NISER
National ICT Security and Emergency Response Centre

e-Security

National ICT Security and Emergency Response Centre

NISER's Quarterly Bulletin

Volume 6 (Q1/2006)

Editor

Philip Victor
Training & Outreach Unit, NISER

Contributors :

From the Editor's Desk

Welcome 2006 and goodbye to 2005! Another new year and more good articles are packed in this issue. More IT Security professionals from within NISER and from the industry have brought together informative and useful articles.

In 2006, we saw the launch of Infosec.my, our local interest group which will see discussions, forums, sharing of ideas and knowledge for IT Security professionals. We have had close to 80 members now and growing. We would like to invite more IT Security professionals to come on board and use this platform to meet, share, exchange ideas and discuss with fellow professionals.

Coming up this July is our Information Security conference, SecureMalaysia 2006 which is jointly organized by NISER and (ISC)2. This year we have brought together some very prominent and globally recognized speakers such as, Howard Schimt, Ralf Moulton, Dr. Corey Schou, kang Meng Chow, Lt Col (R) Husin Jazri, John Meakin, Steve Orlowski, Anil Mahtani and many others. This year we will see very interesting topics being presented and will definitely be exciting. So book your seat early.

Another event we have coming up in May is our CISSP CBK Review Smeinar which will be held from the 21st till 26th May 2006 at the Hilton, PJ. We have received good response for this class and have a few more seats left. The course will be conducted by a certified (ISC)2 instructor from the US and will be taught using the latest updated CISSP materials for 2006 exams. Email to cissp@niser.org.my for details.

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
National ICT Security & Emergency Response Centre
MIMOS Berhad
Technology Park Malaysia,
57000 Kuala Lumpur, Malaysia
Tel: 60 3 8657 7042
Fax : 60 3 8996 0827

Email: training@niser.org.my

Original Issue Date: 10th April 2006

The MyCERT Quarterly Summary is a report which includes some brief descriptions and analysis of major incidents observed during this quarter. This report also features highlights on the statistics of attacks or 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.

Recent Activities

The first quarter 2006 was more hectic compared to the previous quarter. There was no significant outbreak reported in this quarter, but we saw a tremendous surge in intrusions, mainly web defacements of .MY domains and the increase in Forgery incidents. Generally, there was a 26.73% increase in the number of incidents reported in this quarter compared to the previous quarter. The number of incidents reported for this quarter is 4276 with a majority of incidents contributed by reports on spam.

Surge in Intrusion Incidents

The first quarter of 2006 saw a surge on intrusion incidents with a total of 97 cases, which is more than 100% higher than the previous quarter. Mainly, intrusions reported to us involved web defacements of various domains belonging to our constituency. In this quarter, we observed more websites running on Linux platforms fall victim to web defacement and IIS servers, still remains the main victim of web defacement.

Though the number of defaced sites in this quarter is not alarming, MyCERT's concern is if the number increases over the time and year. Thus, MyCERT would like to urge all System Administrators and owners of websites to upgrade and patch the software, services or applications they are currently running on. In addition, it is also recommended to disable unnecessary default services supplied by vendors. MyCERT encourages system administrators to consult MyCERT for further advises and assistance, if they have difficulties in proper securing and hardening of their servers.

MyCERT produced an alert on the recent mass defacement of Malaysian websites, which is made available at:
http://www.mycert.org.my/advisory/MA-103.022006.html
(Released on 21st February 2006)

MyCERT believes majority of web defacements were due to poorly secured and unpatched machines. Apart from that, running vulnerable PHP scripts that could be easily exploited by defacers to deface websites could also be named the main culprit. Some of the exploits used by the defacers are SQL Injection and Unicode vulnerability.

Our analysis shows that majority of previous intrusions such as web defacements were due to vulnerable and unpatched services running on the server. Web defacements involving Linux machines are due to running of older versions of the Apache servers, PHP scripts and OpenSSL. As for IIS web servers, web defacements were commonly due to Microsoft IIS extended Unicode directory traversal vulnerability, Microsoft Frontpage Server Extension vulnerability and WEBDAV vulnerability.

Details of the vulnerabilities and solutions are available at:

1. Apache Web Server Chunk Handling Vulnerability
   http://www.cert.org/advisories/CA-2002-17.html
2. Vulnerabilities in PHP File upload
   http://www.cert.org/advisories/CA-2002-05.html
3. Vulnerabilities in SSL/TLS Implementation
   http://www.cert.org/advisories/CA-2003-26.html
4. WEBDAV Vulnerability
   http://www.cert.org/advisories/CA-2003-09.html
5. Microsoft IIS extended Unicode directory traversal vulnerability
   http://www.mycert.org.my/advisory/MA-024.042001.html

Web servers running Windows IIS servers, may use the IIS Lockdown tool to harden their server.

IIS Lockdown Wizard version 2.1 works by turning off unnecessary features, thus reducing attack surface available to attackers.

The IIS Lockdown tool can be downloaded at:
http://www.microsoft.com/downloads/details.aspx?FamilyID=dde9efc0-bb30-47eb-9a61-fd755d23cdec&DisplayLang=en

Web server running on Linux, may use the TCP filtering mechanism such as TCP Wrappers at the server or gateway level. TCP Wrappers is a tool commonly used on UNIX systems to monitor and filter connections to network services. TCP Wrapper can be downloaded free at:
http://www.cert.org/security-improvement/implementations/i041.07.html

Reports on Forgery Increases

Forgery incidents still continue with a slight increase compared to previous quarter. A total of 54 incidents were reported compared to 48 in previous quarter, which represents a 12.5% increase. Majority of forgery incidents were phishing activities, which mainly involved foreign financial institutions such as the Ebay and Paypal, with a few involving local financial institutions. As was in previous quarter, this quarter continues 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. Fortunately, the phishing sites were removed successfully within 6 hours or less. We also advised the respective ISPs, data centers and organizations to investigate the affected machines and rectify the error, as we believe the machines

were compromised due to some unpatched vulnerability.
MyCERT strongly urges users who receive emails purportedly from financial institutions requesting to change their logon and password to ignore and delete such emails immediately. Users are also advised to refer and verify such emails with their ISPs, CERTs or with the particular financial institutions mentioned.
In addition, MyCERT also advises organizations to secure and harden their servers to prevent the servers from being compromised and used for malicious purposes, such as running phishing sites.
Besides phishing reports, MyCERT also received few reports from our constituency regarding Internet scams, which is worth highlighting in this issue. 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 Scams
e) Get Rich Scams

Number of victims and monetary loss to the above scams reported to us are low and not alarming. The mode of operation of the above scams is almost similar, which is to cheat users.

Some scams have manipulated names of some local law enforcement agencies to convince the users. These scams also resort to using invalid company addresses and valid contact numbers to run their activities. Based on our analysis, the websites used to run the scams are mostly registered and hosted in foreign countries, thus tracing the operators are difficult. However, we believe some of the operators could be foreigners based in Malaysia. We came to the conclusion by looking at the nature and modus operandi of the scams. Most of the Internet scam cases are referred to the local law enforcement agencies, such as the police and the Bank Negara Malaysia for further investigation.

MyCERT advises users not to deposit or pay any amount of money to a third party except to licensed financial institutions. Users are advise to ignore suspicious emails that request users to bank in certain amount of money to an account. Users may also verify such emails with their ISPs, CERTs or with Bank Negara Malaysia.

Harassment on Continuous

Incidents on harassment are still on the continuous and remain the same with a total of 14 reports in this quarter.
Majority of harassment incidents received in this quarter, involved those committed via emails, chat forums and web forums. Websites are being misused as platforms to harass a nation, by putting up misleading and false information about a nation. Most of harassment reports were referred to the law enforcement agencies for further investigation. MyCERT has also assisted the police in analysing some reported cases.
MyCERT advise users who are harassed via Internet or any individuals who observed any kind of harassments via web forums, which has religious, social, political or economic implications to report to MyCERT for further analysis.
In addition, we also advise users to be more careful while communicating either via emails, chat forums or web forums.
They should never reveal or upload their personal information such as their contact numbers, home or office addresses, photos or pictures on the net or to non-trustworthy parties as this information could be abused by a third for malicious purposes.

Drop in Malicious Code Incidents

Incidents on malicious code had dropped to 17 for this quarter from 30 in the previous quarter. It represents a 43.3% decrease. Majority of worm reports received in this quarter are the W32.Nyxem/Blackmal and W32.Brontok worms. Overall, no significant worm outbreak in the constituency was reported in this quarter, though there were some organizations that were affected by the above worms. However, the situation was contained and the recovery process was successful, due to MyCERT's advises and guides.

MyCERT has released the following alerts related the W32.Nyxem and W32.Brontok worms:
W32.Brontok Worm (Released on 22nd March 2006) http://www.mycert.org.my/advisory/MA-104.032006.html
W32.Nyxem.D (Released on 24th January 2006) http://www.mycert.org.my/advisory/MA-101.012006.html
W32.Nyxem.E (Released on 3rd February 2006) http://www.mycert.org.my/advisory/MA-102.022006.html
MyCERT advise users and organizations to take precautions always against worm incidents, even though there are no worm outbreaks observed within our constituency. Some of the precautions that can be taken are:

• Email Gateway Filtering

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

• System/Host

i. Users must make sure that their PCs are installed with anti-virus software and are updated continuously with the latest signature files. Users who do not have an anti-virus installed on their PCs may download an anti-virus from the following site:
http://www.mycert.org.my/anti-virus.htm
ii. Users need to make sure that their PCs or machines are always updated with the latest service packs and patches, as some worms propagate by exploiting unpatched programs present in PCs or machines.
iii.Enable a personal firewall on your computers.

• Safe Email Practices

MyCERT has strongly advised users not to open any unknown attachments, which they have received via emails. Any suspicious emails should 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.htm

Decrease in Hack Attempts

Incidents on hacking attempts showed a decrease of 53.8% in this quarter. A total of 6 reports were received on hacking attempts for this quarter compared to 13 in the previous quarter. Hack threats targets mainly on organizations' systems and networks. Home users PCs are also becoming the attackers target on port scanning.

