INFORMATION SECURITY GUIDE FOR SMALL BUSINESSES

Published by

香港電腦保安事故協調中心
Hong Kong Computer
Emergency Response Team Coordination Centre

香港警務處 科技罪案組
Technology Crime Division
Hong Kong Police Force

政府資訊科技總監辦公室 資訊安全網
INFOSEC,
Office of the Government Chief Information Officer

2007
Third Edition

About this Guide

Objective of this guide

The "Information Security Guide for Small Business" is written by the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), the Office of the Government Chief Information Officer (OGCIO) and the Technology Crime Division, Hong Kong Police Force (HKPF) of the HKSAR Government. The objective of the guide is to provide a concise guideline to small and medium enterprise (SME) users who need to manage the information security threats everyday with limited resources.

What is covered and not covered in this guide

The guide tries to consolidate a collection of guidelines and articles available to the public into a one coordinated presentation of information security risk management. It does not intend to duplicate some existing good guidelines like the guides to personal data privacy. It does not cover home computing topics such as parental guidance and it does not intend to cover very in-depth topics like individual computer crime ordinances and very technical steps. Whenever appropriate we provide pointers to the relevant resources for the readers who would like to obtain more details.

How this guide is organized

Section 1 provides a brief overview of the information security management problem of small business in Hong Kong. Sections 2-5 are organized in a logical sequence according to the risk management model.

While you may find that it is easy to follow the sequential flow, we have also made each section an independent unit. You can go straight into individual section and should still be able to follow the points presented.

At the end of this guide you can find some useful references, including information on the Ordinances Related to Computer Crime, Useful Contacts and Useful Resources for information security. They can also be used independently.

FORMATION SECURITY GUIDE
OR SMALL BUSINESSES

Table of content

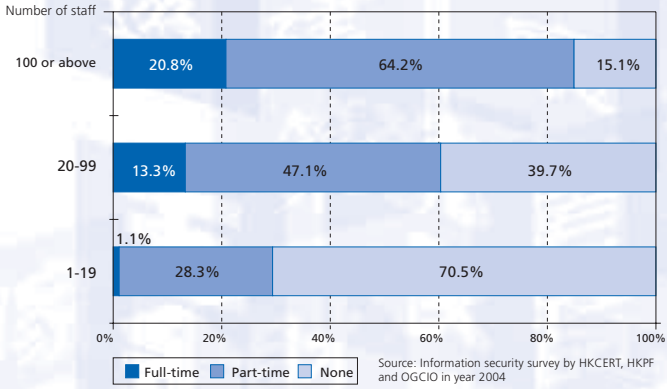
INTRODUCTION 1

1.1 Information Security Threats in Global and Local Views

Internet has changed the way people conducting business. Networked computers allow people to communicate in a much faster way and to a much broader coverage than ever. Internet has also provided a platform for new electronic commerce to flourish.

At the same time, Internet has brought about tremendous increase of information security threats. The number of HKCERT security incident reports increased from 150 in year 2001 to 1,127 in year 2006. In January 2003, the SQL Slammer worm had clogged Internet traffic flow for several days. The estimated loss in productivity in its first five days worldwide accounted to over one US$1.0 billion. But that only puts it at No. 9 position on the list of the most costly malicious code, behind the Code Red worm which cost US$2.6 billion in productivity loss. Research on the sophistication of security attack pointed out that while experienced intruders are getting smarter, it is becoming easier for novice intruders with least knowledge to duplicate known attacks with the widely available intrusion tools and exploit scripts. It is also said that more and more hackers are well organized, and focusing on money. We observed that some worms had left backdoors to those hackers, making infected machines become mailing server of junk mails. Some worms look for personal information and send them to collection websites, all of these bring "benefit" to hackers. Once hacking activities' inducement includes business concern, security risk raises.

A local survey conducted by the publishers of this guide indicated that more and more companies were willing to purchase security protection tools. On the other hand, 28.3% of the companies were still using simple protection, like anti-virus and password control. From today's point of view, these kinds of protection are not enough. It is even more surprised that about 4% of companies did not adopt any protective measures. We are more concerned about SME's information security. In the same survey, we also investigated the human resources management of information security with respect to companies' size, and presented the finding in form of chart below:



You can see that for medium size enterprises (20-99 people), only 13.3% of them have full-time staff responsible for information security. For small enterprises (1-19 people), only 1% have full-time staff. Even including the part-time staff, still only 30% of enterprises have the related position. From the view of human resources, SME's concern in information security is obviously not enough.

1.2 Information Security in Hong Kong SMEs

Life is full of risks. We have to live with the risks. If we ignore it, then we will pay the cost some day. In business environment, it could cost people their business survival. On the other hand, mitigation of risk does not come free. So it is a matter of striking the balance. Where is balance point? No one can give you an answer. A good understanding of the cost caused by the risks and the cost of mitigation the risks is a good start.

Have you got to the balance point?

What is the current information security status of SMEs in Hong Kong?

The development of small business computing systems has been more rapid than the systems to protect them.

- The Internet has now linked your computer systems to a massive international network of computers and computer users (including hackers).
- The business operations of most SMEs are now highly dependent upon the correct and continual operation of these computing systems.
- SME has only limited budget to invest in security technology to protect their business.
- SME has not got personnel with sufficient knowledge and skills to secure the networks and respond to incidents.
- The complexity of the security problem is growing very fast. New vulnerabilities and hacking techniques continually emerge. A secure system yesterday can become vulnerable today.
- There are security problems on and off, here and there. But since the company's main focus is in driving the business to generate revenue, no one has the time to think about it in a more holistic manner.
- Poor computer and network security in one organization can impact upon other organizations with consequential legal consequences, or cause contravention of Government regulation and legislation.

The following dialogues from six people A, B, C, D, E and F are common reflections of the above situation.

A : Security does not generate revenue. Why should I invest on it?	**B :** Since we do not have the expertise, we have to drop it. Sorry!	**C :** Why should I buy a $100,000 firewall to protect a $5000 PC?
D : Everyone out there is the same. Why should I care about it?	**E :** I have to bear legal liability if I were hacked? Are you kidding?	**F :** I've been infected by computer virus before. What a big deal?

A, B and C are saying that security need investment and they cannot afford.

D merely says "I do not want to be the first one" which implies that either (1) he does not consider it worth investing time to consider the problem, or (2) he sees no benefits in the investment in security so he has not put it on the priority list. In the end, D just does not want to invest anything on it. He is same as A.

So we can say that A, B, C, D are aware of the factor of "cost of mitigation".

E just does not believe that security breach of his company can lead to legal liability. He tired to consider the consequence of the security breach is not sure.

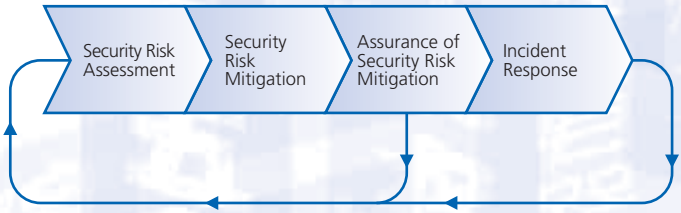
F represents a different group of people. He had experienced a security breach before and has considered the consequence. He thinks that consequence is not so serious. He is happy with the status quo, may be the risk of another virus attack.

E and F are aware of the factor of "cost of risks" or the consequence. E is not sure how great the impact is and F might have underestimated the impact of future attacks.

We do NOT conclude that these 6 people are wrong and they should buy the firewall, intrusion detection system and hire the first class security expert to solve their security problem. No! We are not concerned about their conclusion, but the process that come to this conclusion. If they have treated the consequence of security breach seriously; have done a security risk assessment as they have done for business risks; came to a conclusion that they should take their current strategy, then that is fine. However, in most situations, this is not the case. To conclude:

> Without a careful consideration of the two sides of the balance: (1) the "cost of risks" and (2) the "cost of mitigation", how can we say that we can come to a "balance point"?

1.3 Our Proposed Approach to Security Management



In this guide, we try to use a simple and systematic approach that helps you to start with risk assessment to identify the risks and the associated costs, to prioritize the risks to focus on and to select the proportional risk mitigation strategy. (see Section 2. Security Risk Assessment) Our approach does not require first class risk assessment expert to calculate special formulae but require your common sense to make judgement. It is like what you are doing with your business risk assessment. We do not propose you to buy anything but to make sense what you do or not do.

To help you to mitigate the security risks, we have provided some management and technical guidelines to help you developing your management policy and building your secure infrastructure. (see Section 3. Security Risk Mitigation)

After implementing the risk mitigation strategies, you have to ensure your investment of time, money and effort does not deteriorate. You need some ongoing mechanism to achieve this. We have some advices on the plausible approaches. (see Section 4. Assurance of Security Risk Mitigation)

After all, whether you have done enough to mitigate the risk, you still have to be prepared that security incident will strike without notice. We have provided some general steps for you to follow. (see Section 5. Incident Response)

You can jump to other sections now if you want. But we will use some pages to clarify some of the points that have been raised in the dialogue of the 6 men.

1.4 What are the Consequences of Security Breach?

People think about the $dollar$ to protect the risk but not always calculate the consequences of the risks. There are too many possible consequences to list, but they can be categorized into:

1. Loss of life or injury (more related to physical security breaches);
2. Out of business;
3. Financial Loss;
4. Legal Liability;
5. Loss of Customer;
6. Damage to Reputation;
7. Damage of Information;
8. Leakage of Information;
9. Cost of Recovery; or
10. Loss of Productivity.

Most of them eventually translate into financial loss in the long run. There is different degree of loss in the same category. For example, loss of 1-day productivity and loss of 10-day productivity are very different. In the latter case, the consequence may involve damage to reputation and loss of customer as well.

Some people encountered security breaches, loss in productivity, missed the deadline of delivery, damage the reputation. They are not aware that have paid the cost. They never calculate if they can mitigate with a strategy that can save them against future recurrences. Some may think only of the strategy of elimination (100% removal) of risk and not alternate strategies of mitigation (reduce and control). They soon drew a conclusion that elimination costs them too much and elect to do nothing.

1.4.1 Legal Liabilities as an Impact of Risk

We should not underestimate the impact of legal liabilities in managing security risks.

1.4.1.1 Compliance

There has been a mass of legislation related to computer crime, e-commerce regulations, intellectual property obligations, data protection, personal data privacy etc. These developments have implications for the management and security of computer systems and in particular on the responsibilities of management in terms of the security of these systems.

1.4.1.2 Digital Signatures

According to the Electronic Transaction Ordinance, electronic document signed with a digital signature, supported by a valid digital certificate that was issued by a Certification Authority recognized by the Hong Kong SAR Government is legally binding. If an unauthorized person gains knowledge of, or access to, the private key, corresponding to the public key contained in the digital certificate, then that person can produce documents with the company's signature.

1.4.1.3 Concept of Negligence

Company management may find that their computer or network system has caused damage to some external individual or organization because they have not taken adequate security precautions. Negligence is a 'legal cause' of damage if it directly and in natural and continuous sequence produces or contributes substantially to producing such damage, so it can reasonably be said that if not for the negligence, the loss, injury or damage would not have occurred.

1.4.1.4 Insider Actions

A company that failed to take reasonable precautions to prevent an employee from misusing company systems to break the law, or causes embarrassment or damage to external parties, could find itself embroiled in investigations and possibly legal actions.

1.4.1.5 Leakage of private or confidential information

Companies have the legal obligation to protect their computer system which contains personal data of a customer or an employee. The victim can make complaint to the Privacy Commissioner for Personal Data.

1.4.1.6 Impact of internal failures on other organizations

Computer and network systems have changed the nature of many company operations. For example Electronic Data Interchange and associated Just in Time manufacturing rely upon a chain of suppliers, to provide prompt delivery of essential components. With Just in Time schemes, the failure of a supplier to provide a timely response to a purchase order can have severe impacts upon the purchasing company, because the purchaser does not have large buffer stock levels. Hence a computer security incident could result in a failure to meet contractual obligations. Such an incident could result in legal penalties well in excess of the business impact of a loss of an order.

1.4.1.7 Unintended attacks on external parties

A security flaw in the company system may be transmitted to another organizational system via network, e.g. virus spread to external party or a compromised machine being controlled by a hacker to launch further attacks to other computer systems. The security impact could be serious that the victims claim for compensation.

1.5 More Dialogues on Information Security for SME

There are a lot of interesting dialogues on SME security. We have extracted some of them below. We hope that they could provide you insight on how to deal with your own security risks.

- Prompt 1: Security does not generate revenue. Why should I invest on it?
    - Response: Perhaps you are right, but it helps to contain risks and eventually save money. Does your life insurance generate revenue for you any way?
- Prompt 2: Security surely cost me much money. I don't have that.
- Prompt 3: My company has no expert in security. What can I do?
    - Response1: Patching server vulnerability does not require extra investment in infrastructure. Uninstall unnecessary services to minimize exposure to vulnerability does not require money. It does not require an expert to do as well.
    - Response2: Educate staff to be careful of email attachment does not cost money.
    - Response3: If you do not have the expertise, you can keep the system simple.
    - Response4: Getting updated security alert from HKCERT is free. Getting security information from the INFOSEC website of OGCIO is free. You can respond faster with the information.
    - Response5: Well, you have to spend some manpower and attention on security. This is also cost. Think about the "balance".
- Prompt 4: Why should I spend on a $100,000 firewall to protect my $5,000 PC?
    - Response1: But you need to protect your business data on that PC. If the data on it is of high value (say the loss of a product design costs $1,000,000), you should do something.
    - Response2: There are always cheaper solutions. Using the 80-20 principle, you may invest optimum amount to protect most of the risks. It is better to spend a bit of money to minimize the risk than exposed totally to great risks.
    - Response3: Security is the art of mitigating risk, not totally eliminating risk. Risk mitigation should be proportional to the risk.
- Prompt 5: I've been infected by virus. No big deal!
    - Response1: So are you so lucky next time? Have you considered worst scenario? What will you do if such scenario hits you?
    - Response2: Did you spread the virus to somebody else? Will they still be your friend or your client if you attack them one more time?
    - Response3: How much does it cost you to buy an anti-virus software license? How much loss of productivity you got last time? Have you compared the two figures? What if virus strikes you again some more times? Which costs higher?

- Prompt 6: I know nothing above security; I rely on my technical staff to do it.
    - Response1: Good, you have someone to help you, but the technical staff does not look into the risk assessment and making critical decisions. He can help you by providing daily support.
    - Response2: You are still vulnerable. Have you plan to respond to security incident in a timely manner?
    - Response3: Have you got the staff trained to do a better job in security?
- Prompt 7: I outsource my security management to my service provider. I can leave my hands free now.
    - Response1: Congratulation, you have leveraged on external expertise to help and can focus on your core business.
    - Response2: Can you make sure that you can manage their service level? Have you make sure they provide sufficient procedure to your staff to work with them? If they go, will your system lose control?
    - Response3: Ehh... your hands are free. How about your brain? Who is doing the risk management and who makes decisions when incident occurs?

Assess your Security Risk as you do for your Business.
Give Security a Fair Opportunity!

FORMATION SECURITY GUIDE
OR SMALL BUSINESSES

SECURITY RISK ASSESSMENT 2

The Steps of Risk Assessment are:

1. Identify Information Assets to be protected;
2. Identify Threats associated with the Information Assets;
3. Estimate the Business Impact of the Risks;
4. Set Priority to High Impact Risks;
5. Select the Security Mitigation Strategy that is proportional to the risk; and
6. Identify the Residue Risks to be accepted.

We will go through each step in detail.

2.1 Identify Information Assets to be Protected

2.1.1 What are Information Assets?

An information asset is the item that we need to protect in terms of information security. It may take the form of data asset or service asset.

Information assets consist of data and services.

Data Assets

Here is a list of typical data assets that small businesses possess:

- Data assets common to organizations:
  - Personnel records.
  - Accounting records and financial data.
  - Contracts and agreements.
  - Software licenses and hardware warranties.
  - Taxation records, business registration record.
  - Client contact database.
- Data assets related to specific industry:
  - Software house: program code and documentation.
  - Manufacturing: product design.
  - Travel agency: tour brochure.
  - Warehouse: inventory and scheduling.
  - Property developer: construction project status data.
  - Service provider: new products or services data and marketing plans.

Remark: a company's reputation is an asset that can be damaged by misuse of information assets or computer systems: e.g. defacement of web pages, spam, abusive or virus infected email to clients, or excessive delays in responding to email enquiries.

Service Assets

Service assets include the services delivered directly to clients using computing facilities. Typical services designed to increase productivity include:

- Payroll.
- Inventory level monitoring and reordering.
- Graphics facilities for designers.
- Maintenance scheduling.
- Cost estimation.
- Electronic funds transfer.
- Data centre network service.

There is a close relationship between data assets and services, for example the payroll service depends upon the employee data of wage rates, hours worked, etc.

2.1.2 What Qualities of Information Asset need Protection?

Information assets are easier to be damaged and misused unnoticeably than conventional tangible assets. There are three qualities associated with information assets that we have to protect: confidentiality, integrity, and availability.

