MALAYSIA CYBER SECURITY CENTRE

e-Security

Volume 7 - (Q2/ 2006)

MOSTI

From the Editor's Desk

Greetings from the editor's desk. We have a new look for our newsletter and if you have any feedback on our new design, please do let us know. The new design reflects a more advance and technological look and feel.

So, what has happened in the second quarter? Well, the much awaited SecureMalaysia 2006 Conference and Exhibition took place very successfully from the 24th July - 26th July 2006. The event was opened by Y.B Dato' Sri Dr. Jamaludin Mohd Jarjis, the Minister of Science, Technology & Innovation.

It was a great event with many great speakers from all over the world. We had the honour of having Howard Schmidt, the former advisor to the US President on Cyber Terrorism and also former CISO for Microsoft & Ebay. It was thoroughly refreshing to listen to his talk and also we had Steve Orlowski and Dr. John Meakin.

This issue will see a variety of articles from our contributors touching many areas of information security. I do hope that you will find it useful and able to communicate with the contributors if you need more information.

Our CISSP classes are ongoing and our last class for 2006 is in August 2006 and exams in September and December. Do visit our website at **http://www.niser.org.my/cissp** for updates and information

Once again, we invite more security professionals to contribute to our newsletter and remember that you can view our newsletter online from our website at **http://www.niser.org.my.**

Philip Victor
vphilip@niser.org.my

Reader Enquiry

Training & Outreach Unit
Malaysia Cyber Security Centre
(formerly known as NISER)
MIMOS Berhad
Technology Park Malaysia
57000 Kuala Lumpur, Malaysia
Tel: +60 3 8657 7042 Fax: +60 3 8996 0827

Email: training@niser.org.my

Contributors

MS-106.07 2006: MyCERT Quarterly Summary (Q2) 2006

The MyCERT Quarterly Summary is a report which includes some brief descriptions and analysis of major incidents observed during that quarter. This report also features highlights on the statistics of attacks/incidents reported, as well as other noteworthy incidents and new vulnerability information.

Additionally this summary also directs to resources in dealing with problems related to security incidents, including patches, service packs, upgrades and hardenings.

1.0 Recent Activities

This quarter saw an outbreak of W32.Brontok worm that affected many organizations in the constituency. Besides this outbreak, there was an alarming surge in intrusions of mainly defacements of .MY domains hosted on virtual hosting servers and a tremendous increase in incidents involving forgery or identity theft. However in general, there was a 20.98% decrease in the number of incidents reported in this quarter compared to the previous quarter. The number of incidents reported for this quarter is 3379 compared to 4276 reports in the previous quarter with a majority of incidents contributed to reports on spam.

2.0 Surge in Intrusion

The second quarter of 2006 saw a surge in intrusion incidents with a total of 277 incidents, which is more than two folds from the previous quarter. Intrusions reported to us mainly involved web defacements of various domains belonging to our constituency and mass defacements of websites hosted on virtual hosting servers, inclusive of Windows and Linux platforms. MyCERT had also sent alert to the MyCERT-List members regarding the surge in mass defacements of websites hosted on virtual hosting servers for precautions purposes.

As the number of defaced websites in this quarter is quite alarming, thus, MyCERT would like to urge all system administrators and virtual host administrators to upgrade and patch systems/services/applications they are currently using. In addition, it is also recommended to disable unnecessary/ unneeded default services on the systems. MyCERT encourages system administrators to consult MyCERT for further advice and assistance, if they have difficulties in securing and hardening of their servers.Based on MyCERT's analysis of logs received from owners of victim machines, we found some of the defacements were due to PHP fopen() CRLF Injection vulnerability that were not properly patched besides manipulation of the unpatched WebDAV vulnerability running on web servers.

Details of the vulnerabilities and patches are available at:

1. WEBDAV Vulnerability
   http://www.cert.org/advisories/CA-2003-09.html

2. PHP fopen()CRLF Injection
   http://www.securiteam.com/unixfocus/5OP0C0A8AC.html

Detail guidelines on securing UNIX and Windows Servers are available at:

- UNIX Security Checklist by CERT/CC
  http://www.cert.org/tech_tips/usc20_full.html

- Windows 2000 Server Baseline Security Checklist by Microsoft
  http://www.microsoft.com/technet/security/chklist/iis5cl.mspx

- Windows NT Configuration Guidelines by CERT/CC
  http://www.cert.org/tech_tips/win_configuration_guidelines.html

3.0 Reports on Forgery/Identity Theft Increases

Forgery or identity theft incidents are still increasingly prevalent compared to previous quarter. A total of 89 incidents were received compared to 54 in previous quarter, which represents a 64.8% increase. Majority of Forgery incidents were phishing activities which mainly involved foreign financial institutions such as Ebay and Paypal, with a few involving local Financial Institutions. As was in previous quarter, in this quarter we continued to receive reports from foreign financial organizations and foreign CERTs regarding phishing sites hosted on Malaysian servers. MyCERT responded to the reports by communicating with the respective ISPs, Data Centers and Organizations to remove the phishing sites and within 6 hours or less the phishing sites were removed successfully. We had also advised the respective ISPs, Data Centers and Organizations to investigate the affected machines and rectify them accordingly.

MyCERT strongly urges users who receive emails purportedly from financial institutions requesting to change their logon and password to ignore/delete such emails immediately. When in doubt, users are to refer and verify any such emails with their ISPs, CERTs or with the particular financial institutions mentioned in the email.

In addition, organizations are advised to secure and harden their online services and applications to prevent their system from being compromised and used for malicious activities, such as running phishing sites, open relay, open proxies and zombie drones.

Besides phishing reports, MyCERT also received a few reports from our constituency regarding Internet scams, that are worth highlighting. Some of the Internet scams reported to MyCERT are:

a) Nigerian Scams
b) Benin Import Scams, which targets manufacturers
c) Advance Fee Scams, which targets foreigners looking for jobs in Malaysia
d) Lottery Scam and
e) Get Rich Scams

Nevertheless, the number of victims and monetary loss involved due to the above scams reported are low and not alarming. The modus operandi of the above scams are almost similar to one another as they employ using websites to lure Internet users to visit the website and deposit certain amount of funds to the fraudsters' accounts.Some scams had manipulated names of local law enforcement agencies by convincing Users of their activities via invalid/valid local addresses and contact numbers. Based on our analysis, we found the websites are mostly registered and hosted abroad. However, we believe some of the operators could be foreigners based in Malaysia - based on the nature and mode of the scams. Most of the Internet scam cases are referred to the local law enforcement agencies, i.e. the police and Bank Negara Malaysia for further investigations.

MyCERT advise Users not to deposit or credit funds except to bona fide and licensed financial institutions. Users who receive any or such scam/suspicious emails to ignore such requisitions and further advised to authenticate emails and contents with their respective ISPs, CERTs or Bank Negara Malaysia for clarification.

4.0 Malicious Code Outbreak

Incidents related to malicious code increased to 27 this quarter from 17 in the previous quarter. It represents a 58.82% increase. We observed an outbreak of the W32.Brontok worm in this quarter with about 18 reports on W32.Brontok worm and the rest of reports involved the W32.Nyxem worm. The W32.Brontok worm outbreak had partly affected the constituency with large number of PCs in many organizations. Organizations infected with the worm had their PCs' registries locked up and simultaneously disrupted security settings. However, successful worm eradication and system recovery processes by the respective organizations have had the situation contained. MyCERT had released the following revised alert related the W32.Brontok worms, as below:

- W32.Brontok Worm (Revised on 1st May 2006)
  http://www.mycert.org.my/advisory/MA-104.032006.html

MyCERT advise users/organizations to always take precations against worm incidents.through:

- Email Gateway Filtering

  Sites are encouraged to apply filters at email gateways to block any attachments associated to worms. Sites are also encouraged to close all ports except those necessary to prevent against worms that exploit open ports,

- System/Host Protection

  i. Users must ensure that their PCs are installed with anti-virus softwares and are frequently updated with the latest virus signatures.Users without anti-virus installed on their PCs may download such software from the following site:

     http://www.mycert.org.my/anti-virus.htm

  ii. Users need to ascertain their PCs or machines are always updated with the latest service packs and patches. Some worms propagate by exploiting unpatched programs present in PCs or machines.

  iii. Enable personal/host-based firewalls on PCs.

- Safe Email Practices

  MyCERT strongly advice users not to open any unknown attachments, received via emails. Any suspicious emails shall be deleted or forwarded to the respective ISPs or CERTs for verification. Users may refer to the following guidelines on safe email practices:

  http://www.mycert.org.my/faq-safe_email_practices.hlml

Increase in Hack Threat

Incidents involving hack threat showed an increase of 83.33% in this quarter. A total of 11 reports were received on hack attempts for this quarter compared to 6 in the previous quarter. Hack threats targeted mainly organizations' systems and networks involving network and host scanning activities.

MyCERT's findings for this quarter showed top ports commonly targeted were SSH (TCP/ 22), FTP (TCP/21), HTTP (TCP/ 80), MS SQL (TCP/1433). Port scannings are often actively carried out, using automated or non-automated tools once a new bug or exploit is released to the public. Besides scanning for open ports, scannings are also actively done to detect machines running vulnerable programs and scripts, such as Unicode vulnerability on IIS web servers and scanning machines running vulnerable PHP scripts.

MyCERT recommends the following good practices:

a) Close all ports or unneeded services except http service and other required ports/services should be filtered and patched accordingly.
b) All machines/systems are properly patched and upgraded with latest patches, service packs and upgrades
c) Organizations can install network based or host based IDS to alert scannings and other malicious attempts to their hosts.
d) It is recommended that home users install personal/host-based firewalls in order to alert of any scanning activities targeting their machines, and to block any unauthorized outgoing traffic from their system in the event their host has been compromised with spywares, adwares or trojans.