MyCERT's findings for this quarter showed that the top targeted ports for scanning are SSH (TCP/ 22), FTP (TCP/21), HTTP (TCP/ 80), MS SQL (TCP/1433), which could be possibly due to newly discovered vulnerability on these services. Port scanning is 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, scanning are also actively done to detect any machines running vulnerable programs and scripts, such as scanning for 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 or services should be filtered and patched accordingly.
b) All machines or systems are properly patched and upgraded with the latest patches, service packs and upgrades to fix any vulnerability that may be present in the machines or systems.
c) Organizations can install network based or host based IDS to alert scanning and other malicious attempts to their hosts.
d) It is recommended that home users install personal firewalls in order to alert the owner of any unauthorized scanning to their machine and to block any penetration into their system.
More information on home PC security is available at:
http://www.mycert.org.my/homepcsecurity.html
Other Activities

Spam

Spam incidents still remain on top with a total of 4088 reports, which represents a more than 25.9% increase compared to previous quarter. The main reason for this significant increase may be because of the increased of sophisticated techniques being applied by spammers to carry out their activities. Some spam techniques can even bypass spam filters. The spammers have learned to combine many techniques to improve their activities, often called blended techniques, which are more effective.

Spam has developed from a mere nuisance into an epidemic that threatens all enterprise messaging. There is no perfect technique and tool to eradicate spams totally but there are techniques that can be used to minimize spam emails. Organizations are advised to install anti-spam filters at their email gateways to minimize spam emails and end users are also advised to apply appropriate filters at their PCs to minimize spam emails.

Denial of Service

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

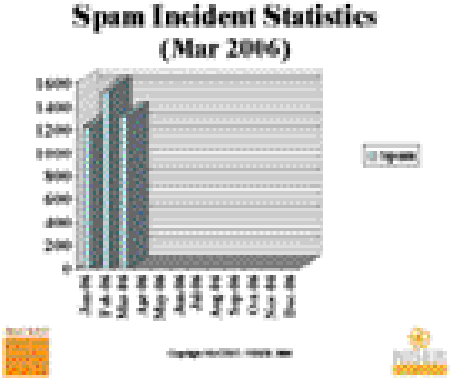
Conclusion

Overall, the number of incidents reported to us has increased to about 26.7% compared to the previous quarter. In this quarter, we also observed increase in most of security incidents. Forgery, intrusion, spam incidents continue to increase. Malicious code and hack threat incidents have decreased compared to previous quarter. As for harassment and denial-of-service, the number remains as was in previous quarter.

Generally, no crisis or significant attacks and incidents were observed for this quarter that caused severe impact to the constituency. Nevertheless, we advise users and organizations to take precautious measures to protect their systems and networks from security incidents. MyCERT also encourages users and organizations to report and seek assistance from us on security incidents.

Complete figures and statistics graph on the Abuse Statistic released by MyCERT monthly is as below:

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Harassment	3	7	4									
Forgery	9	23	22									
Hack Threat	3	1	2									
Malicious Code	1	6	10									
Denial of Service	0	0	0									
Intrusion	26	36	35									
TOTAL	42	73	73									



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Spam	1227	1538	1323									

Introduction

Incidents of espionage as a way of getting military, political or economic secrets have been well documented throughout history, while the method of using a "Trojan" (the Trojan horse) to penetrate the enemy defensive position is a well known exploit in Greek mythology, known as the Trojan war.

The end of the Cold War has resulted the espionage activities been diverted to industrial espionage. Industry players seek competitive advantage by obtaining or stealing its competitor's trade secrets and logistics. The attacks are highly targeted to gain the specific information sought. Companies will devote the necessary resources towards industrial espionage to achieve an acceptable return on investment.

Corporate espionage is a threat to any businesses whose livelihood depends on information.[1] It can also be defined as the theft of trade secrets through illegal means such as wiretaps, bribery and cyber intrusion.[2] In year 1999, Price Waterhouse Coopers reported that U.S. firms lose US$45 billion to espionage, nearly twice the estimate given a few years earlier by the FBI.[3]

Recent development shows that corporate espionage using Trojan is on the rise. With rapid advancement of ICT, espionage activities have been carried out using ICT technologies. These types of cyber attacks are targeted at specific recipients to get past firewalls and gather sensitive data.

1 Robinson, S., Corporate Espionage 101,version 1.3, SANS Institute 2003 *http://www.sans.org/rr/whitepapers/engineering/512.php* , last visited 10 February 2006.

2 Business Week Online, The Case of the Corporate Spy, In recession, competitive intelligence can pay off big, 26 Nov 2001, *http://www.businessweek.com/magazine/content/01_48/b3759083.htm*, last visited 13 February 2006.

3 Sullivan, B., Israel espionage case points to new Net threat, Experts: Targeted spy attacks could be soon be common, MSNBC, 9 June 2005, *http://www.msnbc.com/id/8145520/page/2*, last visited 10 February 2006.

Trojan "hide malicious code" inside a host program that seems to do something useful. Once these programs are executed, the virus, worm or other types of malicious code hidden in the Trojan program is released to attack the workstation, server, or network, or to allow unauthorised access to those devices. Trojans are common tools used to create backdoors into the network for later exploitation by hackers.[4] By creating backdoors of the corporate networks, the hackers could steal corporate secrets or use the compromised computers to send spam and viruses.

Below are some cases of industrial espionage as reported in the media.

4 Krutz, R.L., and Vines, R.D., The CISSP Prep Guide, Second Edition: Mastering the CISSP and ISSEP Exams, Wiley Publishing, Indiana, 2004.

5 Vardi, N., Chinese Take Out, Forbes.com, 25 July 2005, *http://www.forbes.com/home_asia/free_forbs/2005/0725/054.html* , last visited 15 November 2005.

Case 1: Myfib

Myfib Trojan first appeared in August 2004. This Trojan is sent by spam and can navigate a computer network once the attachment is clicked. A US security firm, Lurhq has reversed engineered Myfib codes for clients and discovered that the Trojan was sending stolen data to an Internet user in Tianjin, China.[5] The program appears to have originally developed to steal student exam papers and later expanded to copy many types of documents such as computer assisted drawing and Microsoft Word files. It has been reported that the code has been used to steal sensitive documents such as mechanical designs and circuit board layouts.

In another case, it was reported that a group of Chinese hackers were suspected of launching intelligence-gathering attacks against the U.S government. The hackers, believed to be based in the Chinese province of Guangdong, were believed to have stolen U.S. military secrets, including aviation specifications and flight-planning software.

Case 2: Britain Attacked

In June 2005, the United Kingdom's National Infrastructure Security Coordination Centre (NISCC) provided advice and issued a briefing pertaining to targeted Trojan email attacks against the UK Government and companies.[6] NISCC believed that the principal goal of the attacks is covert gathering and transmitting of privileged information which are commercially or economically viable. These attacks used open source Trojans such as Nethief, MoFei, GWBoy, Grey Pigeon, Magic Link and Bespoke, which were being altered to avoid anti-virus detection. Once installed, the Trojan can collect usernames and passwords of email accounts, collect system information, upload documents and data to a remote computer, downloading of further programs, which can be more sophisticated Trojans, and relay further attacks against other computers and networks. NISCC discovered 17 Trojans or remote monitoring programs between April and May 2005.

Case 3: Trojan-gate

This case came to light when a husband and wife book writing team, Amnon Jackont and Varda Raziel-Jackont found out that passage from their book, which was not yet published then, was posted on the Internet. They suspected that someone has hacked into their computer system and stolen files. Police investigation traced the alleged theft to Varda Raziel-Jackont's former son-in-law, Michael Haepharati, a computer consultant. This case is dubbed the "Trojan Affair" and some are calling it "Trojan-gate". In May 2005, Michael Haepharati was detained in London together with his wife, Roth Brier-Haepharati.[7] Both

6 National Infrastructure Security Co-ordination Centre (NISCC), Targeted Trojan Email Attacks, NISCC Briefing 8/2005, issued 16 June 2005, http://www.egovmonitor.com/reports/rep11599.pdf, last visited 13 February 2006.

7 Trojan Horse developers to be extradited to Israel soon, Hack In The Box, 18 January 2006, http://www.hackinthebox.org/print.php?sid=19044, last visited 13 February 2006.

were repatriated to Israel on 31 January 2006 [8] , soon after the appeal court in London approved their extradition on 13 January 2005, for allegedly selling rogue computer program to Israeli private investigators who use it to spy on their clients' competitors.

The Tel Aviv Magistrate's Court has remanded several people from some of Israel's leading companies and private investigators suspected of commissioning and carrying out industrial espionage against their competitors. It has been reported that at least 18 Israeli firms have been implicated in this case.[9] The act was allegedly carried out by planting Trojan in their competitors' computers. It was discovered that Mr Haepharati had sold the rogue computer program to three private investigation agencies.

How Can You Prevent The Trojan From Installing On Your Computer?

To avoid unintentionally installing Trojans on your computer, below are some suggestions you can practice:

- Do not downloadable free software from untrustworthy source. There are many sites that offer exciting programs or software. You may be exposing your computer to Trojans by downloading some of these programs.

- Choose "no" when you received unexpected questions from unexpected dialog boxes. Be wary of unexpected dialog boxes asking whether you want to run a particular program or perform another type of task. By clicking the dialog boxes questions may install Trojans on your computer.

- Do not click an email attachment that is suspicious. Trojans can bypass most anti-virus software and entice the recipient to believe the e-mail transmitting the Trojans is legitimate. Instead of installing the intended document, you are actually installing Trojans.

- Run a legitimate product specifically designed to scan and remove Trojans in your computer. The Trojans probably undetectable by using normal anti-virus software and could remain hidden on the compromised computers for years.

Conclusion

Home computers and corporate networks are already bombarded by unwanted contents such as spam, phishing, viruses and worms. Perpetrators are continuously conducting in-depth research on network security and find ways on how to penetrate big corporation's network and critical infrastructure organisations without being suspicious. The sophistication levels of attacks are increasing and it is expected that those attacks will grow more slick and secretive in the future.

8 Israel holds couple in corporate espionage case, Reuters, in Yahoo! News,31January 2006, http://news.yahoo.com/s/nm/20060131/tc_nm/crime_israel_spyware_dc, last visited 13 February 2006.

TACKLING THE CONFUSION BETWEEN IDS & IPS

Are Intrusion Detection Systems (IDS) becoming a dying breed to be killed off by the evolving superiority of Intrusion Prevention Solutions (IPS)?

Users are still confused whether to bank on IDS or IPS. And while the debate rages on, malicious code gets into the network, disrupts the business, and cost big money to remediate.

Companies today have invested millions of dollars on perimeter security devices like firewalls, packet filtering routers, and anti-virus gateways, and yet still suffer at the hands of malicious code like Nachi, Blaster, and SoBig.

Sometimes attacks pass by the firewall successfully while others are carried in on the laptop of a mobile employee. CISOs recognize that this is an unacceptable problem and plan to respond with major changes to their network security technology portfolio.

Information security should be based on a layering effect of technologies throughout an organization to provide an umbrella that mitigates risk and thereby reduces threat.