- Confidentiality - knowledge of the data asset contents is not disclosed to people or systems who is not supposed to know.
- Integrity - the contents of the data asset stay as it should be and have not been modified.
- Availability - the information asset is in a form that can be used when required.

Every information asset has different combination of protection requirements on the three qualities. Some examples are listed below. An "X" in this table indicates that special attention should be paid to protecting certain categories of assets.

Information Asset Category	Quality that need protection		
	Confidentiality	Integrity	Availability
Personal data privacy	X		
Company strategic plan	X		
Intellectual property (design, art work, musical piece, etc.)	X	X	
Logistics scheduling data		X	
Stock transaction		X	
Government website		X	
Theatre online ticketing service			X
Supermarket price information			X
Data centre network service			X
Hospital patient record	X	X	X
Online transaction web service	X	X	X

Information Asset Critical Quality Table

2.1.3 How to Identify Information Assets?

1. List down the information assets by broad categories. The information assets can be classified as internal and external.

- Internal information assets : assets that belong to the company
  - o Computer and network equipment.
  - o Information assets stored on, processed by or transmitted by the equipment.
- External information assets which include:
  - o Assets that are held by the company but owned by external party, like customer personal data, domain name (for ISP hosting the domain).
  - o Assets that owned by external party but assessed by the company via network, e.g. communication line, domain name server.

2. Identify the categories that are critical from a Confidentiality, Integrity and Availability viewpoint. In other words company management should produce an Information Asset Critical Quality table.

Information Asset Category of ABC Investment Ltd.	Quality that need protection		
	Confidentiality	Integrity	Availability
Accounting record		X	
Customer database	X		
Company strategic plan	X		
ISP communication line			X
Online trade service	X	X	X

Information Asset Critical Quality Table

To summarize, the identification of information assets is no longer a purely internal affair for the company. In some cases external parties have a right to expect that internal assets be well protected.

2.2 Identify Threats Associated with the Information Assets

The list of possible threats can be very long. We try to list a few of them below.

Threats	Description
Physical Threats	Flooding, typhoons, fire, bomb attack, traffic accidents involving aircraft or large vehicles, power failure, air conditioner failure, etc. can cause considerable physical damage to a company's environment and equipment. These threats cause not only damage to physical assets but will impact upon the availability of information assets (data and services). In Hong Kong, physical damage can come from accidents inside the company or neighbouring premises. Fire, water leakage of overhead pipes and theft are particularly common while power spikes and surges are not rare.
Malicious Code Attack	Malicious code is software that attempts to subvert the confidentiality, integrity or availability of a system. It may be in the form of logic bombs, trapdoors, Trojans, viruses, worms or spyware, which are all terms used to identify malicious code. This can cause damage to data, leakage of information and loss of productivity. If you do not protect your system reasonably and spreads malicious code to other party, you might face claim for compensation.

Hacking Attack	Hacker might compromise a company's machine to crash the system, to steal information on the machine, to deface (modify) the web page on the machine, or launch attack to other computers. The consequence is multiple ways.
Denial of Service Attacks	These attacks can overflow the system capacity and make service unavailable to other users. Examples are: • Flooding a call centre hotline with automatic fax retries. • Flooding a network with excessive traffic. • Disruption of the Internet services by DoS attack DNS server. • Exhausting a FTP server hard disk with garbage files. • Downloading very large file to fill up the company leased line bandwidth.
Spamming Attack	Spamming is a common form of email misuse. This technique is similar to mass junk mail but the sender is saved the cost and effort associated with posting a mass of brochures / advertisements. • It is wasting employee time and email storage. • The company may be deliberately targeted to overload its servers.
Fraudulent website or email	The use of fake websites or spoofed emails claiming to be sent from the company which are potentially related to fraudulent activities. Common attack techniques include phishing and pharming. • Phishing refers to the usage of fraudulent or spoofed email to fool recipients into divulging personal information for the purpose of identity theft. The fraudulent email usually direct recipients to a fraudulent website that appears to be a legitimate organization. • Pharming misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning.
Computer remotely controlled to involve in illegal / criminal activities	A computer can be remotely controlled by hackers or malicious people without the knowledge or permission of the computer owner. This compromised computer, also known as a zombie, will usually be instructed to send spam or launch Distributed Denial of Service (DDoS) attack. A collection of these zombie machines is known as a "botnet". One of the most common methods is to place a malicious code (usually a trojan horse) into a compromised machine and set it waiting for instruction.
Damage due to careless staff	These are unintentional damages caused by careless staff by: • Mis-keying of data entered into files. • Accidental overwriting or deletion of files. • Unintentionally causing excessive Internet traffic or using excessive amount of disk storage. • Revealing confidential data to other employees or external parties. • Failure to observe symptoms of a security event - e.g. virus attack.

Damage caused by misbehaved staff	• Misbehaved staff conduct these using the office network:
	  • Downloading large audio or video files.
	  • Storing child pornography on company web server.
	  • Purchasing goods on Internet using company credit card.
	  • Sending out offensive email in the name of the company.
	• Consequence
	  • Incurring additional ISP charges.
	  • Bringing poor system performance.
	  • Leading to legal cases.
	  • Causing financial loss to company.

Damage due to malicious staff	Disgruntled staff can do a lot harm to the company by: • Deliberately loading or downloading of unauthorized software. • Accessing to stored data with the intention of gaining confidential information. • Intercepting confidential messages. • Modifying of stored data for fraudulent purposes. • Transmitting of message for fraudulent / malicious purposes. • Corrupting / deleting critical data. • Overloading computer and network systems to reduce performance at critical periods. • Sending offensive emails to other parties to discredit the company.
Social Engineering Attack	Employees subject to social pressures from other employees, clients, suppliers, maintenance staff, visitors, telephone callers etc. There is also a common office culture that places urgency ahead of security. Hackers soon discovered that the easiest way to learn a password was to telephone a gullible employee and trick him/her with a plausible tale. A receptionist or help desk assistant may be fooled into revealing passwords or granting access if they can be convinced: • They are speaking to someone in authority. • There is an urgent need to respond to the request.

What you need to do is to identify the threats and rate their expectancy (probability of occurrence in a year). You have to be specific about the threats impacted service.

Threat Identification is to find out which threats are the most probable

Threats	Expectancy
Fire in the office	*
Fire in the neighbouring office	**
Virus / Malicious Code Attack to office network	*****
Hacking Attack to web server	**
Denial of Service Attacks on Internet connection	**
Spamming Attack	****
Damage due to careless staff	***
Damage caused by misbehaved staff	**
Damage due to malicious staff now	*

Rating the Threat Expectancies (***** is highest, * is lowest)

Sort this list with the most probable threats at the top.

2.3 Estimate the Business Impact of the Risks

We have a list of threats with the most probable at the top of the list. Now we consider the likely consequence of that threat event on the information assets, i.e. the potential impact of the threat. The major concern is not what might happen to the computer system, but rather what might happen to the company business.

Impact analysis is to find out what hurts the business most

2.3.1 Steps to Estimate the Business Impact of the Risk

The objective of the exercise is to identify those likely threats that have the potential to cause the most damage to the business. This process involves a number of steps, for example for a physical threat:

1. Select the threat starting with those at the top of the list, i.e. the one that is most likely to occur and for which the vulnerability is not negligible.
2. Identify the items of equipment likely to be affected by the threat.
3. Identify the information assets housed in those items of equipment.
4. Identify the nature of the damage to equipment and the information assets: loss of confidentiality, integrity and availability.
5. Make a statement on the business impacts resulting from the equipment and information asset damage identified in 4.
6. Select the next threat in the list and go to 2.
7. List the "threat-impact pairs" in order of the magnitude of the impacts.

There are two important aspects of the above routine:

- Business impact statements.
- Role of current protection systems.

Business Impact Statements

- We can allocate a dollar value to the business impacts (the quantitative approach). However, forcing company managers to make artificial estimates on the cost of a business impact tends to decrease their confidence in the risk assessment outcomes. Moreover the cost of the protective measures may itself be difficult to estimate, unless such costs relate to easily quantified items such as hardware or software.
- It is suggested that the business impact statement be made in terms most meaningful to the business managers (this is the qualitative approach).

Business Impact Statement	Impact Rating
Company out of business	
Contravention of a regulation or contractual obligation	
Loss of clients to competitors	
Public embarrassment of the company	
Tender data disclosed to competitor	
Compensation of HK$1M to HK$2M	
Failure to meet an important deadline	
Loss of 5 man-day productivity	
Loss of 2 man-day productivity	

Role of the Current Protection Systems

It is common for effect of threats to be discounted on the existence of current protection systems. Hence, if a manager is asked for a business impact arising from the loss of database of client information the answer may be Nil – because we always have a backup copy of that database.

This is NOT a recommended practice in risk assessment for a number of reasons:

- The "threat-impact pair" may not be recorded for future reviews, there is no guarantee that the protective measure will always be there.
- It assumes that the protective measure is completely effective, before it has been subject to careful study.
- It will not allow for the possibility of a better protective measure being implemented.

Risk assessment is not a once and for all activity. Companies should adopt a continuous refinement approach. First go through all the phases: Risk Assessment, Risk Mitigation, Assurance of Risk Mitigation, for the most serious "threat – impact pairs"; then have further review for the remaining "threat-impact pairs".

In the first risk assessment phase the impacts should be stated assuming no protective measures. The current protective measures should be considered in the risk mitigation stage, to determine if they are the most appropriate for the identified threat - impacts.

Once the protective measures have been implemented according to the risk mitigation phase, future risk assessments should consider the residual impacts, i.e. those remaining when the protective measures are applied.

2.4 Set Priority to High Impact Risks

With the result of the business impact analysis, it is not hard to go a step forward to rate the impact and select risks of high impact to focus on (the qualitative approach also needs something to compare!). You can see that some of the business impact can be easily measured in terms of dollars while some are more intangible. The rating is not obvious for everyone. It is best to leave to the business owners who know their business best. They can use their business judgment on the priorities they would give to such statements, and estimate how much cost / time-employee effort they would be prepared to expend in order to avoid these impacts.

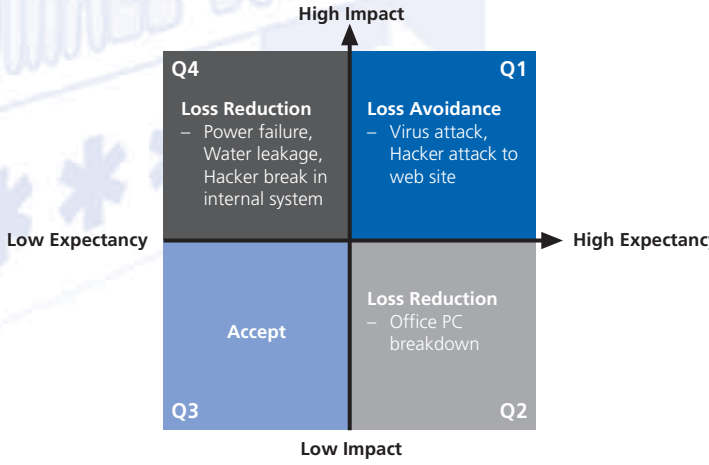
Business Impact Statement	Impact Rating
Company out of business	*****
Contravention of a regulation or contractual obligation	****
Loss of clients to competitors	***
Public embarrassment of the company	***
Tender data disclosed to competitor	***
Compensation of HK$1M to HK$2M	***
Failure to meet an important deadline	**
Loss of 5 man-day productivity	**
Loss of 2 man-day productivity	*

Rating the Business Impact (***** is highest, * is lowest)

2.5 Selecting the Risk Mitigation Strategy

Not all risks are created equal. We have to consider both the expectancy (i.e. the probability) of occurrence of a risk and also the impact of the risk associates when selecting the appropriate strategy to manage the risks. The Risk Control Matrix can help us understand the concept better. The golden rule for selecting risk mitigation strategy is "the cost of risk mitigation should never exceed the cost caused by the risk."

> The cost of risk mitigation should never exceed the cost caused by the risk.



Risk Control Matrix

Risks in quadrant Q1 are of high expectancy and high impact. In other words, they are the most critical to the survival of business. We should select "Loss Avoidance" strategies to handle them. For risks in Q2 (high expectancy and low impact) and Q4 (high impact and low expectancy), we can select a less costly approach to reduce the loss to acceptable extent but not totally eliminate the risk). For risks in Q3, we might choose to accept the risk because we do not want to spend too much for the risk.

Of course, the above is an over-simplified model only to help companies to focus on loss avoidance in Q1. You are always encouraged to adopt a strategy to reduce risks in any quadrant to minimum.

Now you have two tables: (1) Expectancy of Threats and (2) Business Impact Rating

Threats	Expectancy
xxxx	*****
xxxx	****
xxxx	****
xxxx	***
xxxx	**
xxxx	**
xxxx	*

Business Impact Statement	Impact Rating
xxxx	****
xxxx	****
xxxx	***
xxxx	***
xxxx	**
xxxx	*
xxxx	*

Try to map them and put the risks into the 4 quadrants. Then you have an idea which risks you are going to focus on.

Build a Control Cost and Effectiveness table for the critical risks you have selected to focus on to reduce, avoid or transfer the risk. Select the best mitigation strategy by justifying the cost and effectiveness of the control against the impact it incurs. Here is an example.

Risk	Control	Cost	Effectiveness
Fire & damage of equipment	– prepare standby equipment – purchase an insurance	$$$ $$	**** **
Fire & theft of contracts (hardcopy)	– rent a flat in grade-A building – store document in fireproof safe	$$$ $$	*** ***
Contract (Softcopy) being modified without authorization	– save in optical medium – store extra copy offsite	$$ $$$	*** ***
Etc.	xxx	xxx	xxx

Now you have done something to mitigate a list of risks you have identified.

We have to be prepared for security incident in any quadrant to occur. We will deal with this in "Section 5. Incident Response".

2.6 Identify the Residue Risks to be Accepted

Computer and network security protective measures mitigate but do not eliminate risk. The effect of the measure may be to:

- Reduce the magnitude of the risk, e.g. a fire extinguisher may prevent a fire from spreading.
- Reduce the probability of the risk, e.g. moving to another location may guard against damage from a minor flood, but not a major one.
- Reduce the impact of the risk, e.g. storing the more valuable documents in a fire proof safe.
- Give early warning of a risk so that preventive or remedial action can be taken, e.g. smoke detectors.
- Change the nature of the risk to one that can be more easily handled, e.g. locking a confidential file with a password converts the risk of disclosure of the file, to that of disclosure of the password.

Risk management is a continuous process. In the initial stage the major risks are identified and dealt with. In subsequent stages the protected systems should be re-considered and the residual risks and impacts identified and evaluated for further protective measures.

SECURITY RISK MITIGATION 3

After assessing the information security risks, we have to mitigate (i.e. reduce and control) the risks to contain the impacts. There are management and technical aspects in risk mitigation. We cannot exhaust all guidelines of different areas but will highlight the most essential ones in this guide.

3.1 Management Guideline

3.1.1 Security Policy

The starting point of security management is the Security Policy. The security policy documents the company direction for the security management. It should state:

- The objectives of the company in information security;
- The management framework for information security;
- The roles and responsibilities of staff related to information security;
- The strategy and priorities in the implementation of information security systems and processes; and
- The relationship with other organizations from an information security perspective.

How to make a good security policy?

The Security Policy can take any form. It can be very concise to be effective. A user should be able to answer these questions on a security policy:

- Who in the company authorize the security policy?
- Who is involved in establishing the security policy?
- Who is responsible to monitor the compliance of the policy?
- To whom is the security policy disseminated? How? How is receipt acknowledged?
- How often is the security policy updated? How are the updates disseminated and acknowledged?

What is the content of a security policy?

The table below lists the typical sections found in the security policy with their objectives. Some of the sections may be combined and given a different section name. The sections marked with asterisks (*) should be the most basic ones. The point is to make a usable policy for everyone in the company, not a comprehensive essay that no one would like to read and follow.

Section name	Objectives
* Security Policy Objective, Scope and Management process	• To define the business objective of the company, the scope and the applicability of the security policy. • To define the management process of the security policy.
* Compliance	• To ensure that staff of the company shall not contravene the legislative, regulatory, contractual and personnel obligations in performing their duties. • You can refer to “Appendix A: Ordinances related to computer crimes”.
* Personnel Security	• To ensure the staff have a clear information security and incident response responsibility in performing their job, with a procedure to handle staff violation of security policy. • To ensure the management provide user training for staff in information security.