More information on home PC security is available at: **http://www.mycert.org.my/homepcsecurity.html**

Drop in Harrassment

Incidents involving harassment has dropped compared to previous quarter with a total of 11 reports this quarter compared to 14 reports previous quarter. This represents a 21.43% decrease.

Majority of harassment incidents reported, involved emails, chat forums and web forums communication. Most of the reports were referred to the law enforcement agencies for further investigation. MyCERT had also assisted law enforcement agencies in analysing several harassment incidents reported.

MyCERT advise users who are harassed via Internet or harassments of any kind on web forums with religious, social, political or economic implications to report to MyCERT for further analysis.

In addition, we also advise users to be careful while communicating on the net, either via emails, chat forums or web forums. They should never reveal or upload personal information such as their contact numbers, home address, photos on the net or transmit to untrustworthy source as such information could be open for exploitation.

Other Activities

Spam

Spam incidents dropped with a total of 2964 reports which represents a 27.50% decrease compared to previous quarter. The main reason for the decrease may be due to more ISPs and organizations applying anti-spam filters at their gateways to prevent spam emails from dropping into end-users mailbox. We see this as a positive measure in minimizing spam activities in the country.

Spam has developed from a mere nuisance into an epidemic that threatens enterprises. There are no perfect techniques or tools to completely eradicate spams, however there are procedures that can minimize them. Organizations are advised to install anti-spam filters at their email gateways to minimize spam emails and End-Users are also advised to appropriately apply filters to minimize spam emails.

Denial of Service

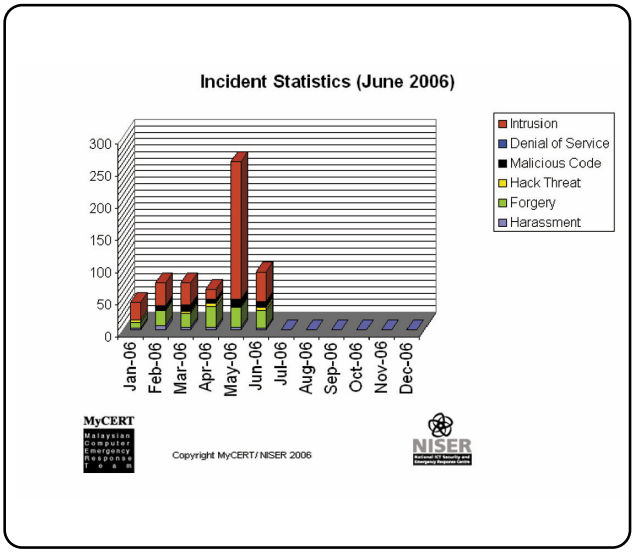
During this quarter, we did not receive any reports on denial of service incidents as was in previous quarter.

Conclusion

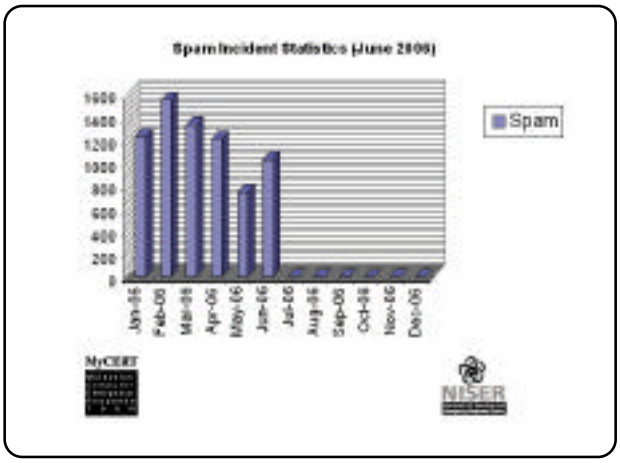
Overall, the number of incidents reported to us had somewhat decreased to about 20.98% compared to the previous quarter. Forgery, intrusion, malicious code and hack threat incidents continue to increase. Harassment related incidents had dropped while Denial-of-Service remained nil as was in previous quarter.

Generally, no crisis was observed this quarter. Nevertheless, we advise users and organizations to take measures to protect their systems and networks from security incidents. MyCERT also encourages users and organizations to report and seek assistance in the event of any security incidents.
Complete statistics on incidents reported to MyCERT by monthly are shown below:

Incident Statistics (June 2006)



Spam Incident Statistics (June 2006)



Dealing with dangers from within

Developments in Information and Communications Technology (ICT) and growing dependencies on information systems have made it more difficult to protect and defend confidential and critical data. And, if defending against intruders and their increasingly sophisticated and powerful tools isn't bad enough, ICT security professionals also have to deal with attacks involving people from within the organisation who already have access to the computer systems. These people take advantage of their knowledge and access privileges to infiltrate networks.

Apart from disgruntled employees wishing to express anger or outrage, these insiders may also have other intentions such as stealing information for competitors.

A report by U.S. Secret Service (USSS) & Computer Emergency Response Team Coordination Centre (CERT/CC) on cases between 1996 and 2002 shows that the highest cases involving insiders are sabotage, followed by fraud and information theft mostly in the banking and finance sectors [1].

These threats become greater with the increase in outsourcing programming that involve contractors or suppliers who have been given privileged access to critical information such as company accounts, employees data, system configurations, and others.

Carelessness also leads to certain unprivileged users gaining access to sensitive data after having obtained access information such as usernames and passwords. This is often done by "shoulder surfing" or watching for username and password pairs entered by other users.

Best Practices

Organisations should take preventative measures to protect against these threats before it harms the entire operation and employ certain best practices in the organisations. There are several recommendations that can and should be implemented by organisations:

- ***Screening the Employees***

Most of studies showed that employees become the greatest risks for the access facility they have. As such, organisations should screen or conduct a background check on the employees especially those who are responsible in areas with critical and confidential information by studying their background, work histories and perhaps, their personalities.

- ***Password and Account Management***

A strict password and account management policy should be implemented to ensure that only eligible personnel can access the network. Also, upon resignation or termination, a former employee's access account must be deactivated immediately.

- ***Security Awareness Training***

Employees should be aware of and understand the issues of information security in their organisations. Organisations should educate their staff on how their actions can threaten the enterprise. Periodic security awareness training is needed for the staff to increase the knowledge in information security such as desktop security and password management.

- ***Monitoring and Audit***

Organisations should employ system monitoring or logging to monitor and audit especially for employees who have privilege to access the system remotely, and ensure that no system irregularity or changes to sensitive information and data.

- ***Backup and Recovery***

To avoid the loss of important data due to accidental deletion or file corruption, a proper backup and recovery strategy should be implemented to ensure organisation's information systems are functioning even in the event of attack.

Conclusion

Threats from intruders within the organisation can cause plenty of damage to a company's computer systems, financial data, business operations and ultimately, reputation. As such, organisations should take preventative measures.

Without firm restrictions and policy enforcement, insider attacks can have far reaching and deeply devastating effects on any business.

REFERENCE

[1] Keeney, Michelle, Eileen Kowalski, Dawn Cappelli & Andrew Moore. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. May 2005. Carnegie Mellon University Software Engineering Institute's CERT Coordination Center and United States Secret Service. November 2005.
<www.cert.org/archive/pdf/insidercross051105.pdf>.

Accreditation for Information Security Laboratory

Introduction

Nowadays, there are many information security laboratory have been established in Malaysia for different purposes. Among them are security assessment, product assessment, common criteria and also digital forensics. These laboratories existence in the industry meet the current demand in ensuring the integrity of a product, a system or a test. Accordingly, the quality of the laboratory management system must also up the premier standards locally as well as internationally.

The most common standard in regard to laboratory in Malaysia is ISO/IEC 17025. This standard is under the responsibility of Department of Standard Malaysia (DSM), MOSTI. Currently, there is yet a specific standard tailors to the district of information security.

What is accreditation?

Accreditation is defined in ISO/IEC Guide 2 as a "procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks". In the case of laboratory accreditation, the tasks are tests or specific types of tests.

What is ISO 17025?

ISO 17025 Laboratory Accreditation is the requirements for laboratories to conform in demonstrating that they are technically competent and effectively operate a quality management system. Besides that, the laboratory should also be capable and competent to provide scientifically sound and valid calibration or testing services as documented on its scope of accreditation and on the calibration certificates and/or test reports it issues.

This standard applies to any organization that wants to assure its customers of its precision, accuracy and repeatability of results. It also includes in-house laboratories where confidence of results is at the highest priority. This standard was developed specifically to give guidance to lab managers on both quality management and the technical requirements for the proper operation of a laboratory.

Why accredited?

- ***Recognition & status to the laboratory***
  Accreditation gives formal recognition to competent laboratories, thus providing options for consumers to choose reliable testing and calibration centers. This recognition needs to be maintained through reassessment periodically by the accreditation body to ensure their continued compliance with requirements, and to check that their standard of operation is being maintained.

- ***Eliminates costs***
  Accredited laboratories receive a form of international recognition, which allows their data to be more readily accepted in the global markets. This is done through a system of international agreements, the Mutual Recognition Arrangement (MRA). Thus, the cost of retesting can be eliminated since manufacturers and exporters have their products or materials tested in accredited laboratories.

- ***Assurance of competency and performance***
  The accreditation reinforces the laboratory to operate a quality system by technically competent analyst to produce technically valid results. Lab personnel are required to be properly qualified and trained in addition to the ongoing commitment to high quality. Laboratory accreditation is highly regarded both nationally and internationally as a reliable indicator of technical competence.