For the last two decades, security technologies have been segregated to the different worlds of IDS, firewalls, routers, switches and more. Each operates in a separate segment of the company network, while together providing threat mitigation and risk reduction through the collection of logs, rules, policy and configurations.

The arrival of IPS now offers one more guarded layer of defense.

Two Different Animals

Gartner's prediction that IDS will soon be dead and that IPS are the answer to most security issues has no doubt thrown the industry into a further state of confusion. IT personnel continue to argue over a philosophical security question: intrusion detection or intrusion prevention?

Comparing the two technologies assumes that they are competitive solutions but a more thorough investigation demonstrates that they are actually quite complementary.

IDS and IPS share a common heritage as each evolved from network analysis or "sniffer" technologies. From these roots the systems split into dissimilar architectures for different purposes.

Think of IDS devices as motion detectors that monitor movement within houses. For example, should a thief penetrate outer defenses like locked doors and windows, motion detectors will act as a defense-in-depth safety net. To put it simply, IDS systems are passive monitoring devices

9 18 Arrested In Israeli Probe Of Computer Espionage, Washington Post, 31 May 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/05/30/AR2005053000486.html, last visited on 13 February 2006.

that were never designed for prevention. When digital bad guys (aka malicious code) gets by active devices like firewalls and anti-virus gateways, IDS systems provide a last line of defense.

But herein lies the problem: IDS systems tends to produce tons of false positive messages. The noise of false positives is a fundamental part of IDS design. One assumes that security personnel will be on hand to analyze IDS alerts, examine individual attacks, and track history to get a better picture of their security profile and network behavior.

Over the past few years, leading IDS vendors have done a good job at reducing IDS chattiness and systems can always be tuned for individual environments, which further reduces false positives. Nevertheless, the ultimate responsibility for IDS systems is in identifying suspicious behavior.

If IDSs are like motion detectors, IPSs are like another layer of locked doors within the house. Both types of systems may watch the network for fishy behavior but this is where the similarity ends. IPS devices live in-band on the network, filtering packets in real-time. A typical architecture would place IPS protection in front of the firewall, in the DMZ and on the corporate backbone. As such, IPS devices join an active, defense-in-depth infrastructure team along with technologies like firewalls, anti-virus software, spam filtering and content security. Each member of this group is tasked with actively blocking specific types of malicious attacks. The IPS's job is to backup these other technologies guarding against worms, viruses, DOS attacks and behavioral anomalies that
could lead to a minor annoyance, an operational fire drill, or a severe business interruption.

Naysayers criticize IPS devices claiming that they represent a single point of failure, impact network performance, and may block legitimate traffic. In the big picture, each of these issues is valid but IPS vendors have gone to great lengths to overcome these objections. First, IPSs tend to be built out of the same type of solid-state components as the networking devices that companies have relied on for years. IPS systems can be clustered for failover and load balancing to guarantee critical network availability. To maintain performance, IPS devices rely on lightning fast ASICs, FPGAs, processors, and memory easily capable of keeping up with the 1Gb backbones in most enterprise LANs. Finally, to make sure that malicious code is blocked while passing along legitimate packets, IPS devices can be tuned over time. Even without tuning however, a standard out-of-box configuration can block a large percentage of the worms and viruses that tend to wreak havoc when they get through the door.

Going for an intergrated approach

One should understand that IDS and IPS serve fundamentally different roles. The best strategy is to integrate both technologies into a defense-in-depth security architecture. Here are the key benefits:

1.Proactive filtering

Preventing the spread of Internet malware is not just marketing hype; IPS signatures and network anomaly heuristics deliver real results to real customers today. They are not 100 percent effective but by filtering a majority of attacks, corporate assets are protected and security staff is spared from fighting fires on additional fronts.

2.Better resource utilization

By blocking malicious code, IPS devices offload processor cycles from other filtering devices like firewalls and anti-virus gateways. This improves overall network performance and helps companies avoid capital spending on equipment upgrades and additional bandwidth.

3.Increased ability to detect unseen security problems

Very often, security issues are caused by misconfigurations and human error, not just viruses and worms. Working together, the IDS/IPS combination can cut down on false positive IDS noise freeing security staff to discover and fix these types of process problems.

4.Historical data trends

While the IPS device filters bad packets, the IDS can continue to capture and store data for network and security analysis. This should help get security staff out of 'panic mode' and give them more time for careful and proactive examination of trends and lingering problems.

While an IDS/IPS solution is ideal, some companies may balk at spending precious
security dollars on two technologies. Since IPS devices can be expensive, companies can justify them based upon ROI metrics like improved network uptime, superior utilization of security equipment, and more efficient use of headcount. Savings in these areas will pay for IPS costs within a relatively short time frame.

Best of both worlds

What does the future hold for intrusion detection and prevention? IDS vs. IPS is a technology war akin to industry debates like Ethernet or Token Ring and Linux or Windows. In the security world, the key requirements are maximum protection of corporate assets, operating efficiency, and reasonable capital expenditure.

Smart security managers can obtain all three via a

comprehensive security infrastructure that combines IDS and IPS. IDS and IPS devices actually work best in tandem. The IPS device blocks known hostile code, while the IDS provides another pair of eyes into real-time and historical security events. In other words, implementing both IDS and IPS devices offers the highest level of security protection.

HACKING!!! UNDERSTANDING THE LEGAL ISSUES

In this article you will lear

- The nature of hacking
- Why lawyers need to understand the nature of hacking before they can provide legal advice
- How to do legal analysis based on an actual hacking incident

Key Points

7.1 Introduction

7.2 The Hacking Process

- 7.2.1 Section 3 of the CCA: Unauthorized Access to Computer Materials
- 7.2.2 Section 5 of the CCA: Unauthorized Modification of the contents of any computer
- 7.2.3 Deletion of the log files & its implications

7.3 Conclusion

KEY POINTS

(1) Hacking is a technical process and a lawyer must understand the mechanics of the hacking process to understand the meaning of unauthorized intrusion or unauthorized modification

(2) When analyzing legal issues, lawyers need to understand the nature of digital evidence before they are able to address the legal implications arising out of the hacking incident such as the burden of proof

7.1 INTRODUCTION

This article seeks to provide a basic understanding of the process of hacking, the most common form of computer crime so that lawyers and other non-technical readers would be able to better able to put the act of hacking in its proper legal context. Before lawyers can do any legal analysis of any fact situation in a hacking incident, they need to understand the processes involved. This article seeks to outline the hacking process, its legal implications and the techniques of legal analysis.

There are two types of scenarios in computer crimes. First where the computer is the target and second where the computer is used as a tool to commit a crime. In situation where the computer is the target, such a crime typically relates to unauthorized access or entry (that is, the typical hacking) and secondly the act of making unauthorized modification of programs or data once the hacker is in the network system or in the computer. An example of a situation where the computer is used as a tool to commit a crime would be someone who breaks into the system of a bank to withdraw money illegally.

In order to understand the hacking process, consider the following event that actually took place in the US[10] :

British National Charged with Hacking Into N.J. Naval Weapons Station Computers, Disabling Network After Sept. 11; Indictment Also Filed in Virginia for Other Military Instructions

An unemployed United Kingdom computer system administrator, McKinnon was charged for allegedly breaking into the computer network at the Earle Naval Weapons Station in the US, stealing computer passwords, and shutting down the network in the immediate aftermath of the September 11 terrorist attacks.

McKinnon was charged with intentional damage to a protected computer for intrusions into 92 computer systems belonging to the U.S. Army, Navy, Air Force, Department of Defense and NASA. As a result of the intrusions into the U.S. military networks, McKinnon rendered the network for the Military District of Washington inoperable. McKinnon is also charged with intrusions into two computers located at the Pentagon. The indictment also charges McKinnon for intrusions into six private companies' networks. McKinnon is charged with causing approximately $900,000 in damages to computers located in 14 states.

According to the charge, on April 7, 2001, McKinnon hacked into the NWS Earle computer network through the Port Services computer, the primary computer used by NWS Earle for monitoring the identity, location, physical condition, staffing, battle readiness and resupply of Navy ships in and near the NWS Earle Pier Complex. At that time, he is alleged to have installed the software program RemotelyAnywhere on the Port Services computer and on other computers connected to the NWS Earle network. RemotelyAnywhere is a commercially available software program that allows an individual to remotely control a computer from any other computer via an Internet connection.

The Indictment further charges that during the period of June 18, 2001 through June 21, 2001, McKinnon obtained unauthorized access to the Port Services computer on several occasions via an Internet connection and, through use of the previously-installed RemotelyAnywhere software, stole approximately 950 passwords stored on server computers connected to the NWS Earle network.

In addition, according to the charge, on Sept. 23, 2001, McKinnon again broke into the NWS Earle computer network by accessing the previously-installed

10 This is based on the press release issued by the US Department of Justice.

RemotelyAnywhere software and using the stolen passwords. During this intrusion into the network, McKinnon allegedly caused approximately $290,431 in damage to NWS Earle by deleting computer files needed to power up some of the computers on the network, deleting computer logs that documented his intrusion into the network, and compromising the security of the network by leaving it vulnerable to him and other intruders via the RemotelyAnywhere software.

7.2 THE HACKING PROCESS

In the above scenario, McKinnon's action that amount to hacking & unauthorized modification is when he:

(1) hacked into the computer network at the Earle Naval Weapons Station
(2) installed the software 'RemotelyAnywhere' into the computer system of the station
(3) stole computer passwords;
(4) deleted files & computer logs; and
(5) shut down the network.

In a typical hacking scenario, the first thing that a hacker such as McKinnnon would do is to decide what he wants to achieve for example:

(1) breaking into the system of a defence agency (just for the thrill of it)
(2) deface the site and leave his 'marks' to boast of his ability to break into secured systems
(3) deny service to users of the system simply to frustrate others
(4) go into the system to obtain confidential data and publicly publish it on the web; or
(5) paralyzed the system as an act of cyber-terrorism

The hacking technique would vary depending on the objectives. For instance, if the hacker simply wants to deny services to users of the system, the hacker need not necessarily have to break into the secured system but he may simply flood the system for example by directing millions of email or simply flooding the system with junk data. One of the most common techniques to do this is called the Ping of Death, where the hacker sends endless 'probing' commands to the server until the server is unable to cope. By doing so, the system gets clogged and the hacker would achieve his goals.

But hackers often break into IT systems and this will be the example that we shall review now. An easy way to understand this for a non-technical person is to imagine a secured system to be like a gated residential area with high security wall or fence. The hacker would be like the thief who wants to steal precious things which may be in one of the exclusive house in the gated residential area.