Organizational Security	• To ensure the basic management principle of the organization information security infrastructure and third-party access is clearly defined.
Asset Classification and Risk Management	• To ensure that all staff are aware of the classification of information assets which require security precautions in terms of confidentiality, integrity and availability. • To ensure there is a proper risk assessment, risk mitigation and review process in risk management.
Physical and Environmental Security	• To ensure the company requirements on secure areas and equipment are met.
Communication and Operation Management	• To ensure that information confidentiality in data handling and exchange, system integrity against malicious software, data availability are protected in operations. • To ensure system planning & acceptance and the network management go through a management approval process. • To ensure security best practices are followed by all staff on using the Internet, email and wireless communication. • To ensure proper controls are in place on the protection against virus and malicious codes, and patch of software vulnerabilities.
Access Control	• To ensure that there is a coherent user management in access to network, system and application for office and remote users. • To ensure that proper access monitoring is in place.
System Development and Maintenance	• To ensure that research, system development, support process and cryptographic control comply with company requirements.
Business Continuity Management	• To ensure that the business continuity management and the incident response processes follow the management priority.

3.1.2 Security Management Personnel

The Security Manager should be responsible for the establishing the security policy and monitor its compliance within the company. In a small company where there is no such full time post, the function may be shared by the financial controller, technical director, or human resource manager, etc.

This security management function should report directly to the top management who is to approve the security policy to show the management commitment.

The security manager coordinates with department heads to monitor the compliance of the policy. The department heads should ensure compliance in their operation via issuing proper guidelines and procedure and monitoring.

The security manager should ensure that the security policy is communicated to the staff in an effective way and it is accessible any time. He/she is also responsible for education and security awareness of company. This can be done via the intranet, notice board, staff handbook or interactive training session.

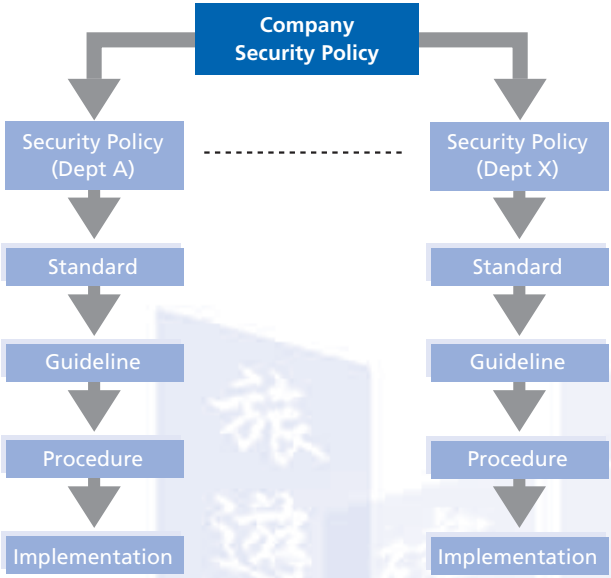
3.1.3 Security Awareness Training

Information security manager should ensure the security policy is accessible to all staff, and can be viewed at any time. He is also responsible to educate and raise security awareness among staff. These goals can be achieved through the use of intranet, notice board, staff handbook or interactive training sessions.

Security awareness training should include the following topics explicitly:

- Compliance with policy.
- Safeguarding against social engineering.
- Best practice on using the Internet and email communication.
- Handling of sensitive / personal data.

3.1.4 Implement Policy by standards, procedure and guidelines



Hierarchy in Information Security Management

Information Security Management is a top down approach to ensure that implementations at the bottom comply with the Security Policy at the top.

All the information security related standards, guidelines and procedure are derived from the security policy. Project planning and implementations should follow the standards and procedure defined. We will only select a few basic management policy documents to discuss: the Personnel Policy, the Access Control Policy and the Acceptable Use Policy.

3.1.5 Personnel Security Policy

This policy is issued by the Personnel or Human Resources Department. Several essential components in the policy are highlighted below:

- Recruitment process:
  - The applicant's supporting references should be verified before accepted.
- Roles and Responsibility in information security:
  - Staff should sign to commit the security requirements of the company.
  - It is wise to include in company properties the assigned passwords and encryption keys. All of them should be returned to the company when requested and when staff leaving the company.

- Probation or Resigned employees should be excluded from sensitive work.
- Effective communicative means should be provided to disseminate company policies to staff.
- Security awareness training should be provided to staff.
- Termination process:
  - The employee termination procedure must integrate tightly with the revocation of physical and network access to computing facilities.
  - Terminated employees' access privileges to company facilities must be revoked on or before their leaving the company.

3.1.6 Access Control Policy

This policy is usually issued by the technical department to ensure that there is a coherent user management in access to network, system and application for office and remote users. It provides the direction in designing, implementing and maintaining the infrastructure. It should consist of these points:

Identification, Authentication and Accountability in user management

- Assign separate account for each user to uniquely identify users and to hold them accountable for their actions.
- Enforce strong password policy in authentication:
  - Enforce to use password authentication or strong authentication in accessing any information system.
  - Set up the minimum password length and combination of characters.
  - Enforce change of passwords regularly and when using an assigned initial password on the first login.
- Enforce strong user authentication (e.g. token or biometrics) for critical systems.
- Enforce intruder logout and alert mechanism to prevent brute force password attacks.
- Control the sharing of user account and password.

Authorization (access control) by the principle of least privilege

- Use Role-based access control as the basis to manage authorization of access:
  - Role-based access control facilitates the "Separation of Duty".
  - It is possible to define the roles associated with the Separation of Duty rules.
  - It is easy to update the privilege of a person when a user has been transferred from one role to another.
- Implementation of role-based access control in systems:
  - Create user group profiles based on the role in the company, such as HR officer, vendor maintenance staff, senior management, backup operator and system administrator.
  - Grant access privilege of resources (printers, folders & files) to user group (the role) as agreed on by the resource owner. The set of privilege should follow the principle of least privilege.

- Individuals are granted privileges by granting membership to the user group(s). If a person is transferred from one role to another, reassign his/her group membership accordingly.
- Individual who need additional access requirement over the group's default should be authorized by management.

3.1.7 Acceptable Use Policy

This policy is issued usually by the technical department to users on the use of computing facilities within the company. It should define:

- Objective and scope of the policy.
- What a user SHOULD do:
  - User responsibility to comply with password policy, operate in a secure manner and report incidents discovered, etc.
- What a user SHOULD NOT do:
  - a list of banned activity: breaking of password, disruption of service, breaking into systems, sniffing, sharing of accounts, install / remove hardware / software from systems, disclose of company sensitive information across the network, etc.
- Authorization for exemption, if any.
- Consequence of violation.

3.2 Contingency Management

Information systems are vulnerable to a variety of disruptions, ranging from mild (e.g. short-term power outage, disk drive failure) to severe disruptions (e.g. equipment destruction, fire, natural disasters). Many of these vulnerabilities and impact may be minimized or eliminated through management, operational and technical controls. A contingency plan should be developed to enable sustained execution of mission critical business activities and information systems in the event of a disastrous disruption.

There are different types of contingency plans. The two most common ones are Business Continuity Plan and Disaster Recovery Plan. Business continuity plan focuses on sustaining an organization's critical business activities during and after a disruption, whereas disaster recovery plan provides detailed procedures to facilitate recovery of IT capabilities.

3.2.1 Business Continuity Planning

Business continuity planning involves the development of a Business Continuity Plan (BCP) to ensure the recovery of critical business activities from natural or man-made failures or disasters to an acceptable level within a predefined time frame, thereby minimizing the loss impact to the organization. Implementing a BCP is essential to every business.

Business continuity planning involves following five major processes:

3.2.1.1 Critical Business Activities Identification

It is crucial to understand where a company needs to focus on in order to recover in case of an incident. The first step in business continuity planning is to identify the most critical business activities to your company's survival. You need to have a good understanding of your business, including its objective, products, services, resources, facilities, suppliers, customers, and their interdependencies.

Critical business activities are those that must be present to sustain the continuity of business, where failing to performing them would lead to:

- Major revenue losses;
- Failure to meet regulatory or contractual requirements;
- Compromise of operational efficiency, or
- Loss of customer / damage of reputation.

Once the critical activities are identified, you should perform analysis on each of them to determine the priority and objective on the recovery of critical business activities based on their importance to the company's achievement of strategic goals. Typical questions to be considered include:

- What are the operational, financial and other competitive impacts to the company if the activities are not functioned?
- How quickly do the activities need to be back in production for your company to survive?
- How much data and financial losses can you afford?

For each of the critical business activity identified, it is also necessary to find out all the supporting resources needed to perform the activity and the effect on the business of the unavailability of the resources. Listed below are the areas of resources you should consider:

- People;
- Information technology (service, application, network, data);
- Data and voice communication;
- Paper-based documents and records;
- Physical infrastructure, key equipment and facilities; and
- External services / products dependencies.

3.2.1.2 Business Continuity Risk Assessment

A disaster could happen to any company – no matter the business size. Risk assessment on critical business activities should be conducted, identifying possible risks and assessing the likelihood and impact of disruptive events. It is vital that you understand the disruptions that would be disastrous to the running of your business. Different disaster scenarios should be considered, some common threats include:

- Natural disaster, such as earthquake, fire, typhoon, flood;
- Loss of key equipment / information system / facility;
- Disruption of external telecommunications services;
- Utility outage, such as failure of power supply;
- Loss of life, disease, health & safety issues; and
- Terrorism & cyber attack.

Risk assessment against different threats may result in different outcomes. Some may require no action, while some require continuity planning to be developed and supported with additional resources. This will help a company to explore the possible effects of disaster incidents. After that, risks can be prioritized against objectives relevant to the organization, including critical resources, impacts of disruptions, allowable outage times, and recovery priorities.

3.2.1.3 Business Continuity Plan Development

BCP allows you to prepare for the worst situation that would keep your business from being operational and to minimize service disruption as well as financial loss. The plan only needs to include the business activities that are most critical to keep your company up and running.

Based on the results from the analysis made on critical business activities and possible risks, you can start developing business continuity and recovery strategies. The selection of strategy may depend upon the criticality of business activities, cost, time for recovery and security.

Listed below are the typical items included in a BCP:

- Individual roles and responsibilities;
- Conditions for its activation;
- Processes to be followed;
- Escalation plan;

- Emergency procedure to handle incident;
- Temporary operational procedure;
- Resumption procedure;
- Fallback procedure; and
- Maintenance schedule and process for testing the plan.

For a small company, a BCP may be simply a printed manual stored safely away from main working location, with emergency contact information, location of offsite data backup storage media, copies of insurance contracts, and other critical material necessary for survival of the business.

The purchase of suitable insurance may be considered as part of the overall business continuity process to recoup losses from risks that cannot be completely prevented or controlled. The decision to obtain insurance should be based on the likelihood and degree of loss identified. Please note that insurance should not be treated as a substitute for an effective BCP since it does not deal with the recovery of business.

Before the plan is put into practice, testing should be conducted to ensure it is effective. Testing may include simulations, business process test, technical recovery and resumption testing, recovery processes testing at alternate site, supplier facilities and services testing etc.

3.2.1.4 Plan Approval and Implementation

Once a BCP is developed, it is important that endorsement should be sought for approval and support.

Points to note during the implementation of BCP:

- BCP should be documented and disseminated to all staff to follow before, during and after disruptive event occurred.
- Awareness training and education for staff should be conducted to help them understanding the business continuity processes and their individual responsibilities and actions to be taken when the plan is invoked. This is to ensure the processes would be carried out effectively.
- Copies of BCP should be stored at remote location and kept updated with the same level of security protection as at the main site.
- Other material necessary to execute the BCP and for organizational survival should also be stored at the remote location, such as offsite data backup storage media and copies of insurance contracts.
- A company may also need to have pre-arrangement with external parties to ensure timely resumption of operations, such as facilities access and telecommunication systems.

3.2.1.5 Regular Review and Ongoing Maintenance

In order to validate the business continuity arrangements, testing, review and ongoing maintenance should be conducted regularly to ensure they are up-to-date and effective.

- Regular review, testing & verification of documented BCP and the technical solutions should be conducted regularly, say annually.
- When any new or major change in business requirements / environment are identified, the existing procedures should be updated as appropriate.

- Procedures should be included within the organization's change management programme to ensure that business continuity matters are always addressed appropriately.
- BCP and the test results should also be subjected to independent audit and review.

3.2.2 Disaster Recovery Planning

Disaster recovery planning is a process to create a disaster recovery plan (DRP) for an information system for the recovery of IT processing facilities. DRP includes a well-planned document to deal with situations when a disaster occurs to an information system and/or its primary site, whereby the systems and data are totally lost.

DRP should include detailed backup procedure of the information system, the recovery procedure of the information system, say to an alternate site, and the procedure to resume data back to the primary site when the site is restored after the disaster. Refer to "Section 3.6 Backup and Recovery" for details on backup and recovery procedures.

Consideration should be given to the possibility that the primary site of the information system may not be available for a prolonged period of time after the disaster, and that the information system at the alternate site will not be run at an optimal performance level (e.g. the performance degradation may be supplemented by manual procedures). There are various means of alternate backup and processing services, such as hot / warm / cold sites subscription service run by third-party, providing different level of supporting facilities.

A detailed and well-tested procedure for data recovery and verification should be included to increase the accuracy and effectiveness of the procedure. In addition, all necessary materials and documents in recovering the data should be prepared beforehand, such as the arrangement of telecommunication network services at the alternate site.

Proper security protection should also be put in place and incorporated in the DRP. Security best practices should be followed and not ignored so that security level could be maintained after the recovery process (e.g. check and avoid restoring from unauthorized backup media which may contain malicious code). Security areas to ponder include perimeter defense, intrusion detection system, virus protection, system patching and configurations.

Similar to BCP, DRP should be maintained with updated information, especially when there are changes to the information system. Scheduled disaster recovery drill should be performed to test for the accuracy and effectiveness of DRP. But since carrying out a disaster recovery can be time-consuming and may affect normal operations, the frequency of conducting drills would be determined according to business environment and needs.

3.3 Building a Secure Physical Site

Objective: To ensure the security of human life and the information processing facilities.

Physical security deals with the environmental security controls and the physical access control of the information processing facilities. In all cases, human life is the top priority concern in mitigation of physical security risks.

Human life is the top priority concern in mitigation of physical security risks.

3.3.1 Environmental Security Controls

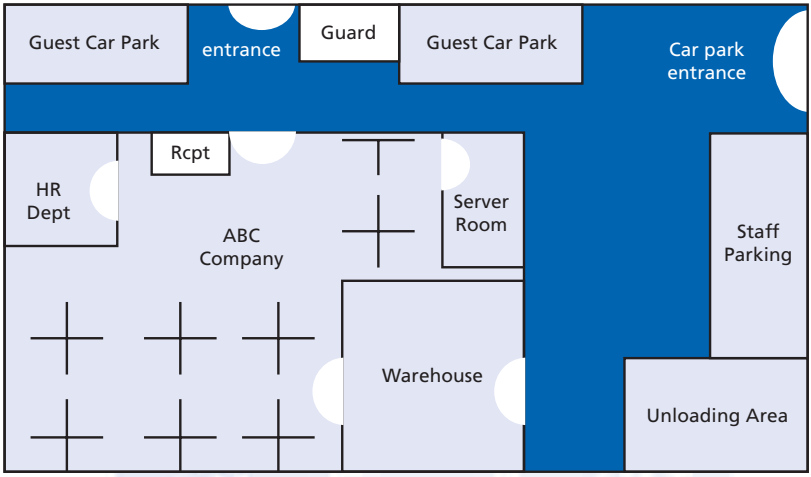
Item	Risks and Mitigation
Water	Risks • Water can cause disastrous damage to computing facilities. It may come from raining, flooding, water leakage or spilling. Mitigation • Protect computing facilities in water-proof enclosure with roof and shielding. • Build the server room on raised floor. Do not build server room on ground floor and basement. • Use data centre with dry pipe or FM200 fire suppression system.
Fire	Risks • Heat, smoke and fire suppression agent (water, extinguisher) might cause disastrous damage the computing facilities. Fire is also hazardous to human life. Mitigation • Assign fire wardens and conduct regular fire drill. • Install smoke detectors near equipment. • Keep fire extinguishers near equipment and train employees in their proper use. • Store data backup tapes in fire-proof safe. • Use data centre with dry pipe or FM200 fire suppression system.
Temperature and Humidity	Risks • Computing facilities have a controlled working environment in terms of temperature, humidity and dust density. Mitigation • Put computing facility in dedicated room with 24-hour air conditioning. • Avoid congesting machines in a small space. • Use data centre with Heating, Ventilating, Air Conditioning (HVAC) facilities. • Monitor the working temperatures and humidity versus the specifications (e.g. 10-25°C temperature, 20-70% humidity).
Power	Risks • Electrical power might suffer from spikes or surges. The momentarily instability can cause computing facilities to malfunction. • Electricity disruption can cause your system out of service. Mitigation • Install in-house uninterruptible power supply (UPS) with line filters to critical computing facilities. Remember to replace UPS batteries when they reach the expiry date. • Host critical system in data center with redundant UPS system and diesel generator.
Others	Risks • Your neighbour might cause you problem. Mitigation Investigate the business of neighbours during site selection. This is especially important for data centre site selection. The production process, the product, the transport of equipment might cause you external risks.

