

IT SECURITY REPORT

FOR

A Company

Date

INTRODUCTION

Why IT Security Matters

Security is the biggest challenge facing small and medium-sized enterprises (SMEs). Ever-changing security threats from both inside and outside the business network can wreak havoc on business operations, affecting profitability and customer satisfaction. SMEs must also comply with new regulations and laws created to protect consumer privacy and secure electronic information.

Security Issue 1 – Worms and Viruses

Computer worms and viruses remain the most common security threat, with 75% of SMEs affected by at least one virus in the last year (source: Maritz Research, 2005). Worms and viruses can have a devastating effect on business continuity and the bottom line. Smarter, more destructive strains are spreading faster than ever, infecting an entire office in seconds. Cleaning the infected computers takes much longer. The catastrophic results are lost orders, corrupted databases and angry customers! As businesses struggle to update their computers with the latest operating system patches and anti-virus software, new viruses can penetrate their defences any day of the week. Meanwhile, employees spread viruses and spyware by unwittingly accessing malicious websites, downloading untrustworthy material or opening malicious e-mail attachments. These attacks are unintentionally invited into the organisation, but still cause significant financial losses. Security systems must detect and repel worms, viruses and spyware at all points in the network.

Security Issue 2 – Information Threat

Information theft is big business today. Malevolent hackers break into business networks to steal credit card or social security numbers for profit. SMEs are at risk because they are seen as an easier mark than large corporations. Protecting the perimeter of the network is a good start but it is not enough since many information thefts have help from a trusted insider such as an employee or contractor. Information theft can be costly to SMEs, since they rely on satisfied customers and a good reputation to help grow their business. Businesses that do not adequately protect their information could face negative publicity, government fines or even lawsuits. For example, new consumer laws enacted in California require any business that suspects customer information has been viewed by unauthorised people must notify all their customers. Any security strategy must prevent theft of sensitive electronic information from both inside and outside the business.

Security Issue 3 – Business Availability

Computer worms and viruses can drastically affect the reliability of network resources, which in turn affects businesses' ability to respond quickly to their customers; but worms and viruses are not the only threat to business availability. With networks so critical to day-to-day business operations, cyber-terrorists have begun targeting businesses for blackmail, threatening to bring down websites and e-commerce operations unless their demands are met. These denial-of-service (DoS) attacks send large volumes of traffic to a critical network element, either causing it to fail or to be unable to process legitimate traffic. Once again, the results are disastrous: data and orders are lost and customer requests are not answered. If these attacks become public, a company's credibility is damaged. While most of the publicity surrounding DoS outages has focused on major banks and global 500 companies, SMEs are not immune. They are viewed as less prepared for attacks than large corporations.

There are many other less dramatic but more likely attacks that threaten SMEs' availability and therefore profitability and customer satisfaction. For example, a resource theft attack breaches business computers and networks, using them for illegal file sharing of music, movies or software. Often, businesses are unaware that a security breach is underway. Meanwhile, their computers and networks are slow to respond to customers and their unwitting participation in illegal file sharing leaves them vulnerable to lawsuits.

Security Issue 4 – The Unknown

With every new advance in computing and communications, some malicious hacker finds new ways to exploit that technology for gain or mischief. New hardware or software releases present a new opportunity. Peer-to-peer networking and Internet Messaging (IM) were still relatively new applications when their users were attacked by malicious code written specifically for them. Mobile phones are now targets of viruses. No-one knows what's coming next, but the best defence is one that will be able to easily adapt to future threats without breaking the bank.

Security Issue 5 – Security Legislation

Aside from these malicious security threats, new laws and regulations require that SMEs protect the privacy and integrity of the information entrusted to them. The onus is on businesses to comply with laws and regulations that apply to their business in their markets. Unfortunately, many SMEs find their resources only stretch so far. Yet customers want assurance that the information they entrust to businesses is kept private.

All businesses must take steps to secure their business infrastructure, but SMEs in particular require simple, right-sized, affordable solutions.

1 SECURITY POLICY

1.1 Information Security Policy

Your Organisation's Score: 0%

Recommendations:

The creation of an information security policy is a crucial step towards the effective management of information across all levels of an organisation.