For the hacker, one of the first things he must do is to plan his entry into the target system just as a thief would have to decide how he would penetrate the security wall in the residential area. Planning an entry into a secured system would require a hacker first to determine what the operating system the intended target system is running on. This would be like determining how the gated residential unit security system is controlled and managed.

Once the hacker has identified the operating system, the hacker will next determine how he can hack into the system in such a way that he is able to gain the greatest control with the greatest ease. He would do this by determining known vulnerabilities of this operating system. In our gated residential unit example, the thief would try to obtain any information about the weakness of the security system that is being used by the company operating the security system.

Next the hacker would need to test the system's vulnerabilities. He does this by sending out commands and seeing how the IT security system responds. A particular type of response will require a certain type of break-in strategy and the hacker would continue to test until he finds the best way to break in. Different vulnerabilities have different risk exposures and the hacker would typically understand the range of possibilities and would plan his illegal entry accordingly. Just as the thief breaking into the fenced area would require tools to commit his crime, the hacker would require tools (usually software programs) to break into the IT system. With the known vulnerabilities, he would exploit it using whatever tools he has at his disposal.

The next step that a hacker might do is to try to send some instructions to the server should the vulnerability that is being exploited allows this. A very common way to accomplish this is to send some data to the server that has been designed in such a way that once the server receives the data, the data will turn into certain instructions allowing him either to control the system or to automatically instruct the system to act in a certain manner. The hacker may then probe the system to obtain a list of programs that are available for him to carry out his attacks.

Yet another way for our hacker to break into secured system is what is typically known as a 'brute force' attack, which means running a program that repeatedly tries to login into the system using a special kind of 'dictionary' that contains a huge list of passwords. The aim is to simply try out whatever password that may allow him entry. The process is repeated until the password is discovered.

In some cases, breaking into a system could be a much easier process simply because the whole system was poorly secured and the hacker need not exploit any known vulnerability. In our gated residential area analogy, this would be equivalent to someone who either fail to secure his house properly or uses a faulty lock. In some cases,

therefore, hackers can penetrate into systems easily simply because the IT administrator in charge of security secures the site poorly. In our gated residential area, this would be equivalent to the Head of security simply not following instructions to ensure that his security system works thus making it easier for someone to break into the housing estate.

Once the hacker has successfully entered the system through either the known vulnerabilities or through brute force approach or through any other means, the hacker might need to enable file transfer service in order to allow him to send and install a list of programs that he requires if these programs are not available in the target system. In our case, Mckinnon installed the software RemotelyAnywhere into the target system.

After a hacking attempt has been successfully carried out, a good hacker would typically erase all his tracks by deleting the programs that he has uploaded or any system logs that might have been created.

A more sophisticated hacker would not target the system directly from his computer, but he might hack into another weaker system first and then use this compromised system to hack into the target system. This would make it more difficult for other people to trace his tracks.

Lawyers need to understand the hacking process in order to do a proper legal analysis. An IT professional must in turn understand how the law works in order for cyber criminals to be successfully prosecuted. Let us now look at how this fact situation can be analyzed from the legal perspective in the context of the Malaysian Computer Crimes Act (CCA).

7.2.1 Section 3 of the CCA: Unauthorized Access to Computer Materials

Under Section 3 of the Computer Crimes Act, in order for the hacker to have committed an offence, the following three elements must be fulfilled:

(1) The hacker must 'cause a computer[11] to perform any function'[12] with intent to secure access to any program[13] or data[14] held in any computer;
(2) The access he intends to secure is unauthorized; and
(3) The hacker 'knows at the time when he causes the computer to perform the function that that is the case'

Unauthorized access[15] is in turn defined under Section 2(5) of the CCA (Interpretation Section), as follows:

'…Access of any kind by any person to any program or data held in a computer is unauthorized if (a) he is not himself entitled to control access of the kind in question to the program or data' AND 'he does not have consent or exceeds any right or consent to access by him of the kind in question to the program or data from any person who is so entitled'

In this case, by hacking into the system, the Defendant had intended to secure access to a system in which he is not authorized to access and he knew that that was the case. The hacking into the system itself is an act that 'causes a computer to perform any function with intent to secure access to any program or data held in any computer.

Section 3(2) of the Computer Crimes Act also makes it clear that:

'The intent a person has to have to commit an offence under this section need not be directed at –
(a) any particular program or data;
(b) a program or data of any particular kind; or
(c) a program or data held in any particular computer
Thus in this case it is not relevant whether the Defendant's intention was directed at any particular program or data (for example the computer system in NWS Earle network) or data such as the password that he stole.

Section 4 of the Computer Crimes Act in turn provides:

(1) a person should be guilty of an offence under this section if he commits an offence referred to in Section 3 with intent –
(a) to commit an offence involving fraud or dishonesty or which causes injury as defined in penal code; or
(b) to facilitate the commission of such an offence whether by himself or by any other person.
(2) For the purposes of this section, it is immaterial whether the offence to which this section applies is to be committed at the same time when the unauthorized access is secured or on any future occasion.

To constitute an offence under this section which is a more serious crime, the elements of Section 3 must first be proved. Under Section 4, the person must have the intention to commit an offence involving fraud or dishonesty or which causes injury as defined in Penal Code. It is, however, immaterial whether the offence of fraud or dishonesty has actually been committed. The section further provides that it is still an offence though it is to facilitate the commission of an offence by the third party.

7.2.2 Section 5 of the CCA: Unauthorized Modification of the contents of any computer

An offence under Section 5 is committed when a person 'does any act which he knows will cause unauthorized modifications of the contents of any computer'

'Unauthorized modification' in turn is defined in the interpretation provisions in Section 2(7) and Section 2(8). Under this section, 'a modification of the contents of any computer takes place, if, by the operation of any function of the computer concerned or any other computer –

(1) Any program or data held in the computer concerned is altered or erased;
(2) Any program or data is introduced or added to its contents; or
(3) Any event occurs which impairs the normal operation of any computer,

and any act that contributes towards causing such a modification shall be regarded as causing it'

Under Section 2(8), such a modification is unauthorized if –

(1) The person whose act causes it is not himself entitled to determine whether the modification should be made; and
(2) He does not have the consent to the modification from any person who is so entitled.

In this case the Defendant McKinnon had modified the contents of the computer system of NWS Earle network by introducing the software RemotelyAnywhere and one element under this provision has been fulfilled, that is, he has introduced a program into the system.

The deletion of the files also falls within Section 2(7)(a) as it is an erasure of a program or data. The act of stealing the password in turn can be regarded as a modification too as it could be a form of 'alteration' or 'erasure' to the data in the computer system although the defendant's lawyer could possibly raise the argument that when the passwords are 'stolen' there has been no alteration or erasure as only a copy was made. The fact, however, that a hacker enters into a system and have access to the password by whatever means such as copying is by itself an act of alteration of the data in the computer system.

The shutting down of the system in turn would fall under the definition of an event which 'impairs the normal operation of any computer'

7.2.3 Deletion of the log files & its implications

The deletion of the log files may make it difficult for the prosecution to prove its case beyond reasonable doubt. Log files provide evidence of the crime and it is one of the most important evidence that has to be produced in court by the prosecution.

Under Section 90A(1)[16] of the Malaysian Evidence Act 1950:

'In any criminal or civil proceeding a document produced by a computer or a statement contained in such document, shall be admissible as evidence of any fact stated therein if the document was produced by a computer in the course of its ordinary use, whether or not the person tendering the same is the maker of such document or statement.'

Section 90A(2) of the Evidence Act 1950 further provides that it may be proved that a document was produced 'in the course of its ordinary use' by tendering to court a certificate signed by a person responsible for either:

(i) the management of the operation of that computer; or
(ii) the conduct of the activities for which the computer was used;

whether before or after the production of the document. That certificate may be stated to the best of the knowledge or belief of the person stating it. Once there is a certificate, it shall be accepted as 'prima facie proof' of all matters stated in it without proof of the signature on it, and there shall arise a presumption that the computer in question was in good working order and was working properly in all respects throughout the material part of the period during which the document was produced.'

So if there were log files or such other forms of digital evidence in the form of a document produced by a computer, such evidence would be admissible. In this case the fact that the log files were deleted and this would mean that that prosecution would need to tender other supporting evidence, failing which the prosecution would not be able to prove its case beyond reasonable doubt.

7.3 CONCLUSION

The above example demonstrates the need for both IT professionals to understand how the law works and for the lawyers, they also need to understand how the system works in order for them to do a proper legal analysis. One cannot do a proper legal analysis without understanding how the act of hacking is done.

11 'Computer' under the CCA means 'an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related device, performing logical arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, or a portable handheld calculator or other similar device which is non-programmable or which does not contain any data storage facility' In subsection 2(10), any reference to a computer 'includes a reference to a computer network'.

12 Function is defined in Section 2(1) as including 'logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer'.

13 Program is defined in Section 2(1) as 'data representing instructions or statements that, when executed in a computer, causes the computer to perform a function'. Under Section 2(10), a reference to a program includes 'a reference to part of a program'.

14 'Data' is defined in Section 2(1) as 'representations of information or of concepts that are being prepared or have been prepared in the form suitable for use in a computer'.

15 The word 'access' itself is not defined in the interpretation section of the CCA although what amounts to unauthorized access is defined in Section 2(5).

16 Section 90A was enacted to bring the 'best evidence rule' up to date with the realities of electronic age according to Mr. Justice Mahadev Shanker JCA in the case of Gnanasegaran a/l Pararajasingam v Public Prosecutor, a decision of the Court of Appeal. at page 14 paragraph A to E

INTRODUCTION TO AUDIO FORENSICS

Audio forensics started in 1941when it was used by the acoustic scientists during World War II as an attempt to identify enemies' voices recorded through telephone and radio.

Figure 1
A Time-Frequency-Amplitude spectrograph

The identification process was done using a Time-Frequency-Amplitude (TFA) spectrograph developed by Bell Telephone laboratory.

The application of audio forensics technologies and methodologies are:

1. Voice identification
2. Listenability analysis
3. Audio enhancement
4. Authentication analysis
5. Sound identification
6. Event sequence analysis
7. Dialogue encoding
8. Other signal analysis

1) Voice identification

Voice identification is the process of comparing a known voice with an unknown voice. The process is to identify the unknown voice or as an attempt to eliminate the known voice as the suspect.

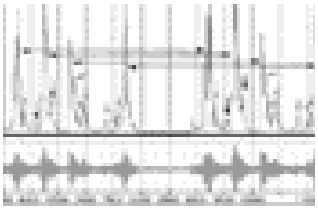


Figure 2
The same pattern revealed in the spectrograph for voice identification

It involves audio signal analysis using the TFA spectrographic and computer. Each individual voice has unique phonetic characteristics that can be identified, analyzed, separated and compared during the identification process.