3.3.2 Physical Access Control

Physical access control prevents risks of damages and thefts to data and computing facilities. The physical premise perimeter security design is the starting point. The following illustration demonstrates the design considerations:

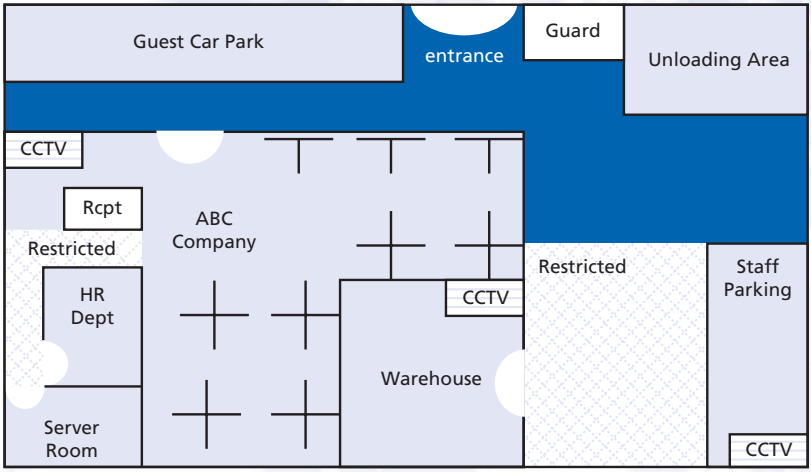
An example to illustrate good design of secure physical perimeter

Floor plan 1 shows a draft premise design of ABC Company. Can you cite the security threats of this design?



Floor Plan 1

Floor plan 2 shows an improved design. Let us illustrate some design criteria of physical security by comparing the two floor plans.



Floor Plan 2

Design Criteria	Improvements in Floor Plan 2
Minimize the number of entry points	• The human entrance and car park entrance have been merged to one, situated next to the guard post. Guards can focus on one entrance. • The back door from the warehouse to the office is removed. • The access path to the HR Dept. office and the Server Room is tunnelled to a narrow passage.
Segregate premise into zones according to security levels	• Guest parking area and the Unloading zone are moved to the outer zone. • Staff parking area is located in the inner zone. • Restricted area set up outside the warehouse. (Clear warning is posted!) • Restricted Zone set up in the office for HR Dept. office and Server Room to guard against visitors and unauthorized staff.
Deploy multiple layers of defense of different technologies and process	• Access to sensitive area need to go through several layers of defense, composed of doors, human monitoring and intrusion detection device (CCTV). • Further defense layer can be added to protect the secure area of HR Dept. and Server Room. For example, access token reader can be effective to guard against unauthorized visitors and staff.
Monitor and Log the traffic	• The guard post has been moved to a location that can oversee all the outdoor areas. • The reception desk is place in front of the HR department and server room to monitor the traffic. • CCTVs are installed to monitor the activities inside and outside the warehouse. • CCTV is installed at the reception area to monitor the traffic through the office entrance and the passage to the secure area of HR Dept. office and Server Room.
Human Escort to secure area	• Access to secure area shall be guarded by human escort: o A visitor truck can only enter the restricted area outside the warehouse to load cargo if escorted by responsible company personnel. o An internal staff can only enter the Server Room when escorted by responsible company personnel.

Good design in physical access controls

- Maintaining a simple perimeter and minimizing the number of entry points.
- Deploy more layers of defense to protection.
- Enforce identification by:
  - o Requiring all staff and visitors to wear a badge.
  - o Use staff access card to make staff accountable for his/her activity.
- Enforce strong authentication in secure areas, such as using access token with password.
- Apply the principle of minimum privilege: only responsible personnel can access the required asset.
- Build up human control which is a very effective defense measure:
  - o Educate staff to be aware of strangers passing by in the office.
  - o Security guard and sign-in process can be applied to critical premise or computing facilities.
  - o Visitor's activity in secure areas can be monitored by escorting personnel.

The fewer people can access the computing facilities, the less vulnerable they are.

- Protect the keys and pass codes for access and enforce policy to control the sharing of keys and pass codes.
- Detect intrusion of sensitive areas by installing CCTV and motion sensor & alarm. Record the activity for reference.
- Integrate tightly the revocation of access by terminated staff into Personnel Department employee exit procedure.

Advices on protection against Theft

Theft can cause the loss of valuable asset / data and leakage of valuable information. The consequence can be disastrous. To mitigate the risks:

- A complete record of all critical information assets must be maintained.
- An asset loss reporting system must be developed as part of the incident response.

Item	Risks and Mitigation
Theft of asset away from the office	**Risks:** loss of Asset and Data Mitigation • All equipment must be labelled and identified. Strong labelled like engraving is effective. • Do not store sensitive data in removable media or device. • Back up sensitive data regularly. • Secure sensitive equipment in locked room or cabinet. • Develop "Outgoing equipment approval procedure" and require all staff to follow.
Theft of mobile devices	**Risks:** loss of Asset and Data Mitigation • Assign mobile device to accountable persons. • Do not store sensitive data in PDA. • Do not store sensitive data in notebook computer hard disk. If it is required, use encryption technologies. Store the data encrypted in removable media and store it in safe place. • Back up sensitive data regularly. • Install secure operating system that requires authentication. If possible, use hardware token solution to lock the machine. • Turn off "remember" password and "auto-complete forms" features.
Theft of asset on transport	**Risk:** loss of backup tape and data Mitigation • Off-site media storage must be kept in physically secure site and locked. • Transport of media must be secured.
Theft of data via disposed items	**Risk:** information leakage Mitigation • Develop the data disposal procedure that includes: o Shred paper document before disposal. o Erase hard disk and removable media before disposal. For critical data storage device, degauss or physically destroyed the device completely.

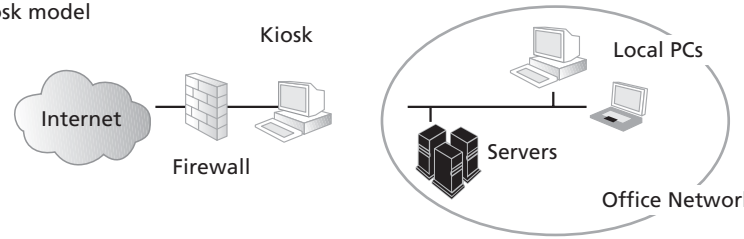
3.4 Building a Secure Network

The office network provides the core services to the company. Everyone utilize this shared medium to do productive work, including file sharing, printing, emailing and web browsing. The following are the steps to build a secure network. (Note that we inevitably include some technical information. If you find difficulty in understanding that portion, you can consult the technical staff.)

3.4.1 Building a Secure Office Network

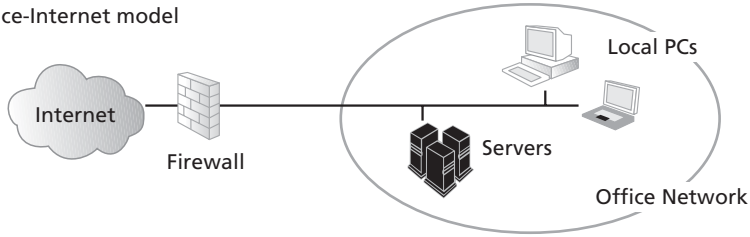
1. Put security into your network planning
   - Address all security issues in the deployment, including the management policy, technical training and outsourcing requirements.
   - Address security requirements when selecting network and server. For example, you should not select the server which is known to have many security holes, although you may be familiar with building application on it.
2. Design physical and environmental security for the network and systems
   - Put critical assets in locked rooms or cabinets. They include network communication lines, routers, switches, firewall, and file servers. Printers of sensitive departments should be located in the department's enclosed room or next to the user.
   - Enforce policy to ban network media access by visitors.
3. Use private IP addressing scheme for internal networks.
   - This will prevent internal network from access by external network. Use public IP addresses only for public accessible servers.
4. Design the network security model by zoning (segregation of network according to security levels)
   - Choose from one of these four Internet access models:
     (1) Kiosk model
     (2) Office-Internet model
     (3) Office-DMZ-Internet model
     (4) Office-MultiDMZ-Internet model

(1) Kiosk model



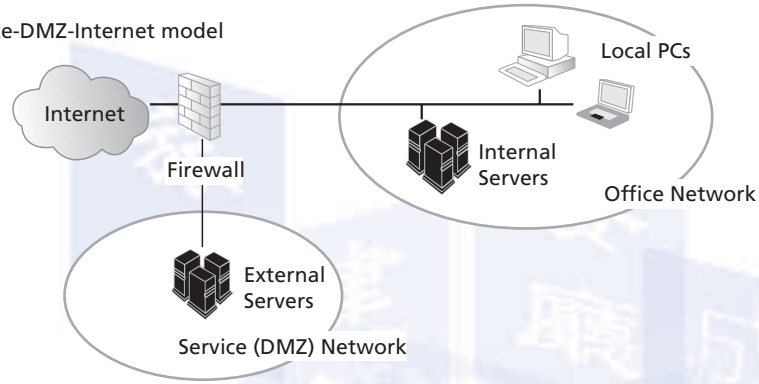
- In this model, a dedicated kiosk PC is connected to the Internet. The office network is totally isolated from the Internet. People have to go to the kiosk physically to access Internet.
- It is the most secure model because the office network is free of attacks from the Internet. However, its productivity is also the lowest.

(2) Office-Internet model



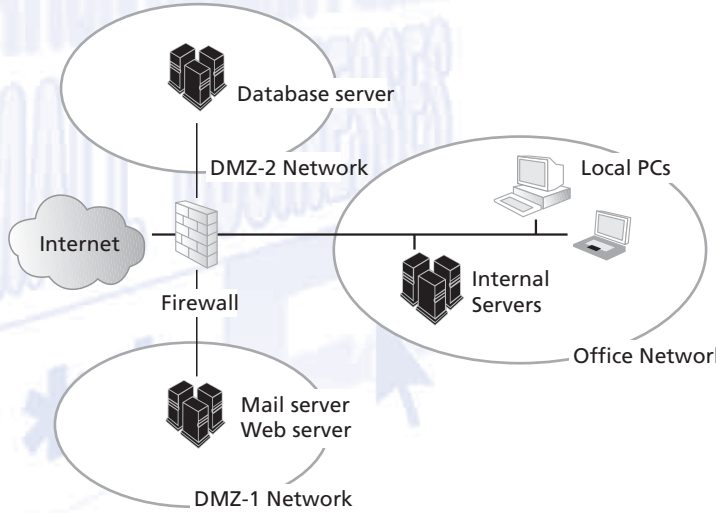
- In this model, the company servers and computers are located behind the firewall which guards against attacks from the Internet.
- Security risk exists when a publicly accessible server has a vulnerability that is exploited by the hacker, the hacker may get access to the office network.
- This model is useful when the company email server is hosted at the ISP and there is no public accessible server in the office

(3) Office-DMZ-Internet model



- This model is similar to the Office-Internet model except that a Service (DMZ) Network (or the demilitarized zone) is added. The company servers are divided into 2 groups with the publicly accessible servers put in the DMZ network.
- If the external server is compromised, only servers in the DMZ network are exposed. The office network stays safe.
- This model is useful when the company need to host her own email server and web server.

(4) Office-MultiDMZ-Internet model



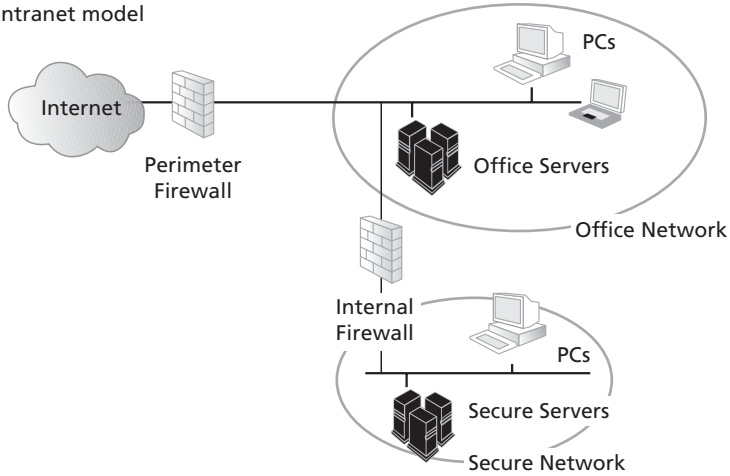
- This model is an extension of the Office-DMZ-Internet model, with more than one DMZ networks. The public servers are further divided into 2 groups, each of which sits in a separate DMZ network.
- Servers (mail and web) in DMZ-1 network are accessed by public. Database server in DMZ-2 serves data for the web server and is not directly accessed by the public. If the mail or web server is compromised, the Database server is still safe.
- This model is useful when the company need to host her web server with data server and wants to protect the database server from Internet attack.

Variations of network infrastructures can be derived from the network models above.

> Note:
>
> If you have selected the Office-MultiDMZ-Internet model or its variations, please also refer to "Section 3.4.2 Building a Secure Internet Site" for more information.

- Determine the internal access network model. Select from one of the models:
  - o Simple intranet model – it consists of a single office network.
  - o Layered intranet model – it consists of multiple internal networks of different security levels. The networks are connected by internal firewall(s) which control the flow of traffic.

Layered intranet model



- Based on the selected models for Internet access and intranet access, design and extend the network architecture. Put the servers and computers into the corresponding zones.

5. Configure the firewalls and network routers for better security
   - Firewall is an essential component of your perimeter protection. Working with a secured router can block most of the external attacks. To make it effective, it must be your only entry point of external traffic. If you have multiple entry points, each of them must be guarded similarly.
   - The firewall and routers should be hardened by:
     - o Limiting the installed services.
     - o Encrypting the administrative password.
   - Ensure the administrative access are secure:
     - o Limiting the administrative access to specified locations.
     - o Using encrypted communication channel (e.g. SSH) for administration.
   - Define the firewall rules for each network interface:
     - o Close unnecessary network services for incoming traffic. This prevents hackers from making use of vulnerabilities in existing services that you do not need.
     - o Close unnecessary network services for outgoing traffic.
   - Use network switch instead of hubs in connecting up the systems. Switches are less prone to sniffing attack.

Technical reference on securing firewall and router can be found below:

Firewall & Perimeter Protection:	http://www.sans.org/reading_room/whitepapers/firewalls/
Cisco router hardening:	http://www.sans.org/reading_room/whitepapers/firewalls/794.php?portal=6db7a7ffa450ec4d4abec1821c87b586

6. Configuring the servers for better security
    - Secure the server operating system. The common techniques including: uninstall unnecessary services and software, patch the system timely, change default administrator user ID and password, disable unused accounts and apply strong password policy.

Technical reference on system hardening can be found below:

Windows 2000:
http://www.microsoft.com/technet/security/prodtech/windows2000/win2khg/01intro.mspx

Unix: http://www.cert.org/tech_tips/unix_security_checklist2.0.html

Linux: http://www.bastille-linux.org
http://www.linux-mag.com/2002-09/guru_01.html
http://www.linux-mag.com/2002-10/guru_01.html
http://www.linux-mag.com/2002-11/guru_01.html

7. Secure the application (refer to "Section 3.4.2 Building a Secure Internet Site")
8. Filter virus and malicious code
    - Deploy anti-virus solution at gateway and desktop (refer to "Section 3.6 Virus Prevention").
9. Log security events and review regularly (refer to "Section 4. Assurance of Security Risk Mitigation")
10. Develop a standard build of secure desktop
    - If you consider it can save your effort, develop a secured workstation configuration as the standard build of the company. Make image backup of the build and replicate to the company desktops.
11. Develop backup and recovery strategies (refer to "Section 3.7 Backup and Recovery")
12. Develop the security management procedure
    For example patch management, security log monitoring, change management, etc.
13. Maintain good documentation of configuration and procedure
    Because of the complexity of this section, several sub-sections should be referenced for other aspects of office network:
    - 3.4.2 Building a Secure Internet Site
    - 3.4.3 Building a Secure Wireless LAN
    - 3.4.4 Building a Secure Remote Access & VPN

Useful links for Building a Secure Network

CERT Technical Tips: http://www.cert.org/tech_tips/

SANS Reading Room: http://www.sans.org/rr/

National Institute of Standards and Technology Publications, FBI, USA:
http://csrc.nist.gov/publications/nistpubs/

3.4.2 Building a Secure Internet Site

Approaches to Reduce Risks of providing Internet service

When the company elects to provide Internet services, there are accompanying security risks. To manage the security risks, a company has two approaches:

(1) Transfer part of the risks to service provider
- Host the whole public access server at ISP.
- Outsource part or all of the design, implementation and maintenance function to the third-party service provider.

(2) Build up the capability to manage the risks

If you choose Option 1, it is essential to put in the contract clear terms to manage the quality and response time of the service provider, and make sure the service provider able to deliver a secure network service to you. This section can be a useful reference. If you choose Option 2, you have to build your own network and this section is a must-read for you.