It is critical that any information security policy created by an organisation is approved by management, and that this is subsequently published and communicated to all employees.

This document should be maintained and reviewed regularly, or in response to a change in circumstances that may affect the risks to an organisation's information. An example here may be the introduction of a web site, or the use of e-commerce.

2 SECURITY ORGANISATION

2.1 Information Security Infrastructure

Your Organisation's Score: 50%

Recommendations:

Successful implementation of a security programme is more likely if there is some formality to the roles, responsibilities and communication involved in securing a company's information.

The most successful implementations normally involve integrating this formality with current management structures rather than trying to impose something alien that cuts across normal reporting and communication lines.

A fundamental element of this approach is the identification of external resources (people, organisations etc) that have specialist knowledge and skills. Information security is at times a complex discipline that requires specialists. Keeping up to date with trends, concepts, tools, standards and methods can prove invaluable, and specialist services can often do this more effectively than general management. An example of such specialist services is the control and eradication of computer virus infections.

2.2 Third Party Access

Your Organisation's Score: 50%

Recommendations:

It is vital that any third party organisations that have access to your information are managed effectively.

Careful consideration needs to be given to:

1. Who has access to your buildings and IT systems?
2. The reasons why access has been granted e.g. trading partners or joint ventures.
3. Any third parties that may be located on site for a period of time, such as contractors.

Ensuring any contracts you have include relevant clauses outlining information security responsibilities can save you from considerable pain. A common practice is to request that third parties agree to abide by your information security policy.

Examples of some of the areas that such a contract may cover could include:

1. The general policy on information security.
2. A description of the service provided.
3. Target levels of service.
4. The respective liabilities of parties.
5. Responsibility with respect to legal matters, such as data protection legislation and intellectual property rights (IPR).
6. Access control agreements.

The above have been included as examples and any contracts drawn up may include all of these and many more.

2.3 Outsourcing

Your Organisation's Score: 100%, therefore no recommendations are required.

3 ASSET CLASSIFICATION & CONTROL

3.1 Accountability

Your Organisation's Score: 75%

Recommendations:

This is a fundamental concept of information management. Without a comprehensive identification of your company's information and supporting technical assets, it would be impossible to tell if they are being protected effectively.

You should be able to identify clearly your assets, their relative value and their importance. With this information, you can provide levels of protection appropriate to the value and importance of the assets.

Examples of assets are:

1. Information assets e.g. databases, archived information.
2. Software assets e.g. application software, system software.
3. Physical assets e.g. computer equipment, communications equipment, media.
4. Services e.g. general utilities such as heating and lighting.

3.2 Information Classification

Your Organisation's Score: 60%

Recommendations:

It makes sense to manage your sensitive and confidential information more carefully than information which is of little value. An acceptable approach to simplify this is to classify information into tiers. The more sensitive tiers of information are subject to more stringent controls.

Not doing this could result in information that is overprotected. This wastes time and money and can bring the security process into disrepute if your staff think established controls inappropriate. Applying insufficient control can result in real harm to your company through information loss, theft or disclosure.

Any classification scheme should be simple. To use more than three tiers (for example, 1. Secret, 2. Restricted and 3. Internal) with everything else being 'public' is very difficult to manage.

4 PERSONNEL SECURITY

4.1 Security in Job Definition & Resourcing

Your Organisation's Score: 20%

Recommendations:

A well-trained, well-educated and suitably motivated workforce is one of the most cost-effective means of ensuring ongoing information security. It is recognised, however, that malevolent or ill-disposed staff can pose a real threat to a company's information assets.

To address this, there are a variety of measures that can be used to reduce the risk. These include:

1. Incorporating security in job descriptions – this should include any general responsibilities for the implementation or maintenance of security, as well as any specific responsibilities such as the execution of a particular process e.g. virus scanning, back-ups.
2. Personnel screening – where possible, verification checks on permanent staff should be carried out at the time of job application. This may include the use of character references, a check of the CV, confirmation of a claimed academic record and professional qualifications. These checks could be extended when an individual is to have access to sensitive information. It is important that similarly appropriate checks are made on contractors and temporary staff who have the same access as permanent staff.
3. Using confidentiality agreements as part of any employment agreement.