2) Listenability analysis

The process involves reconstruction of the acoustic event environment if the event can be heard within normal individual listen ability or subject in question. It is crucial to identify whether the acoustic event is listenable or it was produced by other signal (more dominant acoustic event).

3) Audio enhancement

It is a technique used to enhance the listenability or intelligibility of a sound source.

a) Listenability enhancement

Figure 3
Before: The original recording in low amplitude.

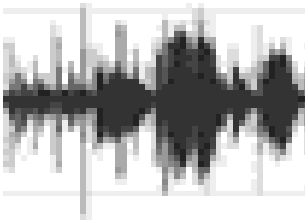


Figure 4
After: By increasing the amplitude of the audio, it is more listenable than the original.

It is a simple procedure by applying equalization, compression or maybe by increasing or limiting the amplitude of an audio recording to make it more listenable.

b) Intelligibility enhancement

It involves more complex process and needs audio engineering tasks. Sometimes it is needed to process a small section of a recording with certain specification and these small sections will be combined back together in exact sequential mirror as the original recording.

Figure 5
Before: The original recording full with hums and buzzes.

Figure 6
After: All hums and buzzes filtered out with

It can produce a spectacular result where it reveals an acoustic event, which is not listenable before the analysis procedure done.

4) Authentication analysis

This analysis used to identify whether a recording has basic similarities with the original acoustic event. Suspicious recording might need authentication through several audio forensics processes and examinations to ensure that it is coming from the same source.

5) Sound identification

Sound identification is a comparison a known sound with an unknown sound in order to identify the unknown sound or an attempt to eliminate the known sound as a suspect. This technique is similar to voice identification. (Please refer figure 2.)

For this type of comparison the original recoding device is needed. Sound identification technique is important

especially during voice or acoustic illusion identification produced from a recording device or an extraneous sound source.

6) Event sequence analysis

This is an analysis on a sequential acoustic event to prove recording components such as timing, frequency and amplitude. This technique can be used to identify the time gap between two gunshots incident were tampered or otherwise. The process can analyse whether the second gunshot is the echo of the first gunshot or whether it was deleted from the recording (tampered recording). The spectrograph analysis will reveal the original when acoustic event took place.

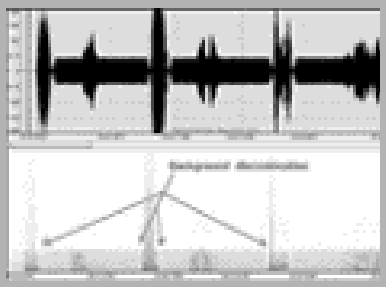


Figure 7
The background discontinuities will reveal using the spectrograph

Event sequence analysis also can be use to identify the authenticity of a recording. For example in an event between A and B recorded inside a tape will be compared to a similar reconstructed event between C and D based on the timing, amplitude, frequency and other relevant factors. This statistical comparison will identify whether the recording has been tampered or vice versa.
Unfortunately, the probability for an acoustic event being duplicated is infinitesimal.

7) Dialogue decoding

It is a process of identifying what was said in a recording. Speech components have patterns, which can be displayed through a spectrograph. Audio forensics analyst can use this technique as to aid them in deciding on word contents and speech.
Vocal chord movement exists inside a voice. Audio forensics analyst can predict the high frequency speech sound such as ‘s’ and also low frequency speech sound such as ‘a’ using spectrograph analysis.
Unfortunately, dialogue decoding is not within the realm of audio forensics but towards speech scientist. It is always the best way for an audio forensics analyst to conduct dialogue-decoding analysis with the presence of speech scientist.

8) Other signal analysis

Audio forensics also can be used to evaluate ‘other’ acoustic event recording that might reveal important information from the investigation such as conversation backgrounds, gunshots, machine and vehicle sounds etc.

Conclusion

Audio forensics can assist an investigation by revealing the information that was uncovered before. It also can assist investigative officers to produce more solid audio evidence from an original recording. However, the audio forensics field remains controversial and faces great opposition in the court of law.

ETHICAL HACKER - THE ICT SIDE OF ACCOUNT AUDITOR

Introduction

Nowadays, we must accept that Information Communication Technology (ICT) has become an essential mechanism in our daily activities. Its evolution has spread not only from the young to the adult but also from social to professional usage. A good example is the personal computer (PC).

There is a PC in almost every home. It has become the equipment a family must have next to the television. The growth on the usage of the PC is phenomenal. Apart from using the spreadsheet software, the PC is being utilized for Internet connectivity. Next, the emails and Internet browsers is required to optimize the usage of the PC.

Not only home users are affected by the ICT, but commercial banking are in dire need to have these PCs and networking gadgets. The scenario is especially true with the foreign banks, as their presence in the local arena are controlled by the government. Therefore, virtual banking is introduced to overcome this limitation.

ICT Attacks

The PC is able to do wonderful things such as software programming, silicon chip designing and other useful product development. On top of this, casual PC use such as for instant messaging, gaming and information gathering via the Internet are the most popular.

However, there are always two sides of a coin. Virus attacks can destroy your PC important files and the worms outbreak may congest you network bandwidth. It is most annoying when it happens.

Network intrusion is another feared term where your system can be compromised. Imagine your virtual banking account is hacked and all the funds are siphoned to another offshore account. This is a serious issue and the users are in a dilemma.

On one hand the ICT is extremely useful and on the other hand it is vulnerable to attacks. How is it mitigated? Perhaps the ICT security topic could at least answer this important question.

Ethical Hacker

What is a hacker? Hacker is a class of people who creates and modifies computer software and computer hardware. The definition also refers to people skilled in computer programming, administration and security.

A black hat hacker, according to Wikipedia, it is a cracker or a dark side of a hacker and is seldom used outside of the security industry.

On the other hand, ethical hacker is a computer and

network expert who attacks a security system on behalf of its owners, seeking vulnerabilities a malicious hacker could exploit. Ethical hackers use the same methods as their less principled counterparts to test the system, but report the problems instead of taking advantage of them. Ethical hacking is also known as penetration testing, intrusion testing or red teaming.

An ethical hacker is sometimes called a white hat, a term that comes from old Western movies, where the "good guy" wore a white hat and the "bad guy" wore a black hat. Ethical hacking has continued to grow in an otherwise lackluster IT industry, and is becoming increasingly common outside the government and technological sectors. Many large companies, such as IBM, maintain employee teams of ethical hackers.

ICT Security

ICT has become the most important tool of any business sectors and social activities. It seems without ICT, these identified sectors would become ineffective and inefficient. Even, almost every Critical Infrastructure (CI) has already integrated with ICT. For example, the power grid has taken Supervisory Control And Data Acquisition (SCADA) system as their core monitoring system and it could be susceptible to black hat attack when connected to Internet.

As a result, many companies are now hiring Security Assurance Analyst to design, monitor and response for any ICT security attacks. From time to time they would be conducting an audit that involves application, network, host, virus management and also the latest wireless. It is more of technical aspects compared to Information Security Management System (ISMS) audit.

Summary

Nowadays, it is common when organization hires an ethical hacker (third party ICT security auditor) to assess its ICT system's security. As a result, the ethical hacker job has become more prevalent. It is comparable to its counterpart that is the accounting auditor. The accounting auditor task is to check whether there is an imbalance in the financial statement. While the ICT auditor is to find if there is any vulnerability in the ICT system's security. It does have some similarities.

ICT forensic is another emerging service in the ICT security. This service involves tracking and identifying the origin of the attacker in an organization's ICT system, which was compromised. Others would include data recovery.

It also important to take note that product evaluation, commonly executed according to Common Criteria (CC) standard is another important area to have some information. It is a technique to proof the concept that the product or system security features are being formally tested for conformance. Procuring a CC evaluated product is a first step to ensure your ICT system's security is going through a thorough setup process.

All of the above mentioned services do involves ICT security experts. During the work some confidential data can either be discovered or required. It is just like account auditor whereby every financial figures of a company is made known or discovered. Therefore, it is important to be ethical when performing this type of work and from this job nature, ethical hacker is most suitable description.

WEB SECURITY EDUCATIONAL TOOLS

Another field of computer security comes to light when the advent of the Internet brings along a technology called the World Wide Web (WWW). At the early presence, this technology seems to be innocent since the protocol it uses called HTTP is stateless in nature. It caters each request independently from previous or upcoming requests. Furthermore, HTTP traffics pass through the network on port 80 are always considered clean by the firewall.

As the time goes by, some advancement on the web technology is added at a regular interval. Online applications are written using some programming languages such as Perl, PHP or VB on top of a web server to cater dynamic contents to the Internet users. These applications may sit on the same server or running from independent application server.

Problems related to web application arise when poor designs, software bugs and poor programming practices often plague applications. It then becomes a target for hackers who may want to do extra damages beside the network by seeking information or doing damages to the data that resides in an application or database.

Educational tools for web security can be used to demonstrate the real threats, which may occur during life production. They can become a playground for web security enthusiasts to exploit known vulnerabilities safely on the mockup application. Amongst those applications, there are three well-demonstrated example applications called WebGoat from OWASP and; Hacme Bank and Hacme Book from Foundstone. They provide easy-to-use learning orientation, credible scenario illustrations and realistic attack lessons with viable solutions.

WebGoat

This application has evolved from a project by OWASP. This group consists of very competent team members and producing real world results for administrators, developers, and security testers. They are also famous with the list of "OWASP Top 10 Web Security Vulnerabilities".

WebGoat is a J2EE web application arranged in a number of security lessons. It is based on Tomcat and JDK 1.5. The package can be downloaded from URL http://www.owasp.org/software/webgoat.html.

Amongst the attacks and solutions provided are cross-site-scripting, SQL injection attacks, thread safety, field and parameter manipulation, session hijacking and management; and weak authentication mechanisms.

Hacme Bank

Hacme Bank simulates a real-world online banking application with a number of known and common vulnerabilities. They are SQL injection (bypassing the login, database modification and command injection in the query), parameter tampering (privilege escalation, unauthorized access, illegal fund transfers and cookie poisoning); and cross-site-scripting to hijack account and

unauthorized access.

This application is built on top of ASP.NET framework and requires Microsoft IIS coupled with Microsoft SQL. Usage of the application requires users to have Internet Explorer 6. The installation file can be downloaded from URL http://www.foundstone.com/s3i.

Hacme Book

Another educational tool from Foundstone is Hacme Book, which is a J2EE application. It is a suitable tool to manipulate Java vulnerabilities plus the source code is made available. The application is running from Apache Tomcat web server with Apache Derby as the embedded RDBMS.