Steps to Build a Secure Internet Site

All the steps in "Section 3.4.1 Building a Secure Office Network" are applicable to building a secure Internet site. Here are some additional notes:

1. Provide secure and trusted channel for online business
   - If you launch business with transactions on web, make sure you provide a secure web page. You can use the widely available Secure Socket Layer (SSL) technology to encrypt the communication.
   - You should use digital certificate from a trusted certificate authority on your SSL web pages. The digital certificate signed by the trusted certificate authority verifies your site's identity.
2. Secure the application
   - All the network security defenses you have built are necessary but not sufficient to guard against hacking activities. The hackers can make use of valid network traffic to attack the vulnerabilities of Internet applications.
   - Nearly every application service on the Internet is vulnerable: the web server (e.g. Apache and Microsoft IIS), DNS server (e.g. BIND, Microsoft DNS), FTP server (e.g. wuFTPD), SMTP server (e.g. sendmail) and SQL server (e.g. mySQL, Microsoft SQL server), etc. They all have track records of being hunted down by hackers exploiting known vulnerabilities.

Technical reference on application and database security can be found below:

Application and Database Security:
http://www.sans.org/reading_room/whitepapers/application/

Top Twenty Security Threats:
http://www.sans.org/top20/

- The application can be secured by several means:
  - o Installing security patch.
  - o Hardening the configuration of the applications.
  - o Jail the environments that the applications run on. This means running the application with a least privilege account on a restricted environment. Even when the service is exploited, the hacker cannot gain administrator access. This is called "chroot" in Unix / Linux platform.

Technical reference on CHROOT can be found below:

Chroot for all services: http://en.tldp.org/linuxfocus/English/Archives/lf-2002_01-0225.pdf
Chroot for BIND DNS: http://www.linuxsecurity.com/docs/LDP/Chroot-BIND-HOWTO.html

3. Review the codes and script of your website
   - Besides the application installed on the server, you might have developed client side script and server side programs in your web pages. Review these codes to make sure that the inputs are validated in terms of boundary and content (to avoid problems like buffer overflow and code injection). Make sure that input forms in secured web pages do not submit to insecure websites.

Technical reference on secure coding can be found below:

http://www.sans.org/reading_room/whitepapers/securecode/

4. Separate your internal servers with external service
   - You may run your email, domain name and web services for both internal staff and external customers. If possible, separate them into different machines and put them in different network zones.
5. Apply more layers of firewall when necessary
   - We can deploy 2 or more layers of firewall for better protection of the internal network and the service network. A hacker successfully compromised the first firewall cannot get full access to the innermost layer of the network.
   - It is recommended to use a mix of technologies in firewall, e.g. packet filtering firewall and proxy firewall to provide a more comprehensive protection.
6. Develop intrusion detection strategies
   - Apart from protection, you need to detect attacks before they can go through the firewall. Network-based intrusion detection system provides a very good way to track attacks on the network, whether it targets a host in your service network or not.
   - Host-based intrusion detection systems can detect attacks targeting at the server and track unauthorized modification to system files.
7. Assess the security of your service provider
   - It is inevitable that part of your Internet infrastructure is provided by the service provider, e.g. the Internet connection, the router, the domain name server, the mail host. Their weak links in security might impact you.
8. Prepare for incident response to attack (refer to "Section 5. Incident Response".)

3.4.3 Building a Secure Wireless LAN

Wireless LAN (WLAN) has several security problems:

- Lacking physical security of wired network.
- Having insecure the default settings in the WLAN devices.
- The current 802.11b technology is not secure enough. There is no authentication mechanism and its encryption protocol, the Wired Equivalent Privacy (WEP) protocol has security flaw.
- Lastly, some people deploy them for serious and sensitive network.

Steps to build a secure business use of WLAN

1. Risk Assessment
   - You have to assess the risk of WLAN before taking it as an option for sensitive and serious services. Put in your budget the extra cost of management and security strategies in WLAN security protection before deploying WLAN.
2. Management Policy
   - Prohibit staff from building their own access point within the company
   - Enforce policy on staff responsibility in protection of security configurations such as password, SSID, WEP key.
   - Educate user the legal and ethical responsibility of unauthorized access, disallowing them to connect to other party's wireless networks.
3. Planning
   - Use upgradeable solution. When choosing a WLAN solution, ensure the access point (AP) and wireless card can update the firmware.
   - Wi-Fi Protected Access (WPA) and WPA2 standards have been released that provide stronger authentication and encryption technology. You should consider your implementation in the most cost-effective way.
   - Choose technology that helps you centrally manage your security, e.g. automated distribution and update of encryption key, integration with company's existing authentication system.
4. Designing and Implementation
   - Secure the access point physically
     - Do not put the WLAN AP close to window or door.
     - Power-off when the access point not in use.
   - Secure the network perimeter
     - Treat WLAN as untrusted network. Segment wireless traffic in a separate network. Install a properly configured firewall between the wired infrastructure and the wireless network to manage traffic going into the internal network or service network.
   - Apply network security control
     - Use static IP address (turn off DHCP) on wireless LAN client. Client without valid IP address cannot connect.
     - Connect AP to network switch (instead of hub) to avoid network sniffing
     - Control access by Media Access Control (MAC) address filtering to permit connection to authorized WLAN card filter. This is effective if the list of WLAN cards is manageable.
     - Use other form of authentication to require user to authenticate before use the WLAN (e.g. RADIUS and Kerberos are available in certain products).

- Encrypt network communication on WLAN
  - Turn on WPA / WPA2 encryption. The longer the pre-shared key length, the better.
  - Change the pre-shared key periodically to further improve the security over time.
  - For serious application, use Virtual Private Network (VPN) technology on top of WPA / WPA2 to encrypt wireless communications.
- Securing SSID
  - If possible, turn off SSID broadcast (some AP manager GUIs provide such function, sometimes called "closed network"). You need to tell individual users the SSID.
- Secure SNMP configuration
  - If your AP is using SNMP administration, enable the SNMP access control list (ACL) to control who can administer the AP.
  - For security over time, change the SNMP community string periodically.
- Secure the default configuration
  - Change the default SSID to something else for your network.
  - Change the default administrator user ID and password to a strong one.
  - If your AP is configured using SNMP, make sure you change the default SNMP name and community string. Use a longer SNMP community string with mix of numerals and alphabets.
- Test your AP broadcasting in the neighborhood.

5. Review and Audit
   - Check periodically if any rogue AP is set up within your company or at your company's neighborhood.

Free tools are available for auditing wireless access point security

Netstumbler for Windows (http://www.netstumbler.com)
KISMET for Linux (http://www.kismetwireless.net)

3.4.4 Building a Secure Remote Access & VPN

Remote access provides the possibility for mobile workforce to do productivity work and system administrators to support the office network after office hour.

However, remote accesses touch down to the heart of company internal network and can bring about serious security issues. It must be carefully planned.

Rules to deployment of Remote Access

1. Restrict the usage by strict management control. Authorization is only granted by management with sound justification.
2. Enforce with sound technical solution in authentication and authorization to protect the confidentiality, integrity of information.

Providing remote access to internal network poses several technical challenges to security:

- How to authenticate the user?
- How to authenticate the destination system?
- How to ensure the confidentiality of the communication?
- How to ensure the integrity of the communication?

Traditional remote access via dial-up to remote access server can hardly answer to these challenges. Furthermore the cost for oversea dialup is high. VPN technology tries to provide answer to all these issues. VPN can be roughly divided into IPSec VPN and SSL VPN.

Benefits of Remote Virtual Private Network

- The VPN technology can build encrypted tunnel through the insecure Internet network to protect information confidentiality.
- If properly configured, the sender and receiver ends address cannot be spoofed (authentication).
- If certificate is used the communication's integrity can be assured.
- Remote VPN can be configured to use private IP addresses of the destination system, thus provide a layer of network security.

Security Issues of Remote VPN and Mitigation

Remote VPN is not problem-free.

- Firstly, VPN protects the information traveling between the laptop and the VPN gateway. It does not protect the laptop from attack. If a laptop is infected by a virus / malicious code, or fall into controlled to a hacker, it can be used to launch attack to the internal network once the VPN is connected. We recommend to:
  - o Enforce installation of personal firewall, anti-virus and anti-spyware solution on the laptop.
  - o (If the VPN gateway support such feature) check the integrity of the laptop software, such as the security patch level of the mail client and browser before granting it access to the network.
- The configuration of the VPN is so flexible that in some case the VPN is not so secure. For example, use of shared secret can open door for hackers who obtain the shared secret by social engineering or from an ex-staff of the company. We recommend using digital certificate to authenticate both the laptop and the VPN gateway.
- Revocation of digital certificates for VPN access of ex-staff should be tied tightly with the personnel staff exit procedure.
- The VPN client configuration should force the user to login before making a connection.
- Enforce access control at the VPN gateway to allow least privilege.
- If a user accesses an internal server via VPN through the Internet, the encrypted tunnel is set up between the laptop and the VPN gateway. The communication from the VPN gateway to the internal server is not encrypted.

More information about IPSec VPN and SSL VPN

Comparison of technology between IPSec VPN and SSL VPN

http://www.slb.com/media/services/software/whitepaper/whitepaper_vpnsra.pdf

3.5 Securing User Internet Access

There are many questions people are asking about Securing User Internet Access. We share some of them below.

1. How to protect my machine from Internet attacks?
   - First and most important, be careful not to introduce malicious code by yourself:
     - o Do not install unsolicited software in your computer, from CDROM or downloaded from Internet.
     - o Do not open suspicious email attachment.
   - Use a PC operating system that requires user login and use strong password. This guards against unauthorized party from accessing your computer and install unsolicited software.
   - Update the security patch of the operating system, Internet browser, mail client and other applications:
     - o Turn on Windows Update and use Microsoft Baseline Security Analyzer.
   - Protect the PC from hacking and scanning:
     - o Install personal firewall and apply filtering on outgoing traffic.
   - Protect your PC from virus and malicious code:
     - o Install anti-virus software and apply the latest virus signature regularly (refer to "Section 3.6 Virus Protection").
   - Protect the PC from spyware:
     - o Read policy of website before download software. Check the digital certificate of downloaded software to verify the source.
     - o Install anti-spyware software and apply the latest definition file.
   - Do not let your PC turned on and connecting to the Internet when you are away.

What Strong Password IS and IS NOT	Free and Useful Tools for protecting your PC
IS NOT: • A word in the dictionary or reverse of a word. • Related directly to the person's information. • Something you share with others. • Same for all system. IS: • A mix of alphanumeric and symbols. • Long enough (minimum length 8 characters). • Something that you can remember easily and others not. • Different for use in situations of different criticality.	• ZoneAlarm personal firewall (http://www.zonelabs.com) • AVG antivirus software (http://www.grisoft.com) • Ad-Aware spyware scanner (http://www.lavasoftusa.com) There are limitations in features of free tools. There are terms & conditions apply in using these free tools. Note that commercial software with support service is available.

2. How to protect your personal data on the computer being captured by website?
   - Read the Privacy and Personal Information Policy of the website.
   - Do not save password on hard disk.
   - Turn off Auto Complete feature of Forms (In Internet Explorer, choose Tools l Internet Options l Content, click "AutoComplete..." button).
   - Configure Cookie settings to suit your need (In Internet Explorer, choose Tools l Internet Options l Privacy).

- Delete Temporary Internet Files after browser is closed (In Internet Explorer, choose Tools l Internet Options l Advanced).
- Clear the cache and history after you use a public Internet kiosk.
- Do not enter personal information on public Internet kiosk.

3. How to avoid personal data being used by others without my consent?
   - Protect your personal data on the computer (read #2).
   - Read the rules, terms and conditions before subscription.
   - Do not reveal personal details when joining chat room and mailing list.
   - Use a separate email address to subscribe mailing list or newsletter.
4. How to handle email spamming?
   - Avoid your personal data being used by others without your consent (read #3).
   - Do not reply to a spam. This does not stop spamming. Besides many spammers use a fake email address.
   - Use a separate email address to subscribe mailing list or newsletter.
   - Use spam filter to filter out spam emails.
   - Report spamming to the ISP. ISPs usually has an email account to handle these abuse case, in the format "abuse@ispnamehere.com".
   - Report to HKCERT for assistance.
   - Refer to the FAQ of Commerce and Economic Development Bureau (CEDB) for help.
5. How to protect your communication confidentiality?
   - If you are browsing on the web, use SSL encrypted pages to encrypt data sent to the web server.
   - If you are using email, use PGP or S/MIME to encrypt the message with the receiver's public key. Only the receiver with the private key can decrypt the message. If you want to receive confidential email, generate your public / private key pair from PGP software or subscribe a personal certificate from a trusted certificate authority (CA).
     - o Note that the PGP has both commercial and free editions. Check the terms and conditions apply for using the free edition.
     - o If you use a personal certificate provided by a trusted CA, make sure your mail client support the use of certificates.
   - If you are accessing your office network for file sharing and emailing, make sure VPN is used.
6. How to do safe on-line purchase?
   (Reference: SafetyNet Guide, Asia Oceania Electronic Marketplace Association)
   - Deal with a site that you trust. You can also verify the merchant's physical address, phone and fax no.
   - Never give out personal information or credit card information easily.
   - Read and understand the Data Privacy Policy of the site. Notice that you should be given choice to allow the company to use your personal information or not.
   - Ensure the transaction takes place over secure channel. Use stronger encryption when

possible (128-bit SSL is stronger than 40-bit SSL). Check that the digital certificate is issued by a trusted certificate authority and is not expired.

- Before making a decision to purchase:
  - o Read and understand the product terms and conditions of warranty.
  - o Check the refund and return policy.
  - o Make sure the above terms and policy applicable to your countries / regions.
- Before clicking the Send button to purchase:
  - o Check the order details, the shipping address.
  - o Verify the amount of purchase with your own calculator. Mind the foreign currency exchange rate.
- Always turn off remember password function.
- Save a copy of the transaction or print the web page that include the transaction detail and order number for future reference.
- Monitor your credit card transaction record for the rest of the days. If there is anomaly, stop the credit card and call for investigation.
- Lowering the credit limit to reduce the risk of credit card fraud.

7. Am I free to use the information found on the Internet, share file and music on the Internet?

- We have to respect the creativity and innovation of others. The copyright of the information posted on the Internet belongs to the author. You have to get prior approval before using it for any other purpose.
- File, music and other pieces of work enjoys the same protection of copyright as in published in other medium.
- The making available of copies of copyright works via the Internet as acts restricted by copyright is an offense. Beware that heavy penalty is imposed on infringement of intellectual property right. Refer to "Appendix A: Ordinances Related to Computer Crime" for more information.

Useful links for Securing User Internet Access

Anti-spam , Office of the Government Chief Information Officer
http://www.antispam.gov.hk/

Anti-SPAM - Code of Practice, Hong Kong Internet Services Provider Association
http://www.hkispa.org.hk/antispam/cop.html

Intellectual Property Department
http://www.ipd.gov.hk/

Hong Kong Post e-Cert
http://www.hongkongpost.gov.hk/

Internet Banking – Keeping your money safe, The Hong Kong Associations of Banks
http://www.hkab.org.hk/PDF/customer_info/ebanking_e.pdf

SafetyNet Guide, Asia Oceania Electronic Marketplace Association
http://www.aoema.org/

The International PGP Home Page
http://www.pgpi.org/

3.6 Virus Prevention

Virus and malicious code attacks are flooding the Internet. A company must be able to deal with these attacks to protect from losses. Prevention is better than Cure. This section gives guideline to virus / malicious code prevention.

Prevention is better than Cure.

"Section 3.7 Backup and Recovery" and "Section 5 Incident Response" contains useful references to complement this guideline.

3.6.1 Deploy Strong Technical Solution of Protection and Detection

- Deploy protection and detection tools
  - o Install anti-virus solution at the Internet email gateway and file server
  - o Install anti-virus solution to filter other traffic that is prone to transport virus, e.g. web browsing and FTP access, if possible.
  - o Install and maintain anti-virus and anti-spyware solution at desktop / notebook to detect and prevent virus/malicious code. Turn on Real-time protection.
- Manage the protection and detection tools
  - o Keep your virus / spyware signature (also called definition file) updated daily before the start of the office hour. We recommend automating the update process.
  - o Use the central management feature to manage and monitor virus / spyware signature update, scanning schedules, scanning reports and infection status of all machines in a central location.
- Scan machine hard disk periodically to detect and remove viruses/malicious code
  - o Schedule at least a weekly scan of your hard disk to check for virus / malicious code. The scheduled scan could be done in non-peak hours, such as during the lunch-break or after office hour.
  - o Turn on "Scan ALL files" option in your anti-virus / anti-spyware software. Do not just scan program files. Many current virus/malicious code are distributed via other forms like .EML, .VBS and .SHS.
- Configure the firewall policy to filter incoming and outgoing traffics
  - o Filter all incoming traffic unless explicitly stated necessary.
  - o Restrict unnecessary outgoing traffic. The outbound filter can effectively stop most of the Trojans from making outbound connections to leak confidential information.
- Configure desktops to detect malicious files that hide their extension
  - o Make sure your Windows Explorer show all file extensions. Go to "Tools | Folder | Options | View" and deselect "Hide file extensions for known file types."
- Install integrity checker software in critical production servers to detect unauthorized modification of system files.