- ***Increase competitiveness and market share:***
  Because of changes in the regulatory environment and the increasing internationalization of the marketplace, laboratory accreditation that can be recognized around the world will soon be counted as one of the keys to corporate survival. Accreditation affirms the competency of the lab to perform certain processes and tasks consistently.

Conclusion

Towards the era of globalization, it is crucial for information security industry to remain competitive at the international level. Being accredited is a strategic approach to be renowned and recognized worldwide. Details of the ISO 17025 will be elaborated in details in the next issue.

How to Develope & Implement Legal Strategies in IT Security Management

1.1 INTRODUCTION

This Chapter builds on the overview in Part I and seeks to introduce the basic steps in developing a strategy in managing legal issues in IT security management

The ability to develop a sound legal strategy in IT security is a must for security professionals. In IT security, having a legal strategy is about understanding the legal risk environment in the provision of IT security services and defining where the enterprise would want to go in the long term and how it is going to get there. Developing a legal strategy is about understanding the legal processes involved and how an organization can avoid potential legal pitfalls by proactively positioning the organization to deal with such legal risk exposures.

There are essentially three levels of legal management:

(1) Strategic;
(2) Tactical; and
(3) Operational level.

Strategic legal management requires the management team in an organization to look at the bigger picture and understand its business as well as legal impact in both the short and long term particularly the legislative or policy environment in a particular jurisdiction that would impact the organization business performance, competitive edge and legal risk liabilities. For instance, at the strategic level, legal advisors in the field of IT security will look at emerging areas of such as downstream liability[1]

The tactical level of legal risk management including deal and document structuring. A typical example would be a legal decision that needs to be made in terms of how the business deal is going to be structured. For example, when digital assets such as intellectual property in digital format (music in electronic form or text in html[2]) needs to be protected, the lawyers need to decide if this form of protection requires a separate legal agreement with different parties and not simply provisions which are buried in some obscure pages in a thick bundle of legal agreement.

[1] The concept of downstream liability simply means the extent a party is legally responsible to others with whom that party has no legal relationship or privity of contract. Thus if Company A is careless in securing its IT infrastructure and a hacker uses this weak system as a staging area to attack Company B, Company B may have a legal basis to sue Company for its negligence on the basis of what is being called "downstream liability". Company B may want to sue Company A perhaps because the latter is partly responsible or perhaps Company A is a company with more money instead of going after the hacker! The concept of downstream liability is not established law in many countries but it is an evolving area of law.

[2] HTML means hyper-text mark up language, the language in which text on website are created.

The operational level involves the drafting of specific agreements right down to the review of specific clauses in legal agreements both online as well as in physical form. The operational level of legal risk management would include for example the day to day management of processes such as handling requests to draft the terms and conditions of email security policies to minimize if not to avoid potential legal risk liabilities on the part of the organization.

Bearing in mind these three levels of legal management, one can now start to plan the substance of what is being managed legally. At the end of the day, it is all about management of legal liability risks. Nothing is more important than protecting oneself against possible suit by others that may result in financial loss. Strategic legal risk management like other areas of management needs to be measurable in order for one to see whether it is working or not. As they say, what you cannot measure, you cannot manage! So in strategic legal risk management, the success of such a strategy must be measurable by, for example, by having a scorecard or some kind of numbers (no matter how imprecise) to measure how much costs have been avoided or saved because your legal risk avoidance or legal risk mitigation strategy has worked to prevent liability on the part of the organization.

1.1.1 Objectives of IT Security: Legal Implications

In developing effective legal strategies in IT security, we begin with the fundamentals. The principal objective of IT security is to protect and assure the confidentiality, integrity, and availability of information systems and the data contained in such system. If a subject circumvents confidentiality measures designed to prevent its access to an object, the object is said to be "compromised."

Integrity measures in turn are meant to protect data from unauthorized modification. The integrity of an object can be evaluated by comparing its current state to its original or intended state. An object which has been modified by a subject without proper authorization is said to be "corrupted". Finally, availability means having an information system and its associated objects accessible and functional when needed by its users. Attacks against availability are called denial of service attacks.

The development of legal strategies in IT security is driven by the need to establish a legal risk management framework that would ultimately assure the organization of the confidentiality, integrity and availability of information system through legal risk avoidance or mitigation. In developing such a strategy, an organization typically begins by reviewing its legal risk environment that poses threats to confidentiality, integrity and availability.

For example, an Internet banking enterprise may rank reputational risk above all others and it may seek to ensure that it develops a management framework that addresses the critical area of customer confidence in the bank's system to ensure confidentiality. In such a scenario, the bank may develop a legal policy environment and a legal framework that seeks to ensure that the organization's reputation is safeguarded as a top corporate priority. If this Internet banking enterprise seeks to brand itself as a top-notch bank that provides blue chip IT security services to its customers, legal objectives and processes must then be in place to achieve this. In order to get there, this enterprise for example may decide that acceptance of a pro-customer security policy and the necessary support legal documentation must take precedence over a legal framework that is driven by the need to avoid all forms of liability for any form of security breaches.

Another enterprise may place protection and commercial exploitation of its business intellectual property, for example, patentable software as a key driver in its business model. If this is the vision of the enterprise, the legal counsel in the company or its external legal advisers must then set the necessary legal framework and processes to achieve such vision. In this scenario, the enterprise will give top priority to legal documentation and processes that focus on asset protection including providing a sound and effective system to protect, manage and exploit such assets commercially. The enterprise may take, for example, an offensive policy to assert its rights by suing others. In other circumstances, the enterprise may be sued by others and therefore requiring it to take a defensive posture.

1.1.2 Where does one start?

In developing sound strategic legal risk management policies at the enterprise level, a good starting point is to develop an overall framework and to start thinking of the methods and processes involved as a map that the team involved can follow to achieve success. If such a framework is developed at the enterprise level and involving every key stakeholder in the enterprise, there is a higher likelihood of ensuring strategic success.Like the formulation of any broad strategy, the three distinct phases in developing a new legal strategy typically involves:

(1) Analysis;
(2) Planning; and
(3) Implementation.

In analyzing the legal risk environment, the key issue that enterprise must address often boils down to the management of legal risk liability, that is, it is a bottom line issue. Legal risk liabilities will direct impact financial liabilities such as when an enterprise is sued for damages. The question is always how an enterprise (or a director in his personal capacity) can ensure that it does not get sued by another party and how it can sue others when the enterprise's rights are violated.

1.2 DESIGNING A LEGAL RISK MANAGEMENT FRAMEWORK

In designing the overall legal risk management framework, enterprises should, as a general rule, have a proactive and structured program of action involving the following elements:

(1) An overall system to identify, classify, measure, prioritize and assess legal risks that are relevant to the enterprise's operations;
(2) A plan that is documented in the form of operation manual (both hard copy and embedded into the system in the form of web-based documents containing policies, practices and procedures that addresses and controls these risks. Such a plan must specify the responsibilities of all parties involved in the whole risk management process from the operational level right up to the CEO;
(3) A regular test plan that when implemented approximates all possible worst-case scenarios for the purpose of testing the system to its fullest potential;
(4) Monitoring program to assess all types of technology and other operational risks and the evaluation of the effectiveness of such program;
(5) Updating such plans in the light of developments in the technology, law and business practices;
(6) Post-incident recovery procedures which must incorporate digital evidence collection, preservation and presentment techniques which are legally compliant;
(7) Fulfillment of legal compliance requirements as specified by the regulatory bodies; and
(8) Security awareness program that will help nurture a more security conscious environment.

See Figure 1.

1.3 LEGAL AUDIT

In designing this legal risk management framework, it is best to start with an audit. This phase involves the senior management in the enterprise and the legal team doing an audit on the adequacy of legal strategies, legal documentation and work procedures and

of legal strategies, legal documentation and work procedures and guidelines that affect the day to day legal management of Internet commerce services. Examples of issues that are usually addressed during the audit include:

(1) The overall legal strategy to handle legal risks that are technology-driven and the objectives and plans currently guiding the enterprise in the area of technology risk management;
(2) An assessment of the legal compliance environment as well as the developments in the legal standard of care in providing security services to protect the enterprise from intrusions or such other forms of attack;
(3) The form and effectiveness of the enterprise's legal standard operating procedures and guidelines and the general organization and administration of legal matters;
(4) Legal cost and economics, for example the cost benefit analysis of getting external lawyers to advise on the legal issues that the enterprise is currently addressing;
(5) Legal department resources and capabilities, i.e., strengths and weaknesses, as related to resources, reputation, services and legal market position. Issues that need to be addressed include whether existing lawyers who are competent in the traditional type of commercial activities such as loan document preparation are competent to handle IT-related legal liability issues for example in the area of security breaches in Internet commerce; and
(6) A forecast of the technology and security risk environment and the legal consequences that flow from it that will affect the legal position of the enterprise and its clients.