Some of the bugs found will be SQL injection, cross-site-scripting, broken authorization, weak passwords and improper use of crypto. For example, there is an exercise for users to deduce the algorithm for discount codes, which uses the method of substitutions.

Support Tools

In order to maximize the use of above tools, users may need some web tools to analyze and manipulate weaknesses in the application. They can be a web vulnerability scanner such as Nikto; interception proxy such as Achilles, Odysseus or Paros; web spider such as Burp Spider and command line web browser such as Curl.

Conclusion

The web security educational tools can be great tools to manipulate web vulnerability without having to attack the life system on the Internet. Therefore, the amateur security enthusiasts can have some experiences on real life threats that can be exploited through the confined of a local system.

THE EMERGING TREND OF IT OUTSOURCING

IT outsourcing and security

RECENT research from the Gartner Group predicts that while less than 3% of global IT services spending was outsourced in 2004, that figure would jump to 7% by 2008. Such changes in the way businesses operate have brought about new practices in managing IT services.

In recent years, a booming trend of transformation in information technology management has taken place, from in-house HR investments to outsourced services that are accessed when and if needed.

Many corporations outsource their IT functions onshore or offshore. Where the focus was initially on mainframe management and data processing services, it has evolved to cover a broad range of services ranging from software development to network management and information security.

Over the past decade, multinationals that outsourced their IT functions enjoyed substantial cost savings by taking advantage of the skills and lower labour rates in countries such as China and India.

A recent benchmarking study on outsourcing locations in the Asia Pacific region has placed Kuala Lumpur as a “clear favourite” for locating offshore shared service operations. The study, by Deloitte Consulting, also described Malaysia as a “credible challenger” to traditional offshore outsourcing locations such as India, China and the Philippines.

Business transformation outsourcing, however, has not only endowed corporations with greater flexibility in managing projects and an improved cost structure in maneuvering internal IT Services, but also exposed outsourced services to risks by involving intermediaries in the processing of information and applications.

As such, baseline controls and measures are heavily used these days to evaluate the performance of the outsourced IT services. In many cases, a service level agreement (SLA) is used to define the type, value and conditions of outsourcing services to be provided.

This brings about an interactive outsourcing practice, which drives providers to develop and enhance vertical solutions to meet the same quality and performance standards as in-house applications; and at the same time allowing buyers to seek benchmarking services through outsourcing.

While there is a remodeling of the outsourcing process and standards now and then, many prominent international security vendors aim to capture a larger market share and expand their scope of business by offering expertise in outsourcing management services, predominantly to multinational companies.

In Malaysia, security outsourcing like Managed Security Service (MSS) has been adopted chiefly by the financial services sector for the past four years. The objectives are:

- BNM JPI26 and GPIS-1 compliance
- Check and balance between the IT/IS team and MSS provider
- Risk mitigation via proactive intrusion detection and escalation via the MSS provider
- Proactive countermeasure against any cyber threats
- Risk and trend analysis

Generally speaking, outsourcing helps organizations reduce costs. On the other hand, it gives rise to potential problems that should not be overlooked.

Apart from measures to sustain a certain level of standards in outsourced services, cultural differences and political instability have nonetheless come to the forefront in many offshore outsourcing initiatives.

INFORMATION SECURITY ASIA 2006

presents

SecureMalaysia2006

Conference & Exhibition

Concurrent Events:

Asia2006 Conference & Exhibition

RFID ASIA Conference & Exhibition

24 - 26 July 2006
PWTC, Kuala Lumpur

Conference Organised by: (ISC)² NISER

Exhibition Organised by: protemp

Conference Enquiry : [illegible]
Exhibition Enquiry : info@protemp.com.my

Information Security Asia 2006

presents

SecureMalaysia2006 Conference

24 - 26 July 2006 • Putra World Trade Centre, Kuala Lumpur, Malaysia

An (ISC)² Security Leadership Event

Speaker Biographies

ANIL K MAHTANI:
Regional Head, Information Risk Management, ING Insurance Asia/Pacific

Dr. COREY SCHOU:
Prof. of Information & Information Systems, Associate Dean, College of Business, Idaho State University and Vice Chairperson, (ISC)² Board USA

Dr. Corey Schou, honorary CISSP, Vice Chairperson, ISC² Board of Directors, is professor and associate dean for computer information systems programs at Idaho State University, based in Pocatello, Idaho. He is also director of the National Information Assurance Training and Education Center (NIATEC) and the Security Decision Support Center (SDSC). In addition, he is a founder and current chairman of the National Consortium for Information Systems Security Education.

HOWARD SCHMIDT:
Chief Information Security Officer, eBay, and former Cyber Security Advisor to the President of USA, USA

Howard Schmidt, Honorary CISSP, is currently the chief information security officer for eBay and was formerly cyber security advisor to the President of the United States of America. He served as vice chairman of the Bush Administration's Critical Infrastructure Protection Board (CIPB) which developed and introduced the 'National Strategy to secure cyberspace', a plan for protecting the country's most critical systems and networks. Prior to his work on the CIPB, he was the chief security officer for Microsoft Corp, where he managed the secure strategies group.

Lt Col (R) HUSIN JAZRI:
Director of the National ICT Security and Emergency Response Centre (NISER), Malaysia

Lt Col Husin Jazri is currently the Director of the National ICT Security and Emergency Response Centre (NISER), an organisation formed by the National IT Council and operated under the purview of the Ministry of Science, Technology and Innovation, Malaysia. He receives an engineering degree from the University of Hartford, Connecticut, USA, a Post Graduate Diploma in System Analysis from UiTM Shah Alam, Malaysia, Master of Science (with distinction) in Information Security from the Royal Holloway University of London and MBA from University Putra Malaysia, Serdang. He is a Certified Information System Security Professional (CISSP) from ISC², certified BS7799 Lead Auditor, and a visiting lecturer in information security for the University Teknologi Malaysia and Universiti Putra Malaysia. He is also a member of (ISC)² Asian Advisory Board.

BENG CHOW KANG:
Chief Security & Data Privacy Advisor Microsoft, Asia Pacific and Chairman of IT Security and Privacy Standards Technical Committee, Singapore

JOHN MEARN:
Group Head of Information Security, Standard Chartered Bank, UK

John Mearn is a specialist in information security (usable security) with more than eighteen years experience. He has previously been responsible for leading systems security policy and strategy at Reuters, the Royal Bank of Scotland, Swiss Bank Corporation, and the investment banking arm of Dresdner Bank, where he built teams providing a full range of IT security services.

Since mid 2002 he has led a global information security team at Standard Chartered Bank as Group Head of Information Security. Here he is applying his experience in new challenges posed by high geographically and culturally diverse business. He has also provided information security consultancy support to a number of blue chip clients aimed at improving their systems security and effectiveness.

John has a particular interest in better modeling and managing the costs and benefits of security to the business, as well as in shifting the emphasis of commercial security efforts into dynamic management and monitoring rather than basic prevention. He has a PhD in Experimental Solid State Physics from Cambridge University, plays football regularly and builds computers in his spare time. He speaks regularly at conferences and public forums on a variety of topics.

ROLF MOULTON:
President and Chief Executive Officer (Emeritus), (ISC)² USA

Rolf Moulton, CISSP-ISSMP, LISA, CCP, President and Chief Executive Officer (Emeritus), (ISC)² has more than 20 years experience as a Chief Information Security Officer (CISO) at large multi-national organizations where he has developed, implemented and managed comprehensive information risk and security services programs in diverse global, local and government operating environments. His employers have included Unilever, BP America, and the New York City Department of Investigation. He is a respected author and reviewer and has been involved in professional organizations for many years.

STEVE ORLOWSKI:
ex-chair, APEC e-Security Task Group, Australia

Steve Orlowski, from 1997 to 2003 Steve was Chair of the APEC eSecurity Task Group leading its work on the security of information and communications infrastructures and issues relating to cybercrime and the use of electronic authentication. He presented the report Electronic Authentication - Issues relating to its selection and use. In 2000 Steve retired as Special Advisor IT Security Policy in the Information and Security Law Division of the Australian Attorney General's Department. His duties focused on the development and implementation of national and international policies and strategies for the security of information systems including Australia's National Information Infrastructure. He compiled the report Protecting Australia's National Information Infrastructure. Steve has represented Australia at various committees of the OECD, APEC and the United Nations dealing with IT security and electronic commerce issues. He was a member of a number of committees of the Standards Association of Australia dealing with IT security and electronic commerce issues. In July 2004 Steve was awarded the designation Honorary Certified Information System Security Professional (CISSP) in recognition of his profound, positive impact on the information security profession through his work in the Australian Government sector, APEC and the OECD.

Introduction

Without a security policy, the availability of your network can be compromised. The policy begins with assessing the risk to the network and building a team to respond. Continuation of the policy requires implementing a security change management practice and monitoring the network for security violations. Lastly, the review process modifies the existing policy and adapts to lessons learned.
This document is divided into three areas: preparation, prevention, and response. Let's look at each of these steps in detail.

Preparation

Prior to implementing a security policy, you must do the following:
- Create usage policy statements.
- Conduct a risk analysis.
- Establish a security team structure.

Create Usage Policy Statements
We recommend creating usage policy statements that outline users' roles and responsibilities with regard to security. You can start with a general policy that covers all network systems and data within your company. This document should provide the general user community with an understanding of the security policy, its purpose, guidelines for improving their security practices, and definitions of their security responsibilities. If your company has identified specific actions that could result in punitive or disciplinary actions against an employee, these actions and how to avoid them should be clearly articulated in this document.

The next step is to create a partner acceptable use statement to provide partners with an understanding of the information that is available to them, the expected disposition of that information, as well as the conduct of the employees of your company. You should clearly explain any specific acts that have been identified as security attacks and the punitive actions that will be taken should a security attack be detected.

Lastly, create an administrator acceptable use statement to explain the procedures for user account administration, policy enforcement, and privilege review. If your company has specific policies concerning user passwords or subsequent handling of data, clearly present those policies as well. Check the policy against the partner acceptable use and the user acceptable use policy statements to ensure uniformity. Make sure that administrator requirements listed in the acceptable use policy are reflected in training plans and performance evaluations.

Conduct a Risk Analysis

A risk analysis should identify the risks to your network, network resources, and data. This doesn't mean you should identify every possible entry point to the network, nor every possible means of attack. The intent of a risk analysis is to identify portions of your network, assign a threat rating to each portion, and apply an appropriate level of security. This helps maintain a workable balance between security and required network access.