3.6.2 Minimize the Risk of Possible Virus Attacks

- Guard your network against virus / malicious code spreading by external parties
  - Restrict external parties, e.g. guests and contractors, from tapping into your network before you have verified their machines are clean.
- Uninstall / disable unnecessary software / service
  - Many worms are attacking vulnerabilities of software components installed on the machine, e.g. IIS, SQL, DNS services. If you do not need them, uninstall / disable them can reduce your chance of being attacked.
- Patch the system and applications in a timely manner
  - Patch the software, including the operating system, browser and office application.
  - Monitor the latest patch information, e.g. turning on the Windows Update feature or subscribe to information security news.
- Limit the permission of access to use your computer
  - Do not allow other people to use your computer unless really necessary. These people might introduce malicious software and virus to your machine. In case you really need to allow such access, limit their access privilege to restricted access to folders and files only.
  - Avoid sharing out folders. If there is a valid reason to do so, share the folder with user name and password settings. Scan this folder for virus more frequently.
- Run applications with minimum privilege can prevent malicious code from gaining system privilege to do more harm to the system.
- Make sure your server and PC does not boot from floppy diskette drive or CDROM drive. Change the BIOS setting to boot from the local hard disk only. This is an effective measure against boot sector viruses.
- If there is any public accessed Internet kiosk in the company, isolate it from office network. It will minimize the impact to the company when this machine is infected.

3.6.3 Develop Best Practice in Handling Email and Files with Care

Do not rely solely on tools to detect and protect you from virus / malicious code attack. Human care must be exercised to detect and avoid virus attack. This is critical when the tools are still not updated of the signature of the new virus.

- Handle email attachment carefully
  - Do not open e-mail attachments from unexpected sources. Some viruses / malicious code disguise themselves as season's greetings / celebrations. Do not execute any attachment unless you are sure what it does.
  - Scan the e-mail attachments with anti-virus software before execution.
  - Use MS Office Viewer (Word / Excel / PowerPoint) to read office documents attached to emails. These viewers do not run the macro scripts embedded in the documents and can therefore avoid macro viruses. They are available for download at the Microsoft website.
- Check external files before use

- Check floppy diskettes, CD-ROMs and files downloaded from the Internet with anti-virus software before use.
- Legitimate downloaded code may include digital signatures that allow you to check if the source of the code is a trusted party.

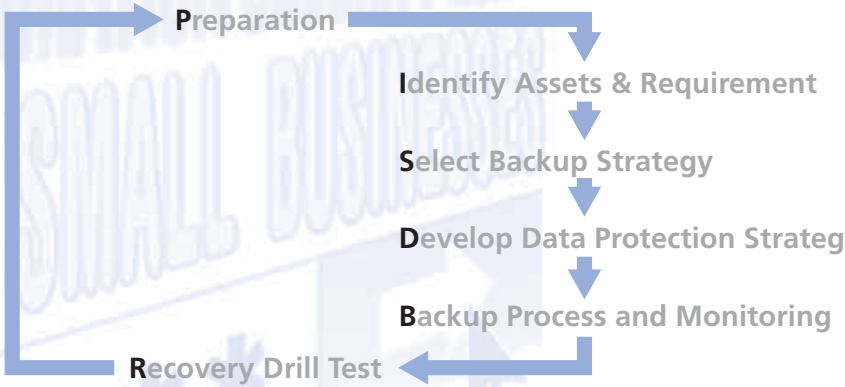
- Do not use illegal software
  - Using illegal software is very dangerous. It may contain virus, worm or Trojan. You may infect your own system by installing them on your machine.
- Learn about hoaxes
  - Do not send hoaxes to others. Hoaxes often spread fake alarms. They usually come in an email in a chain letter fashion describing some highly unlikely type of virus. A hoax usually has no reference to a trustworthy third party who can validate the claim of the message.

3.6.4 Develop Incident Response Capability

Section 5 of this booklet outlines the general steps of incident response and can be used as a reference. Here we list steps relevant for handling virus / malicious code incidents.

- Keep informed of virus information and alerts
  - Subscribe to information security and virus news, e.g. HKCERT free Information Security Alert Service and your company anti-virus software provider mailing list.
- Establish incident response strategy
  - Develop reporting, response and recovery procedure to handle security incidents that include virus / malicious code infection. Define the roles and responsibilities of users and the response/recovery personnel.
- Prepare for the recovery of system and data
  - Create Emergency Recovery Diskette / CD-ROM and put in a safe place. This is a diskette/CD that helps to start your system. Create also the Rescue Diskette of the anti-virus software. The rescue diskette helps to delete any virus in the system during recovery.
  - Backup your data regularly to media other than your local hard disk. Data can be recovered even if your machine is totally crashed.
- Report incident to management and HKCERT
  - Incident response team and management must be informed first. The incident response team can call HKCERT for assistance.
- Containing the damage of virus / malicious code attack.
  - Disconnect the machine from the network to stop spread of virus / malicious code.
  - If necessary, scan the connected machines within the same network segment to ensure no further spreading of the virus / malicious code.
- Remove virus or malicious software from the system. Verify that the machine is completely clean.
- Recover the system and data files from a trusted source.
- Review the technical solutions and procedure for improvement.

3.7 Backup and Recovery



Six Steps to the Backup & Recovery

No matter how hard you try to protect data, things can go wrong. Backup is the last defense against data loss.

> Backup is the last defense against data loss.

3.7.1 Preparation

- Planning and preparation must be done beforehand to ensure the backup process is manageable. Including the backup planning in the system design can make the backup management much more effective.
- Centralize the critical data on the secure server where it can be backed up effectively and efficiently.
- Segregate the system files and data files on separate partitions or separate machines to make the backup much easier.
- Design the recovery configuration according to the business continuity plan requirement. If you plan for a machine failure, make sure the backup machine can load the required software and can connect the backup device of production machine. If you plan for a site failure, make sure the availability of the backup device and backup software.
- Define the roles and responsibility of backup and recovery
  - o System administrator is responsible for performing centralized backup and reviewing of backup log, supervised by the system manager.
  - o System user is responsible for performing local / distributed backup and reviewing of backup log, supervised by department management. System administrator should provide technical support when users have technical problems.
  - o System owners have the responsibility to perform backup whenever there is a system change.
- Include the Backup and Recovery Test as a milestone in the project plan. This will ensure the system has gone through backup and recovery test before production.
- Prepare sufficient backup media and the storage cabinet. If offsite media storage strategy is favored, prepare for the offsite storage library.

3.7.2 Identify Information Asset and Backup Requirement

A Backup Information Asset List can be used to collect the information. The sample list below includes both hard and soft copy items.

Item	Criticality	Location	Size	Update frequency
Company server – system file – user profile	— Critical	C:\ on server S1	2GB 10MB	– When changed – Update all the time
Office data	—	D:\Data on server S1	20GB	Every day
Critical data	Critical	D:\Data on server S2	10GB	Every day
Encryption key	Critical	D:\Keys on server S2	1MB	When changed
Password list	Critical	Hard copy	3 pages	When changed
Trading procedure	Critical	Hard copy	30 pages	When changed
Recovery procedure	Critical	Hard copy	5 pages	When changed

Sample Backup Information Asset List

3.7.3 Select the Backup Strategy

Based on the information collected, the backup strategy can be defined.

Strategy options	Recommendations
Centralized / Distributed Backup	• Centralized is most preferred in general. • Distributed is useful for small amount of departmental sensitive files.
Medium (hard / soft)	• Hardcopy is easily backed up by photocopying. You can also convert the hard copy to electronic format to streamline the backup process. • For electronic copy, the selection criteria of storage medium are capacity, durability and the availability of backup device at recovery location.
Backup Frequency and Retention Cycle	• Define the frequency according to the requirement of individual data set. For example: o Server System Disk is imaged on CD-ROMs once a month and is kept for 1 year. o Data is backed up daily from Monday to Friday and is kept for 5 cycles. We recommend keeping at least 3 cycles of backup.
Mode (full / incremental / differential backup)	• Full backup is recommended because it is simplest to maintain. • Incremental/Differential backup is useful when the data set is too large to fit on one backup media. If you have a 5 day cycle and want to restore the data of last Friday: o In incremental backup, you need to restore last Monday's dataset followed by all the other four datasets sequentially. o In differential backup, you need to restore last Monday's dataset followed by the Friday's dataset. So differential backup is more efficient than incremental backup.

There are other strategies for data availability, for example, disk mirroring or data synchronization to backup machine. However, they are considered as redundancy rather than backup strategy because the synchronized replica of dataset can hold only current data.

3.7.4 Develop Data Protection Strategy

There are risks with the storage and handling of backup media. Below are the risks and recommended mitigations.

Risk	Recommended Mitigations
Environmental threats such as fire, water and dust	• Store backup media in fireproof safe in air conditioned room.
Backup tape corruption	• Clean the backup device regularly to extend the lifetime of backup media. • Specify the expiry date of backup media on the media label. • Check the backup log and replace flawed tapes.
Leakage of confidential information and Theft	• Separate backup media of sensitive data from normal data. • Label backup media with sensitivity indicator. • Use encryption technology in backup process. • Store backup media in physically safe place, logging of in/out of tapes. • Ensure transport of media to offsite storage is secure.
Production site not accessible → Backup Media and Recovery Procedure is unavailable	• Store backup media and a copy of recovery procedure offsite.

3.7.5 Backup Process and Monitoring

- Label the backup media with cycle number and tape number. Put also the media expiry date.
- Print out the backup calendar and post in prominent place near the backup console.
- Set up the backup job definition and schedule according to the backup strategy.
- Perform the backup job and keep a record of the backup activity.
- Review the backup log to verify the job can be completed successfully and fix any problem. Record down the problems and follow up. Management should review the log file and record sheet regularly.
- Store the backup media safely. Dispose the expired backup media according to the data protection strategy.

3.7.6 Recovery Drill Test

- A backup that cannot be recovered is completely useless. You must ensure that the backup strategy is useful with time.
- Recovery drill test should be conducted periodically.
  - o If there is no system change, you can do the restoration of system and data once per 3 or 6 months. If there is change to the system, backup software or backup device, you have to do the test immediately.

A backup that cannot be recovered is completely useless.

- Review the backup procedure and technical configuration and recommend improvements.
- Implement the improvements.

ASSURANCE OF SECURITY RISK MITIGATION 4

4.1 Role of Security Assurance and Review

The previous sections have described steps on:

- How to find out what security improvements the company requires;
- How to select solutions and implement them.

However, these steps are usually performed from the perspectives of one who is to protect the system. If we can take the perspectives of an attacker who is to exploit the vulnerabilities, we might have picked up something that we could have missed. It is always better to locate the vulnerability before the attacker tells you. Vulnerability may exist when:

- It was not identified or not given the right priority in the risk assessment stage.
- It was identified and security procedure is in place but the procedure is not followed.
- It is a newly published vulnerability in a vendor product. The company has not installed the related security patch.
- There are changes in the company computing environment without sufficient regard to their security implications.
- The hackers have got smarter.

Use Controls and Audit to assure check the system security is up to the requirement of security policy.

The company managers require assurance mechanisms to ensure that the implemented risk mitigation measures are working as expected, and to scan for significant security vulnerabilities. There are two approaches:

- Controls: the company security environment is continuously monitored and corrective action is taken as necessary.
- Audits: information is collected and analyzed by a separate process to determine if the current state of security in a specified area meets the company management objectives.

The initial flow of security risk assessment →mitigation →assurance is just the start of the information security management cycle. Periodic reviews and improvements are required to attain an optimum security environment. Periodic reviews should include:

- Reports from incident response teams (See "Section 5. Incident Response").
- Audit reports
- Details of actual or proposed changes in the company systems / services.
- Changes in the external environment: technological developments, Government ordinances.

4.2 Controls and Audits

4.2.1 Security Controls

Security controls involve monitoring of and taking necessary corrective actions on key security areas, including:

- Security policy, standards, guidelines and procedures.
- Staff roles and responsibilities.

- Access control such as user ID and passwords, access privileges etc.
- Physical security.
- Change management control.
- Security awareness training.
- Information security incident response and handling.

Some of the most effective controls can be enforced by company management directly. Monitoring measurement should be implemented to detect for violation of security policy, such as:

- Doors to secure areas left open.
- Unattended logged on workstations.
- Power sockets with excessive loads.
- Equipment not checked in and out.
- Password sharing.
- Unaccompanied visitors walking into sensitive area or accessing sensitive data or systems.

If management fails to enforce security policy in the company, then the company security will gradually unwind.

Another class of control is the automatic logging facilities of computer system. Computers and networks can often be configured to record events that have security implications. The log of these events can be invaluable to company management:

- Provide early warnings of actual or attempted misuse of the systems by users.
- Give early warnings of hacker activity or malicious code attack.
    - o System accessed at unusual hours.
    - o Password trial attempts (brute force attack).
    - o Network break-ins attempts.
- Provide diagnostic information relevant to a security incident.
- Provide evidence of illegal activity.

These logs provide an essential record of computer and network usage. Company management should ensure a regular analysis of the logs, accompanied with reporting and corrective action. Here are some recommendations on logging:

- Keep only valuable logs, such as access logs for security audit.
- Synchronize the computing facilities time to make correlation of events possible.
- Review the log regularly and report incident immediately when anomaly is found. Use tools to automate the log review process.
- Store log files in a safe place where unauthorized party cannot read or change.
    - o An option is to transmit the log files to a secure central logging server.
    - o Transmission of log must be via a secure link (link not going through untrusted network) to avoid tampering and sniffing.
- Protect the logging configuration from damage by unauthorized party.
- File, label and index archived logs to facilitate searching.

- Encrypt sensitive log files.
- Retention of logs should be 6 months or more. Archive previous log.
- Cycle logging media should be regularly changed to ensure that no data is lost due to media overflow.

4.2.2 Security Audits

Security audit is an important part of the risk assurance program. The objectives of a security audit include:

- Review of existing security controls on operational, administrative and managerial issues, and ensure compliance to company security policy.
- Identification of existing vulnerabilities.
- Examination of the effectiveness and adequacies of the security policy, standards, guidelines, procedures and implementations.
- Provision of recommendations and corrective actions on security measures after evaluations.

There are two types of audits: Security Audit and Policy Audit

- Security Audit: review security systems against security policies and procedures and looks for system weaknesses and vulnerabilities.
- Policy Audit: test and validate security systems against the company's established security policy, ensuring that your security policy is accurately reflected in your security systems' rules and permissions.

Security audit is an on-going activity and should be conducted periodically. It should be noted that a security audit only gives a snapshot of the vulnerabilities revealed at a particular point in time. There are different situations when a security audit should be performed. The exact timing depends on your system requirements and resources, including:

- Conduct security audit prior to implementation or major enhancements in order to ensure conformance to existing policies and guidelines and meet the configuration standard.
- Conduct vulnerability assessment periodically either manually or automatically using tools in order to detect security loopholes or vulnerabilities.
- Perform random security audit in order to reflect the actual practice.

4.2.3 Regular Vulnerability Assessment

Security audits are usually performed by external auditors. However, a company can always improve its security assurance by conducting regular vulnerability assessment. Regular vulnerability assessment is usually performed by company staff to identify potential security loopholes or vulnerabilities which could allow the company to avoid or minimize potential threats. It is recommended to perform vulnerability assessment after a major system change or twice a year.

A vulnerability assessment can focus on different areas including procedural review of the personnel department, and network vulnerability assessment. We describe one example below: "Network vulnerability assessment".

Regular Vulnerability Assessment can be performed when there is a system change or twice a year.

Network vulnerability assessment

Objective: to locate, identify, and mitigate the risks posed by inadequate security throughout office network.

Activities:

- Typical activities include use of network security analysis tools to scan systems and network assets to identify known security problems with such elements as routers, servers, desktops, and network printers.
- Other activities include:
  - o Reviewing physical infrastructure.
  - o Analyzing policies and physical / procedural controls.
  - o Interviewing security operations personnel to evaluate the mechanisms by which critical systems are maintained and administered.
- Analysis and interpretation of the results.
- Submitting a management report, with recommendation to company management.

Useful free tools for vulnerability test

Network-based:
Nessus http://www.nessus.org
NMap http://www.insecure.org/nmap/

Host-based:
bastille-linux http://www.bastille-linux.org
Microsoft Baseline Security Analyzer
http://www.microsoft.com/technet/security/tools/mbsahome.mspx

Important Note:
Use these tools at your own risk. You must obtain authority from the system owners to assess their systems.

4.2.4 External Audits

External audit is an expensive project for a company, before one is undertaken a number of questions should be addressed:

- Why do we have an audit?
- What is the objective of the audit?
- What is to be audited?
- Who is to do the audit?
- What will be followed up with the report?

The purpose of the external audit is to gain the benefit of the security expertise of the audit team; hence the vulnerabilities or inadequacies discovered should be those that would not be found by company staff alone. The cost of the external audit can be substantially reduced by:

- Good documentation reducing the fact-finding and interviewing effort of the audit team.
- Ensuring that that every effort is made to provide effective security to the system before the audit.