TABLE 1

STEPS TO DEVELOPE A STRATEGIC LEGAL RISK MANAGMENT FRAMEWORK

STRATEGIZE	(1) Where is the organization now? (in terms of trustworthy computing environment, e-security exposure in both the short and long term) (2) Where does the organization want to go? (3) How does it get there?
SITUATION ANALYSIS	(1) Look at the big picture and analyze the overall risk environment including the impact of government legislation, policies, and regulations & overall policy environment & how that impacts the performance of the organization (2) Review corporate, industry and regulatory standards that impacts both security and legal risk liability (example compliance risks, risk of loss of intellectual property, downstream liability etc) (3) Analyze the overall internal corporate strategy, understand the needs of the management and the company & its impact on the legal risk environment (4) Understand your organization's strength & weaknesses (including competitive advantage, if any, in dealing with the legal risk exposures) addressing all aspects from strategy, tactics and ground execution (5) Review management practices & workflow that impacts legal risk liability (6) Review existing contracts and other arrangements (right down to the clause level)
RISK ASSESSMENT	(1) Develop an overall system to identify, classify, measure, prioritize and assess legal risks that are relevant to the enterprise's operations; (2) Identify the legal risks against the context of other risks & prioritize/rank the legal risks (3) Develop plans to mitigate or avoid legal risks at all level & seek third party counsel if necessary (4) Determine legal standard operating procedures and guidelines and the general organization and administration of legal matters

DEVELOP STRUCTUR & DEFINE SCOPE	(1) Focus on areas & set priorities (given limited resources) & integrate strategy with other corporate strategy (2) Develop the formal structure to manage the legal risks at all levels & communicate the strategy effectively (3) Determine project "owners" (4) Set timeline (5) Test the strategy (6) Determine key performance indicators
DETERMINE BUDGET	(1) Work out detailed budget (2) Work out cost-benefit analysis
IMPLEMENT	(1) Implement workflow for more effective legal risk management (2) Appoint personnel, particularly project owners (3) Draft & sign documents
MONITOR & REVIEW	(1) Audit (2) Monitor legal performance & review strategy

1.4 CONCLUSION

At the end of the day, e-security law & strategy is ultimately about how liability issues are managed when there are breaches of e-security. Enterprise must take reasonable steps to secure its information system. This demands a holistic and integrated approach that addresses not only at the technology, processes, administrative controls, procedural precautions but also a structured and proactive legal risk management framework not only within the enterprise's own systems, but also the systems of its networked partners and clients.

Introduction to Project Management

Project Management: The Big Picture

A project is implemented to achieve the organization's business objectives. Whereas business objectives are created to achieve the organization's strategic goals. Thus we could say that a project is also implemented to achieve organization's strategic goals.

What is a project to you? The definition given in PMI, 2004, ***a project is a temporary endeavor undertakes to create a unique product, service or a result.*** Example of a project is, building an office complex, developing a software program or auditing a system. ***Temporary*** meaning the project has definite beginning and definite end. ***Unique*** means a product that is distinguishing way from all other products. All definition where taken from PMI, 2004.

When a group of 2 or more projects being put control under one umbrella, the projects will become a program. There is no specific definition of a program. However, we could say that when many related projects who shares one specific goal could become a program. This program can be called as a mega projects for example building up an aircraft, or sending man to the moon.

There are few examples of a program.

Example 1: A group of related projects with a common objective to obtain benefits and control but could not be managed individually can also be a program (PMI, 2004).

Example 2: An on-going work after a project has been completed and launched can also be a program. An example of an on-going work is developing new model of a car including the manufacturing.

Example 3: Repetitive or cyclical projects such as newspaper and magazines.

Example 4: There are also projects which are not related has their own individual objective, however for a better control and convenience, there are managed in a coordinated way. For example, projects where delivered to a same client or multiple projects that share same resources.

The next definition would be a project portfolio. What do we know about project portfolio? We know that in each company, it has their own research and development unit or an IT unit that controls and monitor all network activities and maintenance of your company's network and of course a finance unit. These units have their own strategic business objectives. Every projects under these units will managed together to meet their strategic business objectives. Thus, a project portfolio is a collection of projects or programs that are being managed together to meet the unit strategic business objectives.

So what is a project management? Project management is an application of knowledge, tools, skills and techniques to the above defined project activities to meet the project requirement (PMI,2004). A project manager is a person who manages the project and will always face triple constraint which is project scope, time and cost. The project quality will be affected by these constraints. Project management office will consist of project managers and assistant if there is any, hand in hand managing the project including project planning which include project budget planning, duration, resources gathering and logistics.

Choosing a Project.

There are many ways, models and methodologies used when it comes to choosing a project. One of the models that I would like to share is called Funnel and Filters® Model. This model can be used in any 'end-to-end' life cycle of products or services process. There are three parts that made up the model. The parts are the head, the body and the leg. The illustration of the Funnel and Filters® Model are shown at figure one. The parts represent the phases that require us to follow in order to complete a project (PMBOK® Guide 2000 Edition). The phases are:

1. Initiation
2. Planning
3. Executing
4. Controlling
5. Closing.

The above 5 phases could be represented in three broad phases which are Initiation, Development and Production. In the illustration, any projects that enter the funnel at the top will go through the phases and moves along until it reach one point where it can be launched and officially closed.

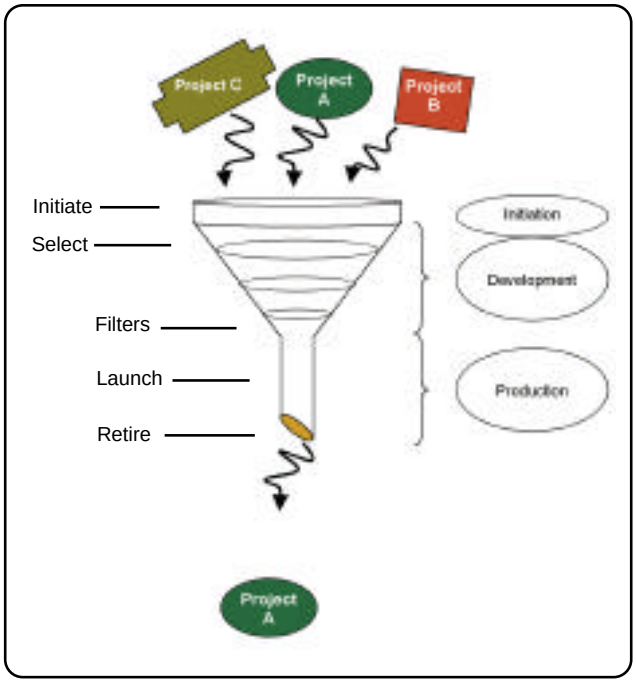


Figure 1

In the funnel, individual project will be managed to achieve its objectives and collectively the projects are managed to achieve the portfolios objectives.

For further understanding of the Funnel and Filters® Model, let us go through the phases one by one.

Initiation Phase

In the initiation phase, managers together hand in hand with the project management office will do the assessment, feasibility studies/analysis and the selection of the project. In this phase, project ideas are initiated and each idea is evaluated on its individual merit as well as how it stacks up against the other competing ideas. The ideas go through a filter(s) that screens out those projects that are not deem worthwhile. The Selected ideas become 'formal' projects and enter the next phase

Development Phase

The objective of this phase is to develop the product or service that is targeted to be launched. The development took place in this phase is characterized by four phases. The phases are;

1. Planning
2. Execution
3. Control
4. Closeout.

Thus together with the initiation phase, this will form the overall five-phase project life cycle, this is as illustrated in figure two below (PMBOK® Guide 2000 Edition).

1. Initiation
2. Planning
3. Execution
4. Control
5. Closeout.

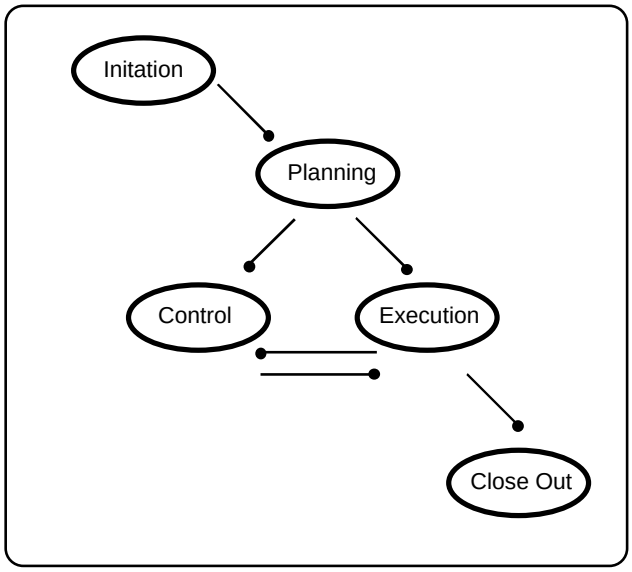


Figure 2: Linking among process group in phase (PMBOK® Guide 2000 Edition).

Throughout the development phase, the whole process may occur more then once. Each process is linked with each other by the results they produce. The process could also be overlapping with one another throughout the phase process. Finally, a close-out of a one phase could become the initiation of a next phase. For an example, a result of the design phase is an initiation for the implementation phase. Project Process is an article by it self. I will cover this in another time.

Let us go back to the Funnel and Filters® Model. Now, if you look back at the Funnel and Filters® Model figure one, you can find that the filters are aligned through out the development phase. Roles of filters represent the decision points made by the management. The first filter is where you select the right project. The second, third and forth filter is where we evaluate each project during the development. This will gives us decisions whether to remain, halt or terminate a project.

The filters will take place on regular cycle either semi-annual or annually when all the competing projects are evaluated at the same time for funding on their relative merit.

Generally, filters at head is to initial project selection as filters at the body of the funnel is where the project reprioritization and termination may be done after the project has been selected, funded and has made progress in the development phase.

Always remind yourself that filters is not a 'stage/gates™'. 'Stage/gates™' is decision points specific to individual project in the portfolio where by the objective is to control project life cycle from one phase to the next phase. Where by decision made at the filters in the funnel is to compete at relative merit with other projects in the portfolio for further funding.

Lastly, we have reached the final phase which is the production phase. The production phase is the final product lifecycle. Here as a result we have produced a complete product that could be sold and maintain. As for services, it could only be involved supporting. At the end of the product cycles, the product will be obsolete and no longer be sold or supported. This is where we call, a product "retires" from its life cycle.