Assign each network resource one of the following three risk levels:
- **Low Risk** Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would not disrupt the business or cause legal or financial ramifications. The targeted system or data can be easily restored and does not permit further access of other systems.
- **Medium Risk** Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause a moderate disruption in the business, minor legal or financial ramifications, or provide further access to other systems. The targeted system or data requires a moderate effort to restore or the restoration process is disruptive to the system.
- **High Risk** Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause an extreme disruption in the business, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore or the restoration process is disruptive to the business or other systems.

Assign a risk level to each of the following: core network devices, distribution network devices, access network devices, network monitoring devices (SNMP monitors and RMON probes), network security devices (RADIUS and TACACS), e-mail systems, network file servers, network print servers, network application servers (DNS and DHCP), data application servers (Oracle or other standalone applications), desktop computers, and other devices (standalone print servers and network fax machines).

Network equipment such as switches, routers, DNS servers, and DHCP servers can allow further access into the network, and are therefore either medium or high risk devices. It is also possible that corruption of this equipment could cause the network itself to collapse. Such a failure can be extremely disruptive to the business.

Once you've assigned a risk level, it's necessary to identify the types of users of that system. The five most common types of users are:

- **Administrators** Internal users responsible for network resources.
- **Privileged** Internal users with a need for greater access.
- **Users** Internal users with general access.
- **Partners** External users with a need to access some resources.
- **Others** External users or customers.

The identification of the risk level and the type of access required of each network system forms the basis of the following security matrix. The security matrix provides a quick reference for each system and a starting point for further security measures, such as creating an appropriate strategy for restricting access to network resources.

System	Description	Risk Level	Types of Users
ATM switches	Core network device	High	Administrators for device configuration (support staff only): All others for use as a transport
Network routers	Distribution network device	High	Administrators for device configuration (support staff only): All others for use as a transport
Closet switches	Access network device	Medium	Administrators for device configuration (support staff only): All others for use as a transport
ISDN or dial up servers	Access network device	Medium	Administrators for device configuration (support staff only): All others for use as a transport
Firewall	Access network device	High	Administrators for device configuration (support staff only): All others for use as a transport
DNS and DHCP servers	Network applications	Medium	Administrators for configuration: General and priviliged users for use
External e-mail server	Network application	Low	Administrators for configuration: All others for mail transport between the Internet and the internet mail server
Internal e-mail server	Network applications	Medium	Administrators for configuration: All other internal users for use
Oracle database	Network application	Medium or High	Administrators for system administration: privileged users for data access: All others for partial data access

Establish a Security Team Structure

Create a cross-functional security team led by a Security Manager with participants from each of your company's operational areas. The representatives on the team should be aware of the security policy and the technical aspects of security design and implementation. Often, this requires additional training for the team members. The security team has three areas of responsibilities: policy development, practice, and response.

Policy development is focused on establishing and reviewing security policies for the company. At a minimum, review both the risk analysis and the security policy on an annual basis.

Practice is the stage during which the security team conducts the risk analysis, the approval of security change requests, reviews security alerts from both vendors and the CERT mailing list, and turns plain language security policy requirements into specific technical implementations.

The last area of responsibility is response. While network monitoring often identifies a security violation, it is the

security team members who do the actual troubleshooting and fixing of such a violation. Each security team member should know in detail the security features provided by the equipment in his or her operational area.

While we have defined the responsibilities of the team as a whole, you should define the individual roles and responsibilities of the security team members in your security policy.

Prevention

Prevention can be broken into two parts: approving security changes and monitoring security of your network.

Approving Security Changes

Security changes are defined as changes to network equipment that have a possible impact on the overall security of the network. Your security policy should identify specific security configuration requirements in non-technical terms. In other words, instead of defining a requirement as "No outside sources FTP connections will be permitted through the firewall", define the requirement as "Outside connections should not be able to retrieve files from the inside network". You'll need to define a unique set of requirements for your organization.

The security team should review the list of plain language requirements to identify specific network configuration or design issues that meet the requirements. Once the team has created the required network configuration changes to implement the security policy, you can apply these to any future configuration changes. While it's possible for the security team to review all changes, this process allows them to only review changes that pose enough risk to warrant special treatment.

We recommend that the security team review the following types of changes:

- Any change to the firewall configuration.
- Any change to access control lists (ACL).
- Any change to Simple Network Management Protocol (SNMP) configuration.
- Any change or update in software that differs from the approved software revision level list.

We also recommend adhering to the following guidelines:

- Change passwords to network devices on a routine basis.
- Restrict access to network devices to an approved list of personnel.
- Ensure that the current software revision levels of network equipment and server environments are in compliance with the security configuration requirements.

In addition to these approval guidelines, have a representative from the security team sit on the change management approval board, in order to monitor all changes that the board reviews. The security team representative can deny any change that is considered a security change until it has been approved by the security team.

Monitoring Security of Your Network

Security monitoring is similar to network monitoring, except it focuses on detecting changes in the network that indicate a security violation. The starting point for security monitoring is determining what is a violation. In Conduct a Risk Analysis, we identified the level of monitoring required based on the threat to the system. In Approving Security Changes, we identified specific threats to the network. By looking at both these parameters, we'll develop a clear picture of what you need to monitor and how often.

In the Risk Analysis matrix, the firewall is considered a high-risk network device, which indicates that you should monitor it in real time. From the Approving Security Changes section, you see that you should monitor for any changes to the firewall. This means that the SNMP polling agent should monitor such things as failed login attempts, unusual traffic, changes to the firewall, access granted to the firewall, and connections setup through the firewall.

Following this example, create a monitoring policy for each area identified in your risk analysis. We recommend monitoring low-risk equipment weekly, medium-risk equipment daily, and high-risk equipment hourly. If you require more rapid detection, monitor on a shorter time frame.

Lastly, your security policy should address how to notify the security team of security violations. Often, your network monitoring software will be the first to detect the violation. It should trigger a notification to the operations center, which in turn should notify the security team, using a pager if necessary.

Response

Response can be broken into three parts: security violations, restoration, and review.

Security Violations

When a violation is detected, the ability to protect network equipment, determine the extent of the intrusion, and recover normal operations depends on quick decisions. Having these decisions made ahead of time makes responding to an intrusion much more manageable.

The first action following the detection of an intrusion is the notification of the security team. Without a procedure in place, there will be considerable delay in getting the correct people to

apply the correct response. Define a procedure in your security policy that is available 24 hours a day, 7 days a week.

Next you should define the level of authority given to the security team to make changes, and in what order the changes should be made. Possible corrective actions are:

- Implementing changes to prevent further access to the violation.
- Isolating the violated systems.
- Contacting the carrier or ISP in an attempt to trace the attack.
- Using recording devices to gather evidence.
- Disconnecting violated systems or the source of the violation.
- Contacting the police, or other government agencies.
- Shutting down violated systems.
- Restoring systems according to a prioritized list.
- Notifying internal managerial and legal personnel.

Be sure to detail any changes that can be conducted without management approval in the security policy.

Lastly, there are two reasons for collecting and maintaining information during a security attack: to determine the extent to which systems have been compromised by a security attack, and to prosecute external violations. The type of information and the manner in which you collect it differs according to your goal.

To determine the extent of the violation, do the following:

- Record the event by obtaining sniffer traces of the network, copies of log files, active user accounts, and network connections.
- Limit further compromise by disabling accounts, disconnecting network equipment from the network, and disconnecting from the Internet.
- Backup the compromised system to aid in a detailed analysis of the damage and method of attack.
- Look for other signs of compromise. Often when a system is compromised, there are other systems or accounts involved.
- Maintain and review security device log files and network monitoring log files, as they often provide clues to the method of attack.

If you're interested in taking legal action, have your legal department review the procedures for gathering evidence and involvement of the authorities. Such a review increases the effectiveness of the evidence in legal proceedings. If the violation was internal in nature, contact your Human Resources department.

Restoration

Restoration of normal network operations is the final goal of any security violation response. Define in the security policy how you conduct, secure, and make available normal backups. As each system has its own means and procedures for backing up, the security policy should act as a meta-policy, detailing for each system the security conditions that require restoration from backup. If approval is required before restoration can be done, include the process for obtaining approval as well.

Review

The review process is the final effort in creating and maintaining a security policy. There are three things you'll need to review: policy, posture, and practice.

The security policy should be a living document that adapts to an ever-changing environment. Reviewing the existing policy against known Best Practices keeps the network up to date. Also, check the CERT web site for useful tips, practices, security improvements, and alerts that can be incorporated into your security policy.

You should also review the network's posture in comparison with the desired security posture. An outside firm that specializes in security can attempt to penetrate the network and test not only the posture of the network, but the security response of your organization as well. For high-availability networks, we recommend conducting such a test annually.

Finally, practice is defined as a drill or test of the support staff to insure that they have a clear understanding of what to do during a security violation. Often, this drill is unannounced by management and done in conjunction with the network posture test. This review identifies gaps in procedures and training of personnel so that corrective action can be taken.

WEATHERING A CRISIS

Have you ever wondered how long it would take your business to get back on track if your IT system crash? What impact would it have on your company's revenue and reputation? How long can you tolerate the downtime? How can you ensure your organisation complies with the regulations, guidelines or best practices directed by the authorities?

A well thought out and properly tested IT Disaster Recovery (ITDR) plan is crucial for dealing with these questions and may potentially damaging circumstances. ITDR plans help ensure an organisation's networks and computer systems are fully functional at all times and continues providing its services without an intolerable delay. But many seem reluctant to implement ITDR plan in their organisations due to the wrong impression that it takes a large commitment in the budget and company resources.

One of the most important factors in developing an ITDR plan is getting full support from top management. Their support and commitment is significant to ensure you have enough budget and the necessary resources throughout the implementation process. But convincing top management certainly isn't easy. You need to properly justify the potential losses and additional expenditure would have to bear as well as returns and long term benefits of having ITDR plan in dealing with a crisis.

After approval from the top management comes the most comprehensive part in developing the ITDR plan - Risk Assessment. The process starts off with the identifying of important assets and is accomplished by assessing the impact of its loss to your organisation. Assets here are not only physical but also include people, key processes and applications amongst others. Next, look into the controls that have implemented. Are they sufficient? If not, identify additional controls to those assets that would minimise those risks. Each weaknesses or vulnerability must be examined and proper countermeasures as well as controls need to be in place.

Another significant process to be conducted is Business Impact Analysis. This process involves identifying critical applications that would cause the greatest impact to your organisation should they fail to function appropriately. The analysis should include an impact study based on adverse scenario such as the total loss to premises, people, records and assets. Recovery Time Objective (RTO) which defines the maximum allowable downtime of these critical business applications will be determined during this process. Recovery strategies are then developed based on prioritised critical applications identified.