In general, external audits may take the form of:

- General control reviews .
- Vulnerability identification.

4.2.4.1 General Control Review

A General Control Review is an overall security audit normally designed to determine if the current security protection conforms to its company security policy or appropriate standards, e.g. ISO 17799. The standard to be used by the audit team should be agreed at the outset. The purpose of the audit is to provide information on the overall level of security within the company for company management, or for external purposes, e.g. as assurance to clients. This type of audit may include:

- Security policy, standards, guidelines and procedures.
- Roles and responsibilities.
- Administration and monitoring.
- Physical control.
- Security incident response.

Company management would be well advised to call upon an external audit team because advice is often required on the adequacy of the security policy developed by management. Good comprehensive, documentation is essential to minimize the audit team's fact-finding effort.

The audit report is likely to report inadequacies in the implementation of current risk mitigation efforts. The company security documentation should include the audit report and company management's decisions on follow up action. The audit report should also be considered at the next security review. It represents a good starting point for the next round of risk assessment and risk mitigation.

4.2.4.2 Vulnerability Identification

This part will concentrate on identifying vulnerabilities using the following methods:

(1) System Review & Vulnerability Scanning
System review identifies any vulnerabilities and weaknesses of network or systems from internal point of access. The audit team should spot if there is any abnormal activity such as intrusion attempt. Furthermore, system configurations and network settings should be checked against the company information security documents (e.g. system hardening standards) or checklist, if any, to identify any difference from the expected settings. Moreover, audit team can perform vulnerability scans, using an automated vulnerability scanning tool, to quickly identify known vulnerabilities on the target hosts or network devices.

(2) Penetration Testing
The term penetration testing is used to cover:

- Deliberate attempts to bypass access control protection by a consultant.
- Testing the defenses of a network using various scanning techniques.

Some consultants, including ex-hackers, will offer to test system security by employing any means to gain unauthorized privileges, including social engineering. This service can cause resentment amongst staff tricked by the consultants. Companies should be aware of the potential disadvantages

and side effects of such penetration test.

Network penetration test should be undertaken after installation or updating of firewall or intrusion detection systems. Network penetration test uses scanning software to provide the company management with a hacker view of their network. It seeks to determine the information and facilities that can be found by connecting to the network as an external party and tests the network defenses. There are three main forms of network penetration tests:

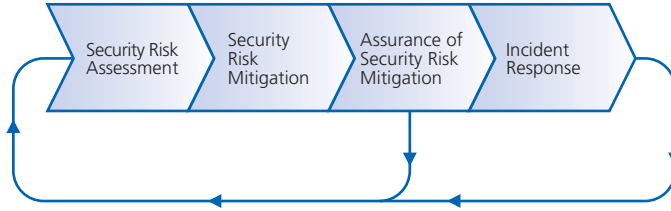
- Footprint analysis: looking for the information on network configuration etc. made available to outsiders.
- Network / service scanning: scans for network and host services that are available and hence potential targets for hacker attack.
- Exploitation analysis: performs limited attacks using the opportunities revealed by the vulnerability assessment to determine the potential damage that could arise, e.g. gaining access to web servers.

Any form of penetration test opens up the company assets to the consulting team; management should ensure that they engage a trustworthy team. The details of the testing process should be specified, e.g. if it is to include exploitation analysis and if so under what terms. Moreover, you should ensure the latest full system backup of the target systems is available since penetration tests may impact the integrity of the data in target system. You may as well consider to arrange the penetration tests to be conducted at non-peak working hours in order not to affect the normal operation of your business.

Penetration tests should only be conducted after every effort has been made by company staff to design the firewall rules in accordance with security policy, and an effective firewall management regime is in place.

Audit team must obtain authority from the system owners to assess their systems.

4.3 Review the Security Process



This guide recommends a staged approach to company security with a risk assessment, risk mitigation and risk assurance projects continually refining the company security environment. Effective information security management demands security expertise and experience from company management and technical staff; the experience gained from one cycle of the security risk assessment, mitigation and assurance can greatly facilitate subsequent cycles.

Complete security reviews should be scheduled by management. These reviews should consider the report and recommendations by the company manager with overall responsibility for security. The review committee should be supplied with:

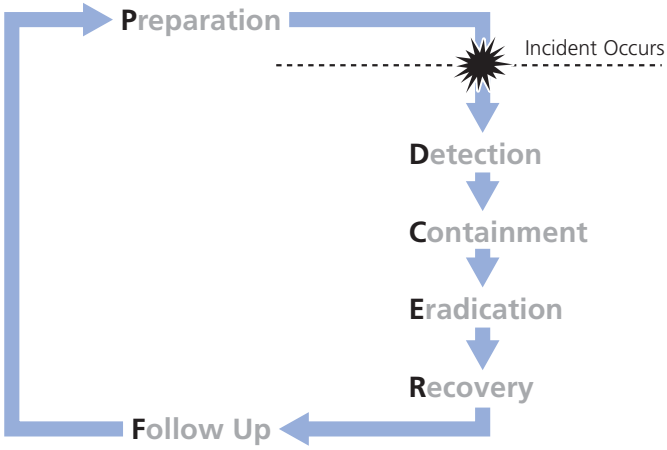
- Current security documentation.
- Incident response and audit reports.
- Details of the implementation of recommendations contained in incident response and audit reports.
- Details in any proposed changes in company systems, services, operations or environment.
- Details of changes in the external environment with security implications:
  - o New technologies.
  - o Security stance of competitors.
  - o New legislation and ordinances.

The review committee should recommend as appropriate:

- Modifications in the current security systems and/or procedures.
- A new assessment, mitigation and assurance cycle with estimated budget.

FORMATION SECURITY GUIDE
OR SMALL BUSINESSES

INCIDENT RESPONSE 5



Six Steps to Incident Response

Objective of Incident Response

- Minimize business losses and subsequent liabilities to the company;
- Minimize the possible impact of the incident in terms of information leakage, corruption and system disruption etc.;
- Ensure that the response is systematic and efficient and that there is prompt recovery for the compromised system;
- Ensure that the required resources are available to deal with the incidents, including manpower, technology, etc.;
- Ensure that all the responsible parties have clear understanding about the tasks they should perform during an incident by following predefined procedures;
- Ensure that the response activities are recognized and coordinated;
- Prevent further attacks and damages; and
- Deal with related legal issues.

A good incident response planning stops an incident from becoming a disaster.

No matter how good the risk mitigation measures can reduce the impact of security incident and the probability of occurrence of incidents, an incident may hit you unexpectedly! You must be prepared.

5.1 Legal and Contractual Considerations of Incident Response

The security policy (refer to Section 3. Security Risk Mitigation) has incorporated the legal and contractual implications in information security which should also be reflected in the Incident Response strategy. For example, service contracts might have set time limits for you to recover the business to a specified level, or to convey security incidents to customers or regulatory body.

Some information security incidents involve criminal offense and some do not. For example, defacing a website, compromising a vulnerable server, spamming and stealing information on a compromised server are offenses in Hong Kong while port scanning is not offense in Hong Kong. You should also notice that different countries have different laws regarding cyber crime. If the incident is an offense, it should be reported to the law enforcement. If you are not sure, you should consult the law enforcement.

Useful Reference on Ordinances Related to Computer Crime

Appendix A contains a list of ordinances related to computer crime in Hong Kong at the time of printing of this booklet.

Dilemma in prosecuting of hacker

Do you want to prosecute the attacker? If so, should you leave the network connection on to track an attacker's activity? But will this allow the attacker to do more harm? What should you do if there is a conflict between resumption of business and tracking and prosecuting the attacker?

No matter what your answer is. You should:

- Involve the management to make the decision.
- Follow the pre-defined priorities and criteria stipulated in the incident response plan to act accordingly.
- Identify the command structure of the decision making and notification to law enforcement.

Considerations in the collection of evidence

Incident response team (or IRT) staffs get in contact with first-hand evidences, such as log files and system status information (e.g. system time, current running processes and connecting machines). It is essential to know how to deal with evidences. Here are some guidelines:

- A piece of Evidence is a fact and the truth.
- Electronic Evidence must be captured as soon as possible.
- A proper chain of custody of the evidence should be maintained. A chain of custody is a history that shows how evidence was collected, analyzed, transported and preserved in order to present as evidence in court. A clearly defined chain of custody demonstrates that the evidence is trustworthy.
- Evidence should be collected with proper (un-contaminated) tools under pre-defined procedures.
- Evidences should be protected from unauthorized access and from modification or damage. Transfer or Copy of Evidence should be approved and witnessed.

IRT refers to the incident response team. Some organizations use computer security incident response team (CSIRT) to refer to the same functional team

Incident response team staffs should take good note of Actions and Results. Applying the guideline of evidence collection, they should:

- Log down events clearly and tidily in chronological order with time stamp. Use preprinted form if possible to make the format consistent. Use other effective media like audio and video taping when necessary.
- Put down facts, not speculation or unsure interpretation. Ambiguous and careless statement might cause damage to the legal case.
- Correct mistake once found and record the cause of the mistake.

Considerations in tracking the source of hacking

Malicious attacks can provoke into strong reactions amongst technical staff. Do not let emotion driving you to take priority to catch hacker over minimizing the impact. Here are some advices:

- Strike back? DO NOT consider this strategy. The attacking system might just be another victim whose control has fallen to the hacker. Secondly, spoofing can cause mis-interpretation of the source of the attacker. Last of all, there is no legal ground of attack for revenge.
- Keep Low Profile. Be careful that you might act in a way that makes the hacker being notified of your action. The hacker might react by erasing the footprint or causing damage to the whole system.
- Be familiar with the technical process and tools to make tracking efficient and unnoticed.

5.2 Six Steps to Incident Response

The six steps model is a generalized process cycle for incident response. The tip to success is getting prepared.

The incident response capability is an indicator of the competence of the company management.

Proper and advanced planning ensures the response activities are known, coordinated and systematically carried out. It also facilitates the management to make appropriate and effective decision in tackling security incident, and in turn minimizes the possible damages caused. The plan includes strengthening of security protection, making appropriate response to the incident, recovery of the system and other follow up activities.

5.2.1 Preparation

Planning allows a top down approach to incident response management to provide an assurance of quality and response time.

- Determine the local policies.
- Make sure the incident response strategy is consistent with the company security policy and sufficient authority is granted to the incident response team to take specified actions, e.g. switch off company web services in the critical moment.
- Define roles and responsibilities of incident response team and parties participating in the security incident handling process.
- Define the roles and responsibilities of other company staffs. Communicate this to functional management.
- Establish the list of prioritized information asset / services and acceptable downtime
- Develop Reporting Procedure, Escalation Procedure and Security Incident Response Procedure. These procedures should be communicated to all employees, including management personnel, for their reference and compliance.
- Facilitate early detection, e.g. by building a simple technical environment sufficient for job function and a user-friendly help desk.
- Develop and maintain good backup strategy.
- Develop and maintain the Call List.
- Update with guideline, checklist and tools of HKCERT and other CERT centers.
- Develop knowledge and skills of incident response team by training and sharing.

Call List is a list of contacts in emergency. They include incident response team, senior management, service providers, etc.

- Provide adequate staff training to ensure all concerned staff and management are capable of handling security incidents.
- Educate users the emergency procedure and incident reporting contacts.
- Set up system time synchronization mechanisms for computer systems.
- Set up monitoring and alerting mechanism for computer systems, such as install intrusion detection system, anti-virus and content filtering tools, enable system & network audit logging and perform periodic security checking using security scanning tools.

5.2.2 Detection

- Monitor abnormal events, e.g. error messages, suspicious events in logs, poor performance and unusual capacity growth.
  - o [Note] Intruder might have installed Trojan on system that hide himself.
- Determine type of problem and extent of impact.
- Start taking record using a standard incident logging form.
- Handle information with reference to the guideline on evidence collection.
- Make a full backup of compromised system as soon as you find it a real incident and store it in secure place.
- Capture records of incidents, e.g. auditing log, accounting log, etc.
- Inform the management and other "Right" people using the call list (IRT, ISP, network service provider...) and call tree (system owner notification). Enforce the "Need to Know" policy and use secure out-of-band communication channel when necessary.

Take sufficient time to assess the incident, get the facts and assess them before jumping to conclusions.

5.2.3 Containment

Activities in this stage may include:

- Conducting impact assessment of the incident on data and information of the system to confirm if the concerned data or information had already been damaged by or infected in the incident;
- Protecting sensitive or critical information and system. For instance, move the critical information to other media (or other systems) which are separated from the compromised system or network;
- Deciding on the operation status of the compromised system;
- Building an image of the compromised system for investigation purpose and as evidence for subsequent follow up action;
- Keeping a record of all actions taken during this stage; and
- Checking any systems associated with the compromised system through shared network-based services or through any trusting relationship.

One of the important decisions to be made is whether to continue or suspend the operation and service of the compromised system. This will very much depend on the type and severity of the incident, the system requirement and the impact on the image of the company, as well as the predefined goals and priorities in the incident handling plan of the system.

Actions to be taken may include:

- Shutting down or isolating the compromised host or system temporarily to prevent further damage to other interconnected systems, in particular for incidents that will spread rapidly, for machines with sensitive information, or to prevent the compromised system from being used to launch attack on other connected systems;

- Stopping operation of the compromised server;
- Disabling some of the system's functions;
- Removing user access or login to the system;
- Continuing the operation to collect evidence for the incident. This may only be applied to non mission-critical system that could accept some risks in service interruption or data damage, and it must be handled with extreme care and under close monitoring.
- Protect computer evidence by moving people out of reach of computer, electric switches, storage media and telephone
- Assess the risk of continuing operation and if the downtime might exceed the acceptable level. Management should make the decision based on the recommendation of the IRT on whether the activation to disaster recovery site if necessary.
- Keep system owner informed of the status to get their trust and make them feel comfortable.

Note:

- Display of a defaced web page can continue even when the web server has been disconnected, because it may be cached by the service providers. A backup server with an appropriate web page indicating that the service is unavailable can overcome this problem.
- Containment is more complex if the incident has law enforcement or legal liability implications. Get management involved in decision making and get advice from law enforcement.

5.2.4 Eradication

The goal of eradication is to eliminate or mitigate the cause of the security incident. During this stage, the following actions may need to be performed depending on the type and nature of the incidents as well as the system requirement:

- Stop or kill all active processes of the hacker to force the hacker out.
- Delete all the fake files created by the hacker. System operators may need also to archive the fake files before deleting to aid case investigation.
- Eliminate all the backdoors and malicious programs installed by the hacker.
- Apply patches and fixes to vulnerabilities found on all operating systems, server and network devices etc. Patches or fixes applied should also be tested thoroughly before the system is restored to normal operation.
- Correct any improper settings in the system and network e.g. mis-configuration in firewall and router.
- In case of a virus infection incident, inoculate the virus from all infected systems and media following anti-virus software vendor advisories.
- Provide assurance that the backups are also clean to prevent the system from being re-infected at a later stage when system recovery from backup is needed.
- Make use of some other security tools to aid in the eradication process, for instance, security scanning tools to detect any intrusion, and apply the recommended solution. These tools should be kept up-to-date with the latest intrusion patterns.
- Update the access passwords of all login accounts that may have been accessed by the hacker.
- In some cases, the supporting staff may need to reformat all the infected media and reinstall the system and data from backup, especially when they are not certain about the extent of the damage in a critical system or it is difficult to completely clean up the system.

5.2.5 Recovery

The purpose of this stage is to restore the system to its normal operation. Examples of tasks include:

- Perform damage assessment.
- Re-install the deleted / damaged files or the whole system, whenever required, from the trusted source.
- Bring up function / service by stages, in a controlled manner, and in order of demand, e.g. the most essential services or those serving the majority may resume first.
- Verify that the restoring operation was successful and the system is back to its normal operation.
- Prior notification to all related parties on resumption of system operation, e.g. operators, administrators, senior management, and other parties involved in the escalation procedure.
- Disable unnecessary services.
- Keep a record of all actions performed.

Note:

- Prior to restoring the system to normal operation, one important action is to conduct a pre-production security assessment to ensure that the compromised system and its related components are secured.

5.2.6 Follow Up

The goal of Follow up is to learn from the lesson of the incident. The follow up should start as soon as possible after the incidents. Management, users and the on-site IRT should be involved.

- A post mortem analysis should be conducted to find out areas of improvement, for example:
  - Checking if the current configuration and procedure are sufficient.
  - Checking if more user education is required.
  - Determining if an external security audit is required.
  - Determining if the incident should require any legal action.
- All parties involved should be invited to give comment to the draft of the post mortem analysis.
- An executive summary with recommendations for improvement should be sent to management.
- The management should assess the report and select the recommendations for improvement to be implemented. Those who report incidents and those who helped to make the incident response successful should be acknowledged or rewarded.

The ability to learn from incidents determines the Incident response capability of a company.

The next step of follow up is going back to the first step "Preparation" for implementation of selected recommendations and starts another cycle of continuous improvement.