Any product/services considered for improvement or enhancement will take it as a new idea and had to go through a new life cycle. The Funnel and Filters® will restart again.

Finally, there are few key points that we should consider which is, each project is initiated based on organization strategic goals. This are investment rather that to be treated as an expensive. Therefore a project portfolio is an approach that can be use effectively to get the best returns. Secondly, a project is a temporary endeavor undertakes to create a unique product, service or result. Lastly, services or product undergone through an end-to-end lifecycle can be characterized by three broad phases which are initiation, development and production.

Keeping Your Database Secure

In today's world a person needs a simple computer with an internet access to gain illegal access to a company's database where 90% of the organization's sensitive information is normally kept. As a result of such possibilities we will describe here some of the best techniques which can help improve the confidentiality and security of data.

This article discusses some of the numerous aspects of the architecture of a reliable database. The following topics are considered: Data Accessibility; Audit procedure, backup and restore strategy, encrypting of data, Insider attacks.

1. DATA ACCESSIBILITY:

Data accessibility is a major goal in database security. Many organizations can not work properly if databases are down. In other words they are mission-critical systems. To make the data available implies to provide the security mechanisms to ensure authentication, authorization and auditing procedures. Authentication means that user identity must be truly verified, commonly through a password only known to the user. This is a critical phase in the foundation of the security strategy. After this first step has been completed, the system must determine the resources that the particular user ID can have access to. This is the authorization phase and all the tasks involved are often referred to as user security administration. Finally, to detect possible intruders and ensure data integrity, auditing utilities must be activated.

While on routing from server to receiver, data passes through different devices where, if security policies have not been applied or are defective, a third-party can get access to the packets. This is potentially dangerous with some kind of information such as credit card numbers, payrolls, social security numbers, and medical records, to name but a few. Obviously, this is a security threat that must be taken into strong consideration. We must ensure that data can only be seen by the same individual we sent the data to while avoiding data corruption by a third party. To achieve the former, encryption must be applied. Data integrity is usually ensured by means of certificates and public key encryption. Another important aspect is non-repudiation. This is extremely important in e-business because it makes sure that a sender cannot deny to have sent the information.

2. AUDIT PROCEDURE:

In many databases, auditing procedures are often inactivated. This helps to avoid decreasing the performance of the system. This however results in an important consideration: there are no records to study any illegitimate activity in the database. This does not mean that recording everything is the optimum solution. Depending on the system nature, an intelligent auditing strategy can be built to highlight security problems whilemaintaining database performance.

Auditors can use audit software to achieve their audit objectives. One popular database auditing solution is DB Audit created by Soft Tree Technologies. This solution helps ease the problems associated with enabling the built-in audit utilities of most databases. DB Audit is easy to customize and does not require installation of any additional software or services on the database server and network. It works with Oracle, Microsoft SQL Server, Sybase ASE, Sybase ASA, and IBM DB2.

This solution is implemented on the database back-end and eliminates any possibility of back door access that would otherwise be unrecorded. The benefits of using a solution such as DB Audit are:

i. Totally transparent system-level and data-change auditing of any existing applications
ii. Improved system security and ensured system accountability
iii. Centralized auditing control of multiple database systems from a single location, and
iv. Audit trail details that are normally unavailable from standard audit utilities.

Database Audit has many useful tools to help the auditor, including pre-built analytical reports that help reduce large amounts of audit data and tools to create custom reports and report filters. The solution also alerts management when changes are made to data within the tables.

A perfect data access auditing solution would address the following six questions:

i. Who accessed the data?
ii. When?
iii. Using what computer program or client software?
iv. From what location on the network?
v. What was the SQL query that accessed the data?
vi. Was it successful; and if so, how many rows of data were retrieved?

3. BACKUP AND RESTORE STRATEGY

A database backup strategy should be customized for the environment. It should take into consideration the system workload, usage schedule, importance of data, and hardware environment of the database. But there are some guidelines that apply to all databases. Incorporating these guidelines into the strategy will ensure more reliable and more cost effective backups. Here are the guidelines.

- Always maintain a log of your backup schedule
- Occasionally store backups in a separate location
- Spread your database across several disks
- Always consider your existing hardware configuration and system workload
- Determine the volatility and value of your data
- Verify the integrity of your database regularly
- Verify the integrity of your backup media after each backup

4. ENCRYPTING DATA:

Encryption in database will render data in storage or in transit to be meaningless to the unauthorized user. Illegal leaking of such data will not compromise protection of the database, as such; cryptographic controls can take a lion's share where access, flow, and inference controls cannot.

It adds an important layer of protection that enforces security. Any user trying to access the data not only needs the right password, but the encryption key as well. One advantage of this schema is that files can be unreadable to people that have access to the database, such as a system administrator, but no databases privileges. Database encryption affects performance and a compromise solution must be found between performance and security, only encrypting tables, or columns with sensitive information.

5. INSIDER ATTACKS:

It is thought that most of the attacks come from outside but, in the real world, a large percentage of the security breaking incidents are made by insiders, people working in the same organization with extra knowledge about the database structure and security policy. It is estimated that 50% of identity theft cases are committed by employees within the organization who have access to the database.

If proper security recommendations are followed, damage caused by insider's activities can be limited and audited. Right security policies largely decrease risks by reducing vulnerabilities and strengthening defenses and countermeasures. A database server with important information is tempting for many people and appropriate measures have to be taken. They include the physical security of the server and the number of people accessing it.

CONCLUSION

The solutions shown above try to guarantee, in the greater degree, as much as possible, both database and data security. The importance to do so has been also highlighted and there is a general recognition that these methods must be applied in the highest level, mostly in databases with very sensitive information. Availability of funds to apply a good security policy is an important feature, but human factor is also essential. Good Database administrators and security managers can handle system resources and improve security by applying some basic low-cost techniques, reducing vulnerabilities and eliminating backdoors. In summary we cannot eliminate risks but we can manage them properly.

REFERENCES

i. BrainTree. "Client/Server Database Security". URL: http://www.bti.com/Whitepapers/3-Tier_Data..._down2/Cswp.pdf

ii. ISS. "Network and Host-based Vulnerability Assessment". URL: http://www.iss.net/prod/whitepapers/nva.pdf

iii. ISS. "Secure E-business". URL: http://www.iss.com/prod/whitepapers/securityebus.pdf

iv. ISS. "Securing Database Servers". URL: http://documents.iss.net/whitepapers/securedbs.pdf

v. Le Tocq, Chris & Young, Steve. "SET Comparative Performance Analysis". 2 Nov 1998. URL: http://www.setco.org/download/setco6.pdf

vi. Legato. "Manager's Guide to Informix Database Protection". URL: http://www.iqproducts.de/iqproducts/whitep...de_informix.pdf

vii. Mattsson, Ulf. "Secure Data Technology Overview". 27 Apr 2001. URL: http://education.protegrity.com/downloads/...eData_IBMv1.pdf

viii. Pentasafe Security Technologies, Inc. "Common Vulnerabilities in Database Security". May 2001. URL: http://www.pentasafe.com/whitepapers/penta...erabilities.pdf

ix. Sybase Inc. "What Backup, Recovery, and Disaster Recovery Mean to Your Adaptive Server Anywhere Databases". 15 Jun1999. URL: http://www.sybase.com/detail/1,3693,47877,00.html

x. Turner, Tom. "Securing the Database: What are the Issues?" URL: http://www.itaudit.org/forum/security/f218se.htm

Noise (audio)

Noise is the unwanted sounds that exist inside audio recordings such as clicks, hiss and static. Its presence is unavoidable no matter how professionally the audio recording process is done. Audio noise presence is more obvious inside an analog recording as compared to digital.

Audio noise only becomes a problem if it was produced within a human listening range (20Hz-20KHz). Otherwise its existence can be masked by other louder elements.

Distortion is similar to noise except distortion has some key characteristics. Audio noise is something that is produced by an outside signal such as a hum. Meanwhile distortion is the signal modification (special effects) on the signal itself.

Types of Noise

The ability to recognize the types of noise is also crucial for audio forensics analysts whilst performing audio restoration process. This will help audio forensics analysts, as they can plan their audio restoration strategy before performing any audio restoration processes.

Broadband Noise

Broadband noise is also known as continuous noise, such as hiss and static that is present at all frequencies, at a given range. In every audio recording there will be a certain amount of broadband noise albeit it was done by professional audio engineers using high-end equipments.

Narrowband Noise

This refers to a sound which occupies a narrow range of frequencies such as hums or buzzes as opposed to broadband or wideband noise. Hums are usually caused by incorrect grounding and poorly shielded cables.

Thermal Noise

It's produced from the electronic circuit itself and impossible to eliminate. However it can be minimized by using added quality components such found inside a high-end sound cards and audio interfaces.

Impulse Noise

It includes a short and sharp sound like clicks and pops. Clicks usually are introduced by minor scratch or small mark caused by dust on a record or CD. Usually it's gathered during recording sessions when digital device is not synchronized. Pops appear due to bad scratch. When the recording is opened in a waveform editor, these clicks and pops will appear like a sharp spike or a deep gap.

Click is distinguished with a narrow spike and might even span a few samples (A sample or data point on a standard CD resolution is 1/44100 per second). Pop is formed by multiple clicks in a row.

Irregular Noise

Irregular Noise includes sound such as background conversation, traffic and rain. These sounds are near impossible to eliminate owing to the fact that they were formed by multiple random sounds in dissimilar frequencies and decibels.

Conclusion

The Objective of Audio restoration process is aimed to significantly reduce noise inside an audio recording at a minimal level possible. Audio restoration processes require very much the use Audio Forensics analysts, as long as it involves eliminating various types of audio filters and noise elimination.