The establishment of alternate site is another critical element in ITDR plan. An alternate site is a separate location where business facilities can be accessed by the organisation as a backup whenever the primary site is inaccessible or unreachable. There are, however, several criteria that need to be considered when deciding on a suitable alternate site. While there are various options available, the selection of alternate site is normally based on each organisation's own disaster recovery strategy. It is important to keep in mind that it is not always necessary to have an alternate site fully functioning round the clock.

Upon successfully developing the plan, it is important that the plan be exercised or tested to ensure it works as intended if ever a disaster occurs. The testing phase should also focus on the people handling the system and not just the business assets involved. Not testing an ITDR plan as good as not creating a plan in the first place. The testing phase not only measures the operability of the plan but also lets everyone within the organisation familarise themselves with their roles and responsibilities in the event of a disaster.

The IT DR plan must be consistently reviewed and updated where necessary and the personnel involved should also be notified about the changes.

Awareness and training programmes are also essential for the success of an ITDR and it should be provided to all staff. Employees need to know what the plan is all about and reasons for its existence.

Although there are no legislative on ITDR Plan in place yet, there are regulatory requirements that were set-up by Bursa Malaysia, Bank Negara Malaysia and the Securities Commission for the financial sector. Progressively, Malaysian standard on Business Continuity Management (BCM) is currently being developed by the Working Group on BCM under SIRIM Berhad. It is hoped that the standard would become a catalyst to drive top management in providing full support and commitment towards a successful implementation of BCM in Malaysia, which ITDR Plan provides an integral part.

SECURE SOFTWARE ? FIRST, BACK TO THE DRAWING BOARD

A security development lifecycle for today's software engineer

In the age of information technology, building user trust in computing is a challenge that software engineers and designers can no longer take a court-side view to. Instead, the sheer dependency on computing at work, home or play means that engineers must now step into court action and take a playing role in addressing security threats, and begin rebuilding and preserving widespread trust in computing.

With the imperative for secure software development increasingly driven by market forces, resulting in information

security being a top CIO priority - means there is an increased business need to protect critical infrastructures and the information which it processes. In the real world, software needs to be created to protect itself once implemented and require less updating through patches and burdensome security management.

Sounds all too familiar, you tell me. And no I'm not surprised. In fact, I'm all too aware of the thin line that today's software engineers need to draw between products designed to unleash productivity on the desktop and ever tightening security measures.

As these pressures mount, software engineers need to transition to a more stringent software development process that focuses, to a greater extent, on security. Such a process is intended to minimise the number of security vulnerabilities extant in the design, coding, and documentation, and to detect and remove those vulnerabilities as early in the development lifecycle as possible. The need for such a process is greatest for enterprise and consumer software, especially those open to the internet, to control critical systems likely to be attacked, or to process personally identifiable information.

Let me share with you a prescriptive Security Development Lifecycle process that will help result in more secure software, simply referred to as SDL from here on. We'll look at processes to augment a typical development lifecycle, what stages of development need to be addressed and a set of high-level guiding principles.

I must point out here, that the intention of this SDL is to modify an organisation's processes, not totally overhaul the process. Rather it seeks to integrate well-defined security checkpoints and security deliverables that lead to improved software security. Key to any SDL is implementing repeatable processes that reliably deliver measurably improved security. This will be our focus.

Guiding Principles

The SDL is based on three guiding principles – that software is secure 1) by design, 2) secure by default, and 3) secure in deployment. While all three principles address the development process, the first two – design and default – bring about the most security benefit. Secure by design mandates processes intended to prevent the introduction of vulnerabilities in the first place, while secure by default requires that the default exposure of the software—its "attack surface" be minimised. Secure deployment means that software needs to be designed from the outset to be able to protect itself and the information it processes, and to resist attacks. It also requires engineers to be forward-looking in preparing tools and guidance to accompany the software so that end-users and administrators can use it securely.

Designing Securely

From a security perspective, the key elements of the design phase are:

1. Define security architecture and design guidelines. Define the overall structure of the software from a security perspective, and identify those components whose correct functioning is essential to security (the "trusted computing base"). Identify design techniques, such as layering, use of strongly typed language, application of least privilege, and minimisation of attack surface, that apply to the software. Specifics of individual elements of the architecture will be detailed in individual design specifications, but the security architecture identifies an overall perspective on security design.

2. Document the elements of the software attack surface. All organisations need to determine and balance broad access against limited access to features from a security perspective. This balance can be achieved by making only features used day-to-day by end users accessible by default, and installed with the minimum feasible level of privilege.

   Measuring the elements of attack surface provides an ongoing metric for default security and enables detection instances where the software has been made more susceptible to attack. While some instances of increased attack surface may be justified by enhanced product function or usability, it is important to detect and question each such instance during design and implementation so that the resulting software is in as secure a default configuration as feasible.

3. Conduct threat modeling. Conduct threat modeling at a component-by-component level. Using a structured methodology, identify the assets that the software must manage and the interfaces by which those assets can be accessed. The threat modeling process identifies threats that can do harm to each asset and the likelihood of harm being done (an estimate of risk). Then identify countermeasures that mitigate the risk—either in the form of security features such as encryption, or in the form of proper functioning of the software that protects the assets from harm. Thus, threat modeling helps identify needs for security features as well as areas where especially careful code review and security testing are required. The threat modeling process should be supported by a tool that captures threat models in machine-readable form for storage and updating.

4. Define supplemental ship criteria. While basic security ship criteria should be defined at the organisation level, individual software releases may have specific criteria that

must be met before released. For example, a product team that is developing an updated version of software that is shipping to customers and subject to extensive attack might elect to require that its new version be free from externally reported vulnerabilities for some period before being considered ready for release. (That is, the development process should have found and removed the vulnerabilities before they were reported rather than the product team having to "fix" them after they are reported.)

Once designed by the engineering team, typically, the software is then released to a product team for test implementation. Here the software is coded, tested, and integrated. Steps are taken to remove security flaws or prevent their initial insertion during this phase are highly leveraged — they significantly reduce the likelihood that security vulnerabilities will make their way into the final version of the software that is released to customers.

In the next edition I'll go in depth into the implementation phase of the SDL. We'll look specifically at how the design processes impacts implementation testing.

I'll round off by saying that secure software is possible, and I hope that I've begun to describe ways in which the engineering and design community can make this happen. At Microsoft, we are committed towards investing deeply in people, processes and practices that deliver more secure computing. We continue to innovate and improve our technology. At the same time, sharing our learnings and best practices with you is another step to ensure we all head in the right direction. Happy designing!

IMPLEMENTING ASSET MANAGEMENT IN ORGANIZATION

Information security is the preservation of confidentiality, integrity and availability of information. We need information security to protect information from a wide range of threats such as malicious code, hacking, fraud, espionage, sabotage, vandalism and natural disasters. This is important to maintain organization's business continuity, competitive edge, profitability, legal compliance, and image.

Information security can be achieved by implementing a suitable set of controls. This includes policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature. In implementing Information Security Management System (ISMS), these controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the information security of the organization can be achieved. This article will discuss Asset Management as one of controls for the implementation of ISMS.

Asset Management is one of the eleven domains in ISO/IEC 17799:2005. This article will give brief guidance on the implementation of the Asset Management as one of the security controls in organization. Among others are requirements for inventory of assets, assigning ownership of assets and information classification.

Inventory of assets

Identification of assets is a crucial part in asset management. It is important to know the organization's assets, their locations and value in order for us to decide the amount of time, effort or money we should spend on securing the assets. All assets should clearly be identified and an inventory on important assets should drawn up and maintained. This inventory should include all necessary information to recover from any security incident, including types of assets, format, locations, business value, backup information and license information and also the ownership. This inventory of assets should not duplicate other inventories unnecessarily, but it should be ensured that the content is aligned.

What exactly is an asset? Is it the hardware, the software or the database? We can broadly classify assets in the following categories:

a. Information assets
   - Every piece of information about your organization falls in this category. This information is collected, classified, organized and stored in various forms. Among others are databases and data files, contracts and agreements, system documentation, training material, user manuals, audit trails and operational procedures.

b. Software assets
   - Software assets could be application software, system software, development tools and utilities

c. Physical assets
   - These are the visible and tangible equipment and could comprise of computer and communication equipment and removable media.

d. Services
   - Services include computing and communication services and general utilities such as lighting, heating and air-conditioning.

e. People
   - People and their qualification, skills and experience.

f. Intangible
   - Intangibles such as reputation and image of the organization.

Ownership of assets

A more difficult task is to establish ownership for the assets. There will be a number of users for these assets. The prime responsibility will lie with the asset owner. The owner of assets refers to individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of assets. The asset owner should be responsible for ensuring that assets are appropriately classified and also responsible for defining and reviewing access restrictions and classifications. The identification of the asset owner is also an important step for one more reason. Only an owner of the asset will be able to decide the business value of the asset. Unless the correct business value of the asset is known, we cannot identify the security requirement of the asset. Routine tasks may be delegated, for example to a custodian looking after the asset on a daily basis, but the responsibility remains with the owner.

Information classification

The next task is to create classification levels. The objective of information classification is to ensure the information receives an appropriate level of protection. Information should be classified to indicate the need, priorities, and expected degree of protection when handling information. What are the criteria that we should look for when performing the information classification? Some of the criteria could be:

a. Confidentiality
   - Confidentiality may define whether the information is freely distributed or only restricted to certain individuals.

b. Value
   - Classification based on value could be high, medium or low. A detailed explanation should be prepared giving the reasoning for this classification.

c. Time
   - Information often ceases to be sensitive or critical after a certain period of time, for example when the information has been made public. These aspects should be taken into account, as over-classification can lead to the implementation of unnecessary controls resulting in additional expenses.

d. Access rights
   - Access rights need to be defined for individuals as well as groups.

e. Destruction
   - Destruction should be a scheduled and controlled activity.

Classification schema should lead to a structure that could be implemented. It should be simple to understand and identify. A practical implementation of classification schema is very important. The classification label should not give an easy way of identification, which could be misused. It should provide the right amount of protection.

Conclusion

Asset management can be a time-consuming and complex task, but it is crucial to implement to ensure that organization's assets achieve appropriate protections. Even though, it is a less glamorous aspect of information security, asset management is the key to various security controls that need to be implemented for achieving information security in an organization.

COMPLETING THE EQUATION: THE PEOPLE FACTOR- MAKING AWARENESS YOUR SECURITY TOOL

Often enough we hear about three very distinct words spoken when it is in relation to Information Security; PEOPLE, PROCESS & TECHNOLOGY. While these three terms are often told and spoken of, you will notice that processes are continuously being refined and new technology is always emerging as new threats are being introduced. PEOPLE is what is missing.

The people factor is often left out of the equation simply because people are the ones developing these new technologies, they