4.2 User Training

Your Organisation's Score: 0%

Recommendations:

Although seen by many as the single most important measure in creating an effective information security infrastructure, user training and education is often ignored. People are often cited as the weakest link in any organisation and training will help significantly to bolster security.

All employees (and where relevant, third parties) should receive appropriate training. This should include security requirements, legal responsibilities, business controls, as well as training in the correct use of IT facilities and applications, e.g. log-on procedures, e-mail use, etc.

Options for delivering this training can vary from face-to-face training to web-based interactive e-learning. Specialist companies often supply this kind of service.

4.3 Responding to Security Incidents & Malfunctions

Your Organisation's Score: 20%

Recommendations:

Security incidents happen, regardless of the range and quality of security measures in place. It is crucial that you learn from such incidents, and that your company establishes the means by which incidents can be reported, recorded and responded to. The first step in this process is the reporting. Incidents should be reported through appropriate management channels as quickly as possible. All employees and contractors should be made aware of the procedure(s).

Allied to this should be a requirement for staff to note and report any observed or suspected security weaknesses in, or threats to, systems. Such a requirement can be built into contracts or employment terms and conditions.

It is important that there is also a process in place for learning from incidents. The types, volumes and costs of incidents and malfunctions should be quantified and monitored, and this information should be used to identify recurring or high impact incidents or malfunctions.

Finally there should be a formal disciplinary process for employees who have violated the organisation's security policies and procedures.

5 PHYSICAL & ENVIRONMENTAL SECURITY

5.1 Secure Areas

Your Organisation's Score: 75%

Recommendations:

A secure area normally contains assets of high value, such as IT equipment or communications conduits. It can also apply to office spaces where sensitive information is routinely handled and stored.

To prevent unauthorised access, damage and interference to such assets, various steps can be taken to reduce the risk and impact of any incidents. Examples include:

1. Physical security measures e.g. floor-to-ceiling walls, a controlled entry gate or a manned reception desk.
2. Physical entry controls e.g. authentication controls, such as swipe cards, visible identification badges, access rights based on a defined process.
3. Securing offices, rooms and facilities by, for example, locking doors and windows when rooms and buildings are left unattended or unoccupied. Other examples include installing suitable intruder detection systems, as well as storing hazardous or combustible materials at a safe distance from secure areas.

5.2 Equipment Security

Your Organisation's Score: 20%

Recommendations:

The following controls could be considered for protecting against environmental threats and hazards:

1. Equipment should be located so as to minimise unnecessary access.
2. Items requiring special protection should be isolated (see Secure Areas).
3. An organisation should consider its policy towards eating, drinking and smoking close to IT equipment.
4. Power supply protection facilities (such as UPSs) should be used to provide the orderly closedown or continuous running of critical IT facilities.
5. Equipment should be maintained in accordance with the manufacturer's specifications and instructions.
6. Only qualified, authorised personnel should carry out repairs or be permitted to service equipment.
7. Records should be kept of all suspected or actual faults and all preventative and corrective maintenance.

5.3 General Controls

Your Organisation's Score: 20%

Recommendations:

General controls are those controls that do not fit into a technical or operational category, but are thought to be simple and effective. Examples of such controls include:

1. A 'clear desk' policy designed to encourage people to place loose papers in storage when their desks are unattended. This can range from formal routines that involve safes and key management to simply locking papers in a desk drawer. However this is done, the practice can prevent real harm, including reducing fire damage (should one occur) and preventing information theft (especially by opportunists).
2. Ensuring that company property (especially valuable IT equipment) is not removed from company buildings without prior authorisation from an appropriate manager.

It would also be useful to undertake a review of products such as Devicewall in order to ensure that portable storage devices do not compromise security on the network.

6 COMMUNICATIONS & OPERATIONS MANAGEMENT

6.1 Operational Procedures & Responsibilities

Your Organisation's Score: 0%

Recommendations:

This subject covers a wide area. The objective of such controls is to help ensure the correct and secure operation of information processing facilities. In order to do this, the following areas need to be considered:

1. Operational procedures need to be documented and maintained. This will include the specification for the detailed execution of each job, including, for example, the processing and handling of information and any support contacts in the event of unexpected difficulties.
2. Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures, especially if the installation is growing in size and complexity. Once a certain size is reached, formal management responsibilities and procedures need to be in place to ensure satisfactory control of all changes to equipment, software, or procedures. When this point is reached is not easily determined. However, even smaller systems can benefit from good discipline in regard to change management.
3. Incident management procedures need to be established to ensure a quick, effective and orderly response to security incidents.
4. In many circumstances it is important that various business roles are segregated e.g. a person who raises a purchase order should not also be the person who verifies that the goods have been received.