Safeguarding Against Email/ Phishing Attemps

1) Identifying phishing/fraudulent attempts:

a) Legitimate online businesses will never ask you for sensitive personal information such as passwords, bank account or credit card numbers, PIN numbers, or Social Security numbers via e-mail. So, if you were asked to reveal this information online, this may be a fraudulent attempt.

b) Phishers normally use convincing messages to ask users to go to their websites and enter personal/sensitive information on the phishing website. It would be advisable to scan the types of messages contained in the email prior to visiting the websites.

Among messages to be cautious of are as follows:

• Security or server updates, maintenance upgrades, online banking problems

• Billing information requests or billing issues

• Official or urgent notices

• Account updates e-mail or account verification requests

• Consumer alerts, customer warnings

• Your account has been, or may be, suspended or needs to be reactivated

• Problems with your account, errors found

• Suspicious transactions, fraud investigation, unusual activity

• Someone sent you money, payment acknowledgments, order confirmations, lottery wins, jackpot wins, competition wins

• Requests for assistance with fund transfers (the infamous 'Nigerian' scam)

• Offers of advice on how to protect yourself from fraudulent transactions, identity theft solutions

c) The phishing email does not address a user by his/her name.

d) No confirmation of the company that does business with you, such as referencing a partial account number.

e) The email warns that your account will be shut down unless you reconfirm your financial information.

f) Spelling or grammatical errors in the phishing emails.

2) Avoiding phishing attempts

a) Do not respond to e-mails requesting for your personal information. Legitimate companies do not ask their customers for confidential information, such as passwords and account numbers, though e-mail.

b) Do not open attachments or download files. Phishers can use these files to infect your computer with a virus or spy ware.

c) Do not click on links provided in e-mails. If you are uncertain about a website address that appears in an e-mail, go to your browser and enter the legitimate address manually. Phishers can use links to point recipients to a "spoofed" site, using an address similar to a real bank's URL. If in doubt, phone the business in question. Use a phone number that you have obtained from a reliable source, and not from the suspected e-mail.

d) Do secure your computer. Uses updated anti-virus software, personal firewalls and apply latest security patches for your operating system and browser to secure your system from unwanted incidents. Anti-spam software can also help stop phishing e-mails from getting into your inbox. Some phishing e-mail may try to release a virus onto your computer.

Internet Explorer (IE) users can download a special patch to protect against certain phishing schemes.

The download is available at:
www.microsoft.com/security/

e) Do report suspicious e-mails to the legitimate company, to your Internet Service Provider (ISP) or to your Computer Emergency Response Team (CERT).

f) Do review your credit card and bank statements regularly to check for errors or unauthorized transactions. If anything looks suspicious, do contact your bank and all card issuers.

g) Do install a Web browser tool bar to help protect you from known phishing fraud websites.

EarthLink ScamBlocker is part of a free browser toolbar that alerts you before you visit a page that's on Earthlink's list of known fraudulent phisher Web sites.

Free download is available at:
http://www.earthlink.net/earthlinktoolbar

h) Do consider protecting yourself from dangerous scripts and spammers and phishers. Software such as the latest version of Outlook Express does make it much easier to do this.

3) Reporting a phishing case

Upon receipt of a report from user, Malaysian Computer Emergency Response Team (MyCERT) will perform below:

a) Verify the existence of the reported phishing site and check if the phishing site is still online or offline.

b) Find out the administrator/location of the Internet Protocol (IP) address where the phishing site is hosted by using 'whois' search tools. 'Whois' is an Internet database that provides information on a person or an organization.

c) Communicate with the administrator of the IP to shutdown the phishing site immediately, within 3 hours if the phishing site is hosted locally and within 24 hours if the phishing site is hosted overseas. For phishing sites hosted overseas, a copy of the notification will be carbon copied to the respective CERT of the country.

d) Monitor the phising sites from time to time if it is still online after notifying the relevant parties, locally and overseas. If it is still online, we shall send reminders to the respective parties.

e) Phishing sites that are not shutdown within 24 hours of notification, particularly the ones hosted on foreign servers, will be referred to the Law Enforcement Agency, the Malaysian Communications and Multimedia Commissions (MCMC), for further action.

Rootkits and Its Growing Underlying Danger

In just three short years, the use of stealth techniques in malicious software (malware) has grown by more than 600 percent. The shocking increase has indicated that rootkits are a pervasive and evasive threat to today's systems. With its increasingly sophisticated stealth techniques, the detection of rootkits and stopping the damage becomes significantly challenging

The History of Stealth Malware (a.k.a Rootkits)

Originally, a rootkit was simply a collection of tools that enabled administrator-level access (also known as ***root*** access in the Unix world) to a computer or network. The term referred to a set of recompiled Unix tools, including ***ps, netstat, ls,*** and ***passwd***. The term rootkit became associated with stealth because the same tools could be used by an attacker to hide any trace of intrusion. When these same strategies were applied to the Windows environment, the rootkit name transferred with them. Today, rootkit is a term commonly used to describe malware – such as Trojan, worms and viruses – that actively conceals its existence and actions from users and other system processes.

The practice of hiding malware from the prying eyes of users and security products dates back to the very first PC virus, ***Brain***[1], which was released in 1989. ***Brain*** escaped detection by intercepting PC boot-sector interrogations and redirecting the read operations to elsewhere on the disk. Virus authors soon recognised that the longevity of any virus was critically dependent upon such stealth techniques when, in 1987, the ***Lehigh*** virus[2] was quickly contained after its release because it made no such attempt to hide its presence.

Malware authors continued to develop ever more complex DOS viruses throughout the late 1980s and early 1990s, adding innovative stealth techniques to mask detection. The advent of the Internet brought new opportunities and capabilities to both attackers and

[1] Brain, ***http://vil.nai.com/vil/content/v_221.htm***
[2] Lehigh, ***http://vil.nai.com/vil/content/v705.htm***

defenders. For malware authors, it added new propagation vectors and masses of exploitable victims. For system defenders, it provided new means of real-time network detection with intrusion prevention system (IPS) devices and other traffic-monitoring equipment to watch for the telltale signs of malicious activity.

Rootkits, Malwares

Malware comes in may form. There are, however, differences between viruses, Trojans, worms and potentially unwanted programs (PUPs). Viruses, like their biological analogues, are self-replicating programs that can also steal confidential information, block system resources, destroy information or perform other malicious acts. Trojans are programs that appear to be benign or even useful software applications on the surface but harbour malicious code within. While Trojans are not self-replicating, they can cause an infected computer to download other malware that is. Worms are malware that replicate by spreading copies of themselves through a shared network, floppy drives or even USB drives, often autonomously without human intervention. Although similar to Trojans and other malware in that they often steal confidential and private information, PUPs are distinct because they are installed and executed with the tacit approval of the user.

Stealth technology, however, is not the exclusive domain of malware. PUPs and commercial software applications are increasingly employing stealth technologies to prevent their removal. In April 2005, ***Adware-Isearch***[3] was one the first adware found to use stealth technology. Since then, several others have been discovered, including ***Apropos***[4]***, Qoolaid***[5] and ***DigitalNames***[6] all of which were reclassified as Trojans because they posed a significant threat to the user.

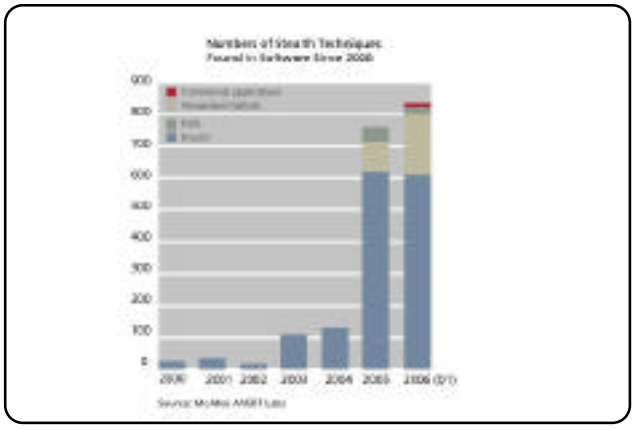
Rootkit Technology Trends

[3] Adware-Isearch, ***http://vil.nai.com/vil/content/v_133320.htm***
[4] Apropos, ***http://vil.nai.com/vil/contents/v_137345.htm***
[5] Qoolaid, ***http://vil.nai.com/vil/content/v_126149.htm***
[6] DigitalNames, ***http://vil.nai.com/vil/content/v_135063.htm***

In this section, we explore the reasoning behind the increase in rootkit adoption and diversity, the motivation driving rootkit writers and the technology trends that will shape the future of rootkits.

Trend 1: Rootkits spread beyond Trojans to other forms of malware and PUPs

Over the past three yeas, the incidence rate of stealth technology in malware, PUPs and commercial applications has more than sextupled. As Graph 1 shows, the use of stealth technologies was no longer the exclusive domain of Trojans in 2005, turning up in other forms of malware, as well as PUPs and commercial applications.



The sudden rise of stealth technologies may be attributable to online collaborative research efforts. Websites, such as www.rookit.com, contain hundred of lines of rootkit code. All of it, plus binary executables, are readily available for injection into malware. Several rootkits observed in the wild are directly borrowed or rootkits observed in the wild are directly borrowed or modified from the stealth technologies found on these Web sites. Some examples include ***AFXrootkit, NTRootkit, FURootkit, He4Hook*** and ***PWS_Progent.*** Even worse, blog entries found on the sites sometimes go as far as teaching readers how to evade virus scan detection by compiling source code themselves.