Useful links for Incident Response

CERT/CC Incident Response FAQ
http://www.cert.org/csirts/csirt_faq.html

Collecting Electronic Evidence After a System Compromise
http://www.auscert.org.au/render.html?it=2247&cid=1920

Steps for Recovering from a UNIX or NT System Compromise
http://www.auscert.org.au/render.html?it=1974&cid=1920

SANS Reading Room – Incident Handling
http://www.sans.org/reading_room/whitepapers/incident/

APPENDIX A:

ORDINANCES RELATED TO COMPUTER CRIME

Computer Crimes Ordinance

The main piece of legislation introduced against computer related crime is the Computer Crimes Ordinance. Enacted in 1993, it has, through amending the Telecommunications Ordinance (Cap. 106), Crimes Ordinance (Cap. 200) and Theft Ordinance (Cap. 210), created some new offences and broadened the coverage of existing offences.

More details is available on the next page

Copyright Ordinance

Hong Kong's new Copyright Ordinance came into effect on 27 June 1997. It provides comprehensive protection for recognized categories of literary, dramatic, musical and artistic works, as well as for films, television broadcasts and cable diffusion, and works made available to the public on the Internet.

More details is available on the next page

Electronic Transactions Ordinance

Enacted on 7 January 2000 to facilitate the use of electronic transactions for commercial and other purposes. It gives electronic records and digital signatures used in electronic transactions the same legal status as that of their paper-based counterparts. It also enables the Postmaster General to provide the services of a certification authority.

Please refer to http://www.info.gov.hk/digital21/eng/ecommerce/etb/etb.html for more details

Personal Data (Privacy) Ordinance

To protect the privacy interests of living individuals in relation to personal data. The Ordinance covers any data relating directly or indirectly to a living individual (data subject), from which it is practicable to ascertain the identity of the individual and which are in a form in which access or processing is practicable. It applies to any person (data user) that controls the collection, holding, processing or use of personal data.

Please refer to http://www.pcpd.org.hk/ for more details

Unsolicited Electronic Messages Ordinance

The purpose of the Ordinance is to strike the right balance between respecting the rights of recipients and allowing the development of legitimate electronic marketing in Hong Kong. Apart from the provisions related to the "opt-out" regime (i.e. part 2 of the Ordinance), the Ordinance has come into force on 1 June 2007.

Please refer to http://www.ofta.gov.hk/ for more details

Computer Crimes Ordinance

The main piece of legislation which has been introduced against computer related crime is the Computer Crimes Ordinance. Enacted in 1993, it has, through amending the Telecommunications Ordinance (Cap. 106), Crimes Ordinance (Cap. 200) and Theft Ordinance (Cap. 210), created some new offences and broadened the coverage of existing offences, as follows:

Table showing related computer crimes ordinances

Law	Provisions	Maximum Penalty
Telecommunications Ordinance S. 27A, Cap. 106	• prohibiting unauthorized access to computer by telecommunication	Fine of $20,000
Crimes Ordinance S. 59, Cap. 200	• extending the meaning of property to include any program or data held in a computer or in computer storage medium	Not applicable
S. 59 and 60, Cap. 200	• extending the meaning of criminal damage to property to misuse of a computer program or data	10 years' imprisonment
S. 85, Cap. 200	• extending the meaning of making false entry in bank book to falsification of the books of account kept at any bank in electronic means	Life imprisonment
S. 161, Cap. 200	• prohibiting access to computer with criminal or dishonest intent	5 years' imprisonment
Theft Ordinance S. 11, Cap. 210	• extending the meaning of burglary to include unlawfully causing a computer to function other than as it has been established and altering, erasing or adding any computer program or data	14 years' imprisonment
S. 19, Cap. 210	• extending the meaning of false accounting to include destroying, defacing, concealing or falsifying records kept by computer	10 years' imprisonment

Source: http://www.infosec.gov.hk/

Copyright Ordinance

Table showing related copyright ordinance

Law	Provisions
Copyright Ordinance Cap. 43 Cap. 514 Cap. 522 Cap. 528 Cap. 568 Cap. 544 Cap. 445	 • Trade Marks • Patents Ordinance • Registered Designs Ordinance • Copyright Ordinance as amended by Intellectual Property (Miscellaneous Amendments) Ordinance 2000 • Copyright (Suspension of Amendments) Ordinance 2001 • Prevention of Copyright Piracy Ordinance • Lay-out Design (Topography) of Integrated Circuits Ordinance

Source: http://www.infosec.gov.hk/

Other Related Ordinances

In many cases, although no explicit reference to the cyber environment is made, the relevant legislation may be interpreted to cover both the physical and the virtual worlds. For example, the provisions of the Personal Data (Privacy) Ordinance are equally applicable to the cyber environment as the physical environment.

Many other legislative provisions refer to "computer" or similar terms. Some examples are set out below.

Table showing other related ordinances

Law	Provisions
Personal Data (Privacy) Ordinance Cap. 486	• protecting the privacy interests of living individuals in relation to personal data; applying to any person (data user) that controls the collection, holding, processing or use of personal data.
Electronic Transactions Ordinance Cap. 553	• giving electronic records and digital signatures used in electronic transactions the same legal status as that of their paper-based counterparts; enabling the Postmaster General to provide the services of a certification authority.
Evidence Ordinance S. 20. Cap. 8 S. 22A. Cap. 8 S. 54. Cap. 8	• making copy of entry in banker's record kept by means of a computer acceptable as evidence • making documentary evidence from computer records acceptable in criminal proceedings • including computer generated records within the meaning of "records"
Securities (Insider Dealing) Ordinance S.2. Cap. 395	• including in the definition of "document" any form of computer input and output
Land Survey Ordinance S. 2. Cap. 473	• including in the definition of "field note" a print-out from an electronic data recorder
Protection of Non-Govt. Cert. of Origin Ordinance S.10. Cap. 324	• empowering an authorised officer to demand any information contained in a computer to be produced in a form which can be taken away and which is either visible or legible
Securities Ordinance S. 83. Cap. 333	• creating an offence for any person who wilfully stores false material particulars or falsifies any entry or destroys records in an electronic device
Smoking (Public Health) Ordinance S. 13B. Cap. 371	• prohibiting the placing of tobacco advertisements on the

Source: http://www.infosec.gov.hk/

FORMATION SECURITY GUIDE
OR SMALL BUSINESSES

USEFUL CONTACTS

Hong Kong Computer Emergency Response Team Coordination Centre	
Email	hkcert@hkcert.org
Contact	8105-6060
Fax	8105-9760
Website	http://www.hkcert.org/english/home.html
Website for Subscription	https://www.hkcert.org/english/subscribe_ssl.html
Enquiry Information	➢ The latest computer virus and security alerts ➢ Related news, events, articles, monthly newsletter and website ➢ 24-hour Incident reporting ➢ (Free) Information Security Alerts by Email and SMS

Hong Kong Police Force – Technology Crime Prevention Unit	
Email	cpu-tcd@police.gov.hk
Contact	2528-3482
Fax	2328-7128
Website	http://www.police.gov.hk/police/hkp-home/english/tcd/contact.htm
Enquiry Information	➢ Services provided by the Technology Crime Prevention Unit (TCPU) ➢ Contact the TCPU

INFOSEC – The Information Security Portal	
Email	webmaster@infosec.gov.hk
Website	http://www.infosec.gov.hk/
Enquiry Information	➢ Information Security ➢ Computer Related Crime ➢ Protecting Yourself ➢ News and Events

Office of the Government Chief Information Officer	
Email	enquiry@ogcio.gov.hk
Contact	2582-4520
Fax	2802-4549
Website	http://www.ogcio.gov.hk/
Enquiry Information	➢ Knowledge on computer virus, information security and other IT-related areas

Commerce and Economic Development Bureau	
Email	webmaster@antispam.gov.hk
Fax	2989-6073
E-mail Spam Website	http://www.antispam.gov.hk/english/email/email7.htm
Enquiry Information	➢ FAQs on spam

Innovation and Technology Commission	
Email	enquiry@itc.gov.hk
Contact	2737-2208
Fax	2730-4633
Website	http://www.itc.gov.hk
Enquiry Information	➢ Internet-based technology information system ➢ Directory on Hong Kong Science & Technology Resources

Hongkong Post e-Cert	
Email	enquiry@hongkongpost.gov.hk
Contact	2921-6633
Fax	2775-9130
Website	http://www.hongkongpost.gov.hk/index.html
Enquiry Information	➢ Apply for e-Cert

Hong Kong Internet Service Providers Association	
Email	info@hkispa.org.hk
Website	http://www.hkispa.org.hk/
Enquiry Information	➢ Issues relating to Internet Service Providers (ISPs) ➢ Code of ethics of ISPs

USEFUL RESOURCES

Note:

This is not an exhaustive list of information security resource. The information contained here is for reference only. The author will not be liable for errors, omissions or inadequacies in the information provided by these resources. The readers assume sole responsibility for using the information to achieve their own purposes.

CERT

Hong Kong Computer Emergency Response Team Coordination Center
香港電腦保安事故協調中心
http://www.hkcert.org

Australia Computer Emergency Response
http://www.auscert.org.au/

China Education and Research Network Computer Emergency Response Team
中國教育和科研計算網機網緊急響應組 (CCERT)
http://www.ccert.edu.cn/

CERT® Coordination Center (CERT/CC)
http://www.cert.org/

National Computer network Emergency Response technical Team /Coordination Center of China
國家計算機網絡應急技術處理協調中心 (CNCERT/CC)
http://www.cert.org.cn/

Japan Computer Emergency Response Team Coordination Center
http://www.jpcert.or.jp/english/

Korea Computer Emergency Response Team and Coordination Center(CERTCC-KR)
http://www.certcc.or.kr/english/

Malaysian Computer Emergency Response Team
http://www.mycert.org.my/

Singapore Computer Emergency Response Team
http://www.singcert.org.sg/

Taiwan Computer Emergency Response Team /Coordination Center
台灣電腦網路危機處理暨協調中心
http://www.cert.org.tw/

United States Computer Emergency Readiness Team (US-CERT)
http://www.us-cert.gov/

News and Information

Hong Kong Police Commercial Crime Bureau – Technology Crime Division
香港警務處商業罪案調查科 — 科技罪案組 (TCD)
http://www.info.gov.hk/police/hkp-home/english/tcd/index.htm
http://www.info.gov.hk/police/hkp-home/chinese/tcd/index.htm

INFOSEC, Office of the Government Chief Information Officer
政府資訊科技總監辦公室資訊安全網
http://www.infosec.gov.hk/

Bilingual Laws Information System
雙語法例資料系統
http://www.legislation.gov.hk/

Hong Kong Internet Service Providers Association (HKISPA)
香港互聯網供應商協會
http://www.hkispa.org.hk/

Hongkong Post e-Cert
香港郵政電子證書
http://www.hongkongpost.gov.hk/

Office of the Privacy Commissioner for Personal Data, Hong Kong
香港個人資料私隱專員公署
http://www.pcpd.org.hk/

Commerce and Economic Development Bureau (CEDB) – E-mail Spam
商務及經濟發展局 — 濫發電郵
http://www.antispam.gov.hk/

ComputerWorld Security Topics
http://www.computerworld.com/securitytopics/security

LinuxSecurity.com
http://www.linuxsecurity.com/

SC Infosecurity News
http://www.scmagazine.com/asia/news/

Virus Information

INFOSEC, Office of the Government Chief Information Officer – Computer Virus
政府資訊科技總監辦公室資訊安全網 — 電腦病毒
http://www.infosec.gov.hk/english/general/virus/index.htm
http://www.infosec.gov.hk/chinese/general/virus/index.htm

Computer Associates Security Advisor
http://www3.ca.com/securityadvisor/

eSafe
http://www.esafe.com/

F-Secure
http://www.f-secure.com/virus-info/v-pics/

Kaspersky Labs
http://www.kasperskylabs.com/

McAfee
http://www.mcafee.com

Network-box
http://response.network-box.com/

NOD32
http://www.virus-radar.com/stat_01_current/index_enu.html

Norman
http://www.norman.com/

Panda Software
http://www.pandasoftware.com/virus_info/

Secunia Vulnerability and Virus Information
http://secunia.com/

Sophos
http://www.sophos.com/

Symantec
http://securityresponse.symantec.com/

Trend Micro
http://www.trendmicro.com/vinfo/

北信源
http://www.vrv.com.cn

瑞星
http://www.rising.com.cn/

金山毒霸
http://www.duba.net

Security Vulnerabilities

CERT® Coordination Center (CERT/CC)
http://www.cert.org/nav/index_red.html

Common Vulnerabilities and Exposures
http://www.cve.mitre.org

SANS Internet Storm Centre
http://isc.sans.org/

Secunia Vulnerability and Virus Information
http://secunia.com/

SecurityFocus
http://www.securityfocus.com/

SecurityTeam
http://www.securiteam.com/securitynews/

Security Patch

SunSolve Patch Support Portal
http://sunsolve.sun.com/pub-cgi/show.pl?target=home

IBM
http://www-03.ibm.com/servers/eserver/support/

HP
http://itrc.hp.com/common/bin/doc.pl

Microsoft TechNet – Security
http://www.microsoft.com/technet/Security/default.mspx

Red Hat Linux
http://www.redhat.com/security/updates/

Security Alert Mailing List

Anti-Phishing Working Group
http://www.antiphishing.org/

Microsoft Security Bulletin Subscription
http://www.microsoft.com/technet/security/bulletin/notify.mspx

SecurityFocus Mailing List
http://www.securityfocus.com/archive

VulnWatch
http://www.vulnwatch.org/subscribe.html

Zone-H Web Defacement Report
http://www.zone-h.org/

Articles

CERT/CC Publications
http://www.cert.org/nav/allpubs.html

Foundstone
http://www.foundstone.com

LinuxSecurity.com
http://www.linuxsecurity.com/docs/

O'Reilly Network
http://www.oreillynet.com/pub/q/articles

SANS Reading Room
http://www.sans.org/rr/

The Safety Mail Guide
http://www.aoema.org/

The Safety Net Guide
http://www.aoema.org/

Security Portal

WiredPatrol
http://www.wiredpatrol.org/

Free Security Tools

> Note:
>
> Please read the terms and conditions for use. License fee may be required for commercial use. The author will not be liable for any problem in using or caused by using these tools The readers assume sole responsibility for using the information to achieve their own purposes.

Ad aware – free multi spyware removal utility
http://www.lavasoft.de/

AVG – free Anti-Virus
http://www.grisoft.com/

eTrust Antivirus
http://www3.ca.com/securityadvisor/virusinfo/scan.aspx

F-secure Online Scanner
http://support.f-secure.com/enu/home/ols.shtml

McAfee FreeScan
http://us.mcafee.com/root/mfs/scan.asp?affid=56

Microsoft Baseline Security Analyzer – free boost-based vulnerability scanner
http://www.microsoft.com/technet/security/tools/mbsahome.mspx

Microsoft Windows Malicious Software Removal Tool
http://www.microsoft.com/downloads/details.aspx?familyid=AD724AE0-E72D-4F54-9AB3-75B8EB148356&displaylang=en

Microsoft Windows Defender (Beta 2) – free anti-spyware
http://www.microsoft.com/athome/security/spyware/software/default.mspx

Nessus - free Security Scanner
http://www.nessus.org/

Symantec free online virus and security check
http://security.symantec.com/default.asp?productid=symhome&langid=ie&venid=sym

Snort - free IDS Program on Linux
http://www.snort.org/

Spybot Search & Destroy – free anti-spyware
http://www.safer-networking.org/

Trend Micro free online virus scanner
http://housecall.trendmicro.com/

ZoneAlarm – free personal firewall
http://www.zonelabs.com/store/content/home.jsp

Associations on Information Security

Business Continuity Institute
企業持續營運協會
http://www.thebci.org

DRI International
國際災難恢復組織
http://www.drii.org/

Hong Kong Computer Society - Information Security Specialist Group (HKCS - ISSG)
香港電腦學會資訊保安專家小組
http://www.hkcs.org.hk/IS_SIG.htm

Information Security and Forensics Society (ISFS)
資訊保安及鑑證公會
http://www.isfs.org.hk/

Information System Audit and Control Association & Foundation (ISACA)
資訊系統審計協會香港分會
http://www.isaca.org.hk/

Information Systems Security Association (ISSA)
資訊系統保安協會
http://www.issa.org.hk/

International High Technology Crime Investigation Association Asia Pacific Chapter (HTCIA)
高科技犯罪調查協會
http://www.htcia.org.hk

International Information Systems Security Certification Consortium, Inc. (ISC^2)
國際信息系統安全核準聯盟
http://www.isc2.org/

Professional Information Security Association (PISA)
專業資訊保安協會
http://www.pisa.org.hk/

For enquiries about the contents of this handbook, please contact

Hong Kong Computer Emergency Response Team
Coordination Centre (HKCERT)
Email : hkcert@hkcert.org
Tel : 8105-6060
Fax : 8105-9760