6.2 System Planning and Acceptance

Your Organisation's Score: Not Applicable

6.3 Protection Against Malicious Software

Your Organisation's Score: 0%

Recommendations:

Precautions are required to detect and prevent the introduction of malicious software. Such protection should be based on security awareness, appropriate systems access and change management controls.

The following controls can be considered:

1. Installation and detection of anti-virus detection and repair software
2. Checking any electronic mail attachments and downloads for malicious software before use
3. A formal policy requiring compliance with software licenses
4. Checking any files on electronic media of uncertain or unauthorised origin

6.4 Housekeeping

Your Organisation's Score: 0%

Recommendations:

Good housekeeping, which involves routine procedures, is one of the most effective means of protecting information systems and the business processes that depend on them. Crucial here is the implementation of routine procedures for carrying out information backups. This normally plays a fundamental role in the maintenance of both the integrity and availability of information, and in some more severe instances, can actually provide a lifeline.

Some of the controls that should be considered include:

1. A minimum level of back-up information, together with accurate and complete records of the back-up copies.
2. The back-up information should be given an appropriate level of physical protection.
3. Back-up media should be regularly tested.
4. Restoration procedures should be regularly checked and tested.

6.5 Network Management

Your Organisation's Score: 75%

Recommendations:

If your company runs an IT network, it is, or very soon will become, an integral part of your business. Networks are technically complex, and are by their nature dispersed. This causes many problems that need focused attention. These issues increase in complexity and potential impact if the networks connect to public services, such as the Internet.

The controls used to mitigate the risks associated with networks are too many to list here. If you do not have specialist network security capability in-house, you should seek specialist assistance if you think you have a problem.

6.6 Exchanges of Information & Software

Your Organisation's Score: 0%

Recommendations:

To prevent damage to information, and to prevent interruptions to normal business activities, it is important that the information storage media (discs, CDs, even tapes in older installations) are handled correctly, and that adequate measures for the disposal of redundant media are in place.

Remember that your company information is often stored on discs that are sent out of the company for disposal or repair. You should develop measures to remove information from media and devices if you are concerned about sensitive data leaving your company's physical control.

7 ACCESS CONTROL

7.1 Business Requirements for Access Control

Your Organisation's Score: 100%, therefore no recommendations required.

7.2 User Access Management

Your Organisation's Score: 0%

Recommendations:

It is important that any access control policies are managed properly. Without ongoing management, such policies may well prove ineffective.

Ongoing management considerations:

1. Registration and de-registration of users.
2. Allocation of passwords should be controlled.
3. Users should be required to maintain their own passwords.
4. Users' access rights should be regularly reviewed.

Therefore, a User Access Management Policy needs to be implemented as soon as possible, as defined by the Security Policy Group.

7.3 User Responsibilities

Your Organisation's Score: 0%

Recommendations:

If passwords are not securely maintained or they are chosen on the basis of personal names or well-known phrases, their overall effectiveness is dramatically reduced. With this in mind, it is recommended:

1. Passwords should be of a minimum length.
2. Passwords should be changed on a regular basis.
3. Passwords should not be shared.
4. Passwords should be changed if it is thought that they may have been compromised.
5. Paper records of passwords should not be kept.
6. Passwords should be kept confidential.

7.4 Operating System Access Control

Your Organisation's Score: 0%

Recommendations:

Security facilities at the operating system level should be used to restrict access to computer resources. These facilities should ensure that:

1. The identity of the user is verified.
2. Any unsuccessful log-on attempts to the system are recorded.
3. Connection time of users is restricted, where appropriate.

Again, this provides an additional layer of security with regard to those who are able to access the system.

7.5 Application Access Control

Your Organisation's Score: 100%, therefore no recommendations required.

