-date Internet browser with encryption
g. [ ] Others (please indicate) _____

8. Which would be the best way to provide you with information on how best to protect you from potential dangers? In other words, are you most likely to pick up information from the:
a. [ ] Newsletters that come to your office
b. [ ] Executive meetings
c [ ] Posters
d. [ ] Emails
e. ____Other (please describe) _____

Thank you for participating in this survey. We plan to use your answers to help us develop information in order to raise awareness of the importance of information security.

Please check here if you would like to receive additional information on information security.
[ ] Yes
[ ] No

Summary

Physical security has played an important role in providing safety and security to businesses in the past, but today we need more than just physical protection that can deter potential attacks to our business systems and data.

The threat from criminal gangs is very real. We need to be exposed to the Internet for communications and services more than ever before. But this exposure introduces risks that must be considered carefully to avoid potential threats and attacks.

The incidence of ...

- ✓ Mass email spamming attacks
- ✓ Malicious emails
- ✓ Website script processes
- ✓ QR Code re-direction

are all gearing up to be major incidents for the year ahead.

The on-going problems of patches of vulnerabilities including new driver issues in 32 and 64 bit operating systems will continue.

Follow a replacement schedule for equipment in order to maintain reliability of components.

Provide regular maintenance of computer equipment - scanning hard disk drives, flash drives, backup devices for viruses, adware or malware.

Perform regular backups of important systems and data, and check that these backups are working.

Ensure staff are aware of the potential risks and dangers on the Internet.

At the organisational level consider Contingency Planning, Disaster Recovery Planning and Risk Assessment.

The warnings are there - so be prepared, and be aware of the potential dangers and risks.

For a confidential, obligation free consultation act now.

Proven Risk Management Programs - Allied provides proven systems to support the integration of security awareness and preparedness into your core business units.

Confidential Obligation Free Consultation - As a commitment to our quest for excellence in standards and quality of service, we etend to you an obligation free, confidential consultation top discuss your specific security and training requirements.

100% Satisfaction Guarantee - Allied provides a 100% satisfaction guarantee attached to all our products and serices. If you are not 100% satisfied with our service and we are unable to deliver within a reasonable time, there will be no charge.

Call us on (02) 9635 0477 today!
Website: www.alliedrisk.com.au
Email: info@alliedrisk.com.au

Master Licence Number: 408900846

References

1. Microsoft fraud link: http://www.ibtimes.com/articles/121395/20110310/microsoft-xbox-live-marketplace-hacked.htm

2. Virus Attacks link: http://www.securityfocus.com/news/2445

3. Insider Risks - Greyhound Lines Inc. IT Failure link: http://www.computerworld.com/computerworld/records/images/pdf/44NfailChart.pdf

4. Vulnerabilities link: http://en.wikipedia.org/wiki/Vulnerability_(computing)

5. Vulnerability link: http://cve.mitre.org/about/terminology.html

6. Threat link: http://www.symantec.com/business/threatreport/quarterly.jsp

7. Threat Activity Trends link: http://www.symantec.com/business/threatreport/

8. Denial Of Service Attacks link: http://www.us-cert.gov/cas/tips/ST04-015.html, Author: Mindi McDowell Copyright 2004 Carnegie Mellon University.

9. Phishing link: http://www.us-cert.gov/cas/tips/ST04-014.html, Author: Mindi McDowell Copyright 2004, 2009 Carnegie Mellon University.

10. Top Security Threats - http://partnerit.com/2009/09/shocking-network-security-numbers/