Trend 2: Rootkit sophistication is increasing

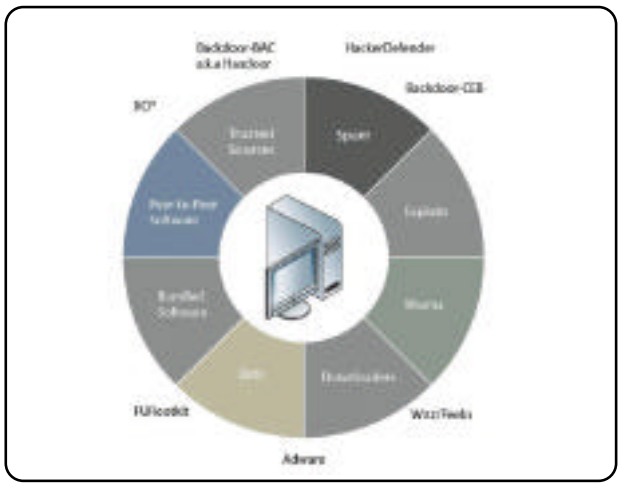
Collaboration does more than just spread stealth technologies. It also fosters the development of new and more sophisticated stealth techniques. One measure of complexity is the number of component files in a software package. For example, if a rootkit package named ***a.exe*** installs the files ***b.exe, c.dll*** and ***d.sys*** in which ***d.sys*** installs the rootkit's stealth component; the total number of components is counted as four. The complexity of known rootkits over the past six years has increased by nearly 200 percent in 2005.

Trend 3: Embedded Windows rootkits become dominant

Most of the rootkit activity observed today is targeted at the Windows platform. After peaking at nearly 70 percent in 2001, Linux-based stealth activity is now negligible. While Linux-based rootkits will almost certainly remain, Windows-based rootkits will clearly dominate the landscape for the foreseeable future, due primarily to the popularity of Windows and the technical challenge resented by the many undocumented Windows APIs.

Trend 4: Rootkit attack vectors found in both illegitimate and legitimate software

The versatility of stealth technologies has driven their spread into nearly every known malware attack vector. Their popularity has even convinced commercial software vendors to begin employing them in their products.



As seen in Figure 1, stealth technology injection vectors now span the spectrum of software delivery methods from exploits that require no user interaction to user-installed, trusted applications. Some examples of well-know rootkits and their attack vectors demonstrate this broad coverage.

Most recently, stealth technologies have spread through commercial software vectors, that is, trusted programs – as seen with the distribution of XCP[1]. Most users unknowingly permitted the installation of ***XCP***'s stealth technology on their systems because they trusted the application and wanted to listen to copyrighted music on Sony CDs. In doing so, however, they created serious security vulnerabilities.

[1] XCP, ***http://vil.nai.com/vil/content/v_136855.htm***

Trend 5: Embedding stealth technology becomes easier

With the availability of rootkit code and stealth-creation kits, malware authors can easily hide processes, files and registries, without detailed knowledge of the target operating system. It is easy to do so as the stealth-creation kit ***Nuclear Rootkit***'s user interface simply requires a file or directory name and with a click, uses various stealth techniques to create binary code that hides the file or directory as well as ports, processes and registry entries.

Although some of the stealth-creation kit shown above is freely available for download, anyone can also buy highly complex and custom stealth-creation kits, such as ***A-311 Death*** and the gold edition of ***Hacker Defender***, for prices that range from USD200 to USD2,000. The implications of this easy access were highlighted by ***Backdoor-BAC***'s (alias ***Haxdoor*** and ***A-311 Death)*** phishing success. The Trojan was able to gather thousands of bank personal identification numbers (PINs), passwords and other sensitive information for its author.[1]

Motivated by financial rewards and faced with relatively inexpensive start-up costs, hackers and malware authors continue to write new rootkits that evade detection by anti-virus scanners and other security products. The online collaboration of these malefactors presents a significant challenge to the security community as the increasing sophistication of their malware makes it even harder to prevent, detect and remove these malicious programs.

The Future

In 2004, McAfee recorded approximately 15,000 Trojans out of which only 0.87 percent was Windows rootkits. In 2005, McAfee saw approximately 30,000 Trojans, but this time rootkits comprised a much more significant chunk, nearly two percent, corresponding to a nominal growth rate of almost 400 percent. Across all malware and PUPs, McAfee has seen a more than 900 percent year-over-year increase in rootkit components submitted in the first quarter of 2006.

[1] Backdoor-BAC.gen, ***http://vil.nai.com/vil/content/v_138676.htm***

Although a new version of Windows (Vista) is expected soon, any drop in malware activity that might accompany its release – comparable, for example, to the lull witnessed with the release of Windows 95 – would not be expected until widespread adoption had taken place. Thus, with the ease of deployment and growing popularity of rootkits among malware authors, we can predict that, in the coming two to three year, the growth of rootkits for the current Windows architecture will reach an annual rate of at least 650 percent and that new and more cunning techniques will likely be introduced.

Why companies must take a closer look at Intrusion Prevention Systems

Although the IT department takes full responsibility for warding off network intrusions, the impact of any attack is often felt throughout an organization today – both in the direct costs of repairing the damage, and in the indirect costs which are incurred when corporate resources are "down".Attacks on the IT network system are getting more sophisticated. To make matters worse, the network threats have moved from predictable front door attacks to all sorts of internal and external, wired and wireless, direct and indirect assaults.

Whether these are virus or worm infestations, denial of service floods, spyware, or active hacking by individuals, it almost does not matter. "Downtime" means "Out of Action" – your business will lose money, the only question is, "How much?"

IDS is not enough

In our previous article, we highlighted that Intrusion Detection System (IDS) has several limitations. When the IDS determines that an attack is taking place, it uses this report generation system to provide console warnings, emails, and even SMS or paged alert messages to system administrators. However by the time warnings are issued, it is too late to do anything but shut the infected system or network down. What's needed is a system that can take a much more ***proactive*** approach to network security. Cataloging and recognizing known attacks are essential, but the only way to truly stay ahead of the security game is to become more predictive and intelligent about blocking attacks.

This can be achieved with Intrusion Prevention System or IPS. An Intrusion Prevention System differs from firewalls, anti-virus software and IDS by proactively inspecting all traffic through Layer 7 and blocking malicious traffic. An IPS is a complement – a necessary complement in our opinion – to your existing security systems, and provides the next level of protection available to companies today.

Making the Business Case for IPS

Every firm should have an IPS front-ending its network. Take the case of consultancy company Telechoice. Prior to the installation of an intrusion prevention system within its corporate network, the organization had to deal with a number of debilitating network attacks which decreased performance, subjected its corporate data to compromise and on several occasions brought their entire network offline.Even with a diligent IT staff, up-to-date server and anti-virus patches, and a top-of-the-line firewall system in place, the firm was unable to keep even their relatively small network (2 main internet connections, less than a dozen servers publicly exposed to the Internet) protected.The installation of an IPS system provided the solution to stem this tide – Telechoice's network has had zero outages related to intrusions since the installation over a year ago. And this record has been maintained in the face of a growing number of intrusion attempts.In fact, in a one month period last year, its IPS blocked nearly 4,900 unique attempts. This is an average of over 170 attacks a day, and on some days the number of attacks spiked to nearly 500.

Any one of these attacks, if successful, could have costed them thousands of dollars in lost productivity, IT staff time and network downtime.

IPS: Heart of the corporate network

At its heart, installing an IPS in a corporate network is, like any capital investment in IT, a business, and not a technical decision. And like any business decision, an investment must provide some payback in order to be worth considering.

The business case for IPS can be made clearly based upon two factors:

• The costs associated with the repair and "clean-up" of compromised systems• The loss of core business productivity and production caused by an attack on the network.Cleaning a compromised system can take a very smart server tech between a day and week in time/labor depending on the type of infection. That can add up quickly when you are faced with an average cost of 40 or more dollars per hour for a system admin to perform major repairs (like rebuilding an affected server).Take, as an example, the case of a large enterprise with 1000 workstations and 50 servers (providing email, messaging, file storage and application services). In a typical instance, a single worm attack that spreads throughout this enterprise could infect a quarter of these servers and 30 percent of these workstations.A conservative estimate for repairing such damage – based upon eight hours of system administration time to rebuild an infected server, and two hours to rebuild a workstation – would put the cost of a single incident in this sample enterprise over US$4,000 for the server and the cost of repairing workstations could be as high as US$24,000.

This figure does not include the costs of patching unaffected systems, nor does it account for overtime or other expenses incurred when the infection occurs after hours or on a weekend/ holiday. It also does not include the lost time of the IT staff doing other business strategic tasks for the firm. And this figure, remember, is for a single incident – many enterprises face such incidents multiple times per year.The costs of IT staff time are

not the only expenses incurred during such a security breach. The lost time and productivity of the corporation's staff during such an outage must also be accounted for.Then there are all the hard-to-estimate costs of an outage – employee disdain for IT, the time involved in each employee resetting all of their cookies and other program settings, that lost file that each was working on when the shutdown occurred, etc. We have not included those in this analysis, but sometimes these are the most expensive aspects of any outage!

This leaves a good, per-incident estimate in losses at nearly US$50,000 — losses that could, in most cases, be eliminated by the introduction of an IPS defense in the corporate network. The cost of an IPS deployment to protect upon such attacks varies from network to network – we typically recommend that an enterprise deploy an IPS system at each outbound network connection point, and some networks may segment internally and apply additional IPS resources at those segmentation points.If you work it out, the cost of an IPS could easily be paid back if it prevented only one or two of the incidents we have described above. And you will not be facing only one or two such incidents; even a smaller enterprise will be facing thousands of such potential intrusions every month.**The Bottom Line**

IPS is an essential part of a comprehensive security strategy for any networked business. The difference that IPS brings to the table is its proactive approach to security. IPS is not simply a static system that fights "yesterday's wars" by attempting to filter out known threats. Nor is it a passive system that warns your network administration after an attack is already underway.

Instead, IPS actively examines your incoming and outgoing traffic and uses a variety of filters, patterns, and algorithms to examine every packet and to make intelligent decisions about the threat level of those packets. IPS then automatically takes timely actions to block those threats without requiring a complete takedown of your network.

If your business is exposed to the Internet, and you value your security, IPS should be the next cornerstone in your security strategy.

The New Version of Common Criteria ISO/IEC 15408

Common Criteria (CC) is an international standard known as ISO/IEC 15408:2005 Evaluation Criteria for Information Technology Security. CC and the related Common Evaluation Methodology (CEM) also known as ISO/IEC 18045 are used as guidelines to develop ICT product with high confidence in security where it provides assurance in the process of specifying, developing and evaluating an ICT product in an accurate manner.

CC describes a framework where the users specify their security requirements in a document known as Protection Profile (PP). Then the developers develop a document call Security Target (ST) to make claims on the security attributes of their products based on the Protection Profile (PP). Lastly, the evaluators will use the Common Evaluation Methodology (CEM) as guideline to evaluate the products to determine if the products meet the developers' claims. CC guarantees that the certified products will provide a confidence that security measures are appropriate to meet a given threats and they are implemented correctly.

History

The CC was developed by the governments of Canada, France, Germany, the Netherlands, United Kingdom and United States. It was originated out from the three standards developed by those countries. The standards are:

- ITSEC (Information Technology Security Evaluation Criteria) is a European Standard which was developed by UK, France, the Netherlands and Germany in early 1990s.
- TCSEC (Trusted Computer System Evaluation Criteria) or "Orange Book". It is issued by the United States Government National Computer Security Council in December 1985.
- CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) a standard for computer security comparable to the TCSEC but more advanced.

CC and its companion methodology document, Common Evaluation Methodology (CEM), version 1.0 were published in January 1996 for public review. Then it was updated to version 2.0 in 1998 and was accepted by the International Organisation for Standards (ISO) as the Final Committee Draft (FCD) document. In August 1999, version 2.1 became an international standard for IT security known as ISO/IEC 15408 and ISO/IEC 18045 standard. Some updates were subsequently incorporated and it becomes version 2.2 in 2004. A draft of the CC and the CEM version 3.0 was published in 2005 for public comment and targeted to fully be used in January 2008.

The New Version Summary

Major changes have been made to the CC and CEM in version 3.0. This is to ensure that the criteria and the methodology are

efficient, effective and relevant to current assurance needs due to the rapid changing of the technologies.

The changes intend to eliminate problems occurred during the evaluation including the redundant evaluation activities, eliminate evaluation activities that contributes little to the final assurance of a product, clarify CC terminology to reduce misunderstandings in the evaluation phases and restructure the evaluation activities to those areas where security assurance would truly be gained.

The improvement made to the CC and CEM are based on the feedback from consumers, developers, evaluators and other expert groups involved in the standardisation process. The CC and CEM have been reordered, simplified and clearly define to make it easier to understand. The CC and CEM have been extensively restructured and simplified where security functional requirements are simplified from 11 classes to 6 classes and security assurance requirements are simplified from 9 classes to 8 classes. The new version also supports the production of certificates for the composition of compatible certified products.

Below are the summary changes of the CC Version 3.0:

Part 1 was updated to define and establish the use of consistent terminology for the entire CC standard. It is also reflected the Assurance Security Target Evaluation (ASE) and Assurance Protection Profile Evaluation (ATE) families because of the changes of the Protection Profile (PP) and Security Target (ST) content structure.

Part 2 was significantly updated to define and explain the terminology used to describe the security functions of the evaluated product (also known as Target of Evaluation (TOE)). The improvements made in Part 2 are due to the complicated writing and understanding of the Protection Profile (PP) and Security Target (ST) in version 2.

The security functionality requirements are simplified from 11 classes to 6 classes and from 67 to 45 families. The new version divides the security behaviour of the TOE into five major areas as follows:

1. Internal security behaviour of the TOE such as access control.
2. External entities and the TOE connection such as identification and authentication.
3. Protecting communication between the TOE and connected external entities to maintain confidentiality, integrity, non-repudiation, etc.
4. Security audit log such as logging on and of
5. Protection of the TOE security function to protects itself against breakdown, physical attacks, resource exhaustion, etc.

Part 3 was also drastically updated to improve the assurance of the TOE with evaluation activities focused on only those areas that contribute to the assurance of a TOE. Security assurance requirement classes were consolidated, eliminated and added to encountered version 2 evaluation difficulties. The 8 new classes for security assurance requirement are:

Security Target Evaluation (ASE) and Protection Profile Evaluation (APE)

The ASE and APE were restructured so that it will help the consumers to understand the product security functionalities in determining whether the product met their needs. These rewrites provide descriptions of good Assumptions, Threats, Organisational Security Policies, and Security Objectives and also clarify the purpose of the TOE Summary Specification to explain how the TOE meets its claimed security requirements.

Configuration Management (ACM), Delivery and Operation (ADO), Guidance Documents (AGD) and Life Cycle Support (ALC)

These assurance classes' contents were rearranged to have clear definition of the purpose of each family. Therefore, these four classes were rearrange into two classes where the configuration management requirements addressed in ACM was placed in the lifecycle of the TOE (ALC) and the actions associated with the start-up of the TOE which is part of ADO is required by the administrator (AGD).

Hence, the new version only maintain the ALC which addresses the requirements associated with the developer's site and AGD which addresses all of the requirements associated with the consumer's site.

Development (ADV)

This class was rewrite to reflect a reasonable scale of increasing assurance with a corresponding amount of the development work. New families were created, some were modified and some were removed for a sound architecture.

Tests (ATE)

This class was updated to reflect the new ADV.

Vulnerability Assessment (AVA)

This class merged the Security of Function (SOF) analysis into the Vulnerability Analysis (VLA) family. It also merged the Misuse (MSU) analysis into the AGD family because it simply extends the requirements of the quality of those documents. Finally, it created a new lowest level of vulnerability analysis, based upon public domain information.

Composition (ACO)

This class is introduced in CC version 3 to address the issue arises when a TOE consist of an evaluated product such as an

application running in an evaluated operating system. CC version 2 does not cater for separate evaluation; in other words, an evaluation must be performed to both the evaluated and non-evaluate products. Therefore, this new class defines what needs to be done to achieve this.

Common Evaluation Methodology (CEM) was also updated according to the changes of the classes, families and components to reflect the structure of the CC. Methodology is provided for all components up through EAL5 and some of the components' methodology is higher than EAL5.

Implementation

Presently, the review and trial period had been closed and all feedback received for version 3 will be updated and expected to be approved by the Common Criteria Recognition Arrangement (CCRA) Committee in July 2006. During this period, the CCRA Committee had agreed to mutually recognise the products evaluation and certification under trials of version 3. After the approval of the version 3, the national schemes are free to choose whether to use the new version immediately or continue using the version 2 in the evaluation and certification. However, the schemes will be able to continue issuing certificates recognised under CCRA against version 2 until 18 months after the CCRA Committee had approved the version 3.

Conclusion

The improvement being made to the CC and the methodology helps the participants of the evaluation including the consumers, developers and evaluators understand the process of the evaluation better. Therefore, the implementation of the new version is essential to the schemes all over the world.

References

1. http://www.commoncriteriaportal.org/public/expert/index.php?menu=3

No	Event	Vanue	Date
1	E-Security Expo and Forum	Kuala Lumpur, Malaysia	5 - 8 Sep 2006
2	Infosecurity Conference & Exhibition	New York, USA	23 - 25 Oct 2006
3	3rd Electronic Warfare 2006 Conference and Exhibition Incorporating Information Warefare and UAVs	Putra World Trade Centre Kuala Lumpur, Malaysia	5 - 7 Sep 2006
4	HITB Security	Westin Hotel, Kuala Lumpur Malaysia	29 - 29 Sep 2006
5	CeBIT Asia	Shanghai New International Expo Centre, China	17 - 10 Sep 2006
6	Infosecurity Asia	Bangalore, India	20 - 22 Sep 2006
7	China Internet Conference	Beijing, China	21- 24 Sep 2006
8	Workshop on Cryptography Hardware and Embedded Systems (CHES 2006)	Yokohama, Japan	10 - 13 Oct 2006
9	International Conference on Information And Communication Technology For The Muslim World 2006 (ICT4M)	Hilton Hotel, Kuala Lumpur Malaysia	21 - 23 Nov 2006
10	Information Security Summit 2006 Hong Kong	Hong Kong	21 - 24 Nov 2006
11	2nd National Conference on Cryptology (NCC06)	Institute For Mathematical Research, Universiti Putra Malaysia, Serdang, Selangor	28 - 29 Nov 2006
12	Inscrypt 2006 (Formerly CISC): Conference on Information Security and Crytology 2006	Beijing, China	29 - 01 Dec 2006
13	Asiacrypt 2006	Shanghai, China	03 -07 Dec 2006

- Back-up all log records
- Take system off the network
- Report to Malaysian Computer Emergency Response Team (MyCERT) for assistance
- Get forensics specialist for intended legal actions

REPORTING INCIDENTS TO MyCERT

Tel : 603 8996 1901 Fax : 603 8996 0827
E-mail : mycert@mycert.org.my SMS : 019-281 3801 (24X7)
Via online : http://www.mycert.org.my/report/form_report.html

Join MyCERT's mailing list for updates and alerts.
Log on to the website to join this free service.

http://www.mycert.org.my

Malaysia Cyber Security Centre

MOSTI