7.6 Mobile Computing & Teleworking

Your Organisation's Score: 50%

Recommendations:

When using mobile IT facilities, e.g. notebooks, palmtops, laptops and mobile phones, special care should be taken to ensure that business information is not compromised.

Care should be taken in public places, meeting rooms and other unprotected areas outside the company's premises. It is very easy to forget you are displaying sensitive information on your laptop. It is also very easy to read a laptop screen over someone's shoulder. This practice (known as 'shoulder-surfing') can result in embarrassing (and worse) loss of confidential information.

Mobile computing facilities should also be protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centres and meeting places.

8 SYSTEMS DEVELOPMENT & MAINTENANCE

8.1 Security Requirements of Systems

Your Organisation's Score: 0%

Recommendations:

When purchasing packaged software, security issues should be considered. This may mean that you might want to make use of independently evaluated and certified products. If this is not possible then consideration could be given to ensuring that products purchased have a documented, successful track record.

It is important to note that controls introduced at the design stage are significantly cheaper to implement and maintain than those included during or after implementation. Some research suggests that it may be 10 times cheaper!

8.2 Security in Application Systems

Your Organisation's Score: 50%

Recommendations:

Where appropriate, application controls may be required for systems that process, or have an impact on, sensitive, valuable or critical organisational assets. These controls may include:

1. Data input to application systems may need validation to ensure that it is correct and appropriate.
2. Validation checks should be incorporated into systems to detect deliberate corruption.
3. Data output from an application system should also be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

Again, the most appropriate way of ensuring that the above controls are in place could be to buy an off-the-shelf product with a proven pedigree and which guarantees that these controls are in-built.

9 BUSINESS CONTINUITY MANAGEMENT

9.1 Aspects of Business Continuity Management

Your Organisation's Score: 20%

Recommendations:

Any company, no matter the size, should have business continuity plans, whether formal or informal, in place. These plans should take account of the consequences of disasters, security failures and loss of service.

Contingency plans should be developed and implemented to ensure that processes can be restored within required timescales.

The process of developing these plans should begin by identifying events that can cause disruption to business processes, e.g. equipment failure, flood, fire. This should then be followed by a risk assessment to determine the impact of those interruptions (both in terms of damage and recovery period).

Depending on the results of this assessment, a strategy plan should be developed to determine the overall approach to BCM. To fail to do so is to invite failure.

10 COMPLIANCE

10.1 Compliance With Legal Requirements

Your Organisation's Score: 0%, therefore no recommendations required.

Recommendations:

When addressing matters regarding compliance with your legal requirements, the first crucial step is that you identify all relevant statutory, regulatory and contractual obligations for your company.

Some areas that might be relevant include:

1. Data Protection
2. Intellectual Property Rights
3. Software licensing
4. Regulation of cryptographic controls
5. Safeguarding organisational records

It is crucial that advice on specific legal requirements is sought where this is not available internally

10.2 Reviews of Security Policy & Technical Compliance

Your Organisation's Score: 0%

Recommendations:

Once you have achieved compliance, it is important that you put in place a monitoring process to ensure that you continue to comply with the relevant legislation, and with your own security policies and standards.

Areas that should be considered for review include:

1. Information Systems
2. System Providers
3. Users
4. Management

One element of this review should include the examination of operational systems to ensure that hardware and software controls have been correctly implemented. This may require external technical assistance.

An example is the use of penetration testing of your systems, which might be carried out by independent experts. This can be useful for detecting vulnerabilities in the system and for checking how effective the controls are in preventing unauthorised access due to these vulnerabilities.

10.3 System Audit Considerations

Your Organisation's Score: 100%, therefore no recommendations required.

SUMMARY

Whilst 100% security guarantees do not exist, properly weighing risks and consequences against the cost of prevention is a good place to start. Now that IT is central to most businesses, doing nothing is simply not an option.

The implementation of the international recognised security standard BS ISO/IEC 27001:2005 will provide *A Company* with a security framework to address all the areas detailed in the security report and this will encompass all the recommendations made in the report.

Once the standard has been achieved there are several key benefits available to *A Company* including an improved competitive advantage above the competitors as *A Company* will be able to demonstrate to their clients that they have achieved a world class international standard for the management and control of security within the organisation, this is especially advantageous in the Government and Public industry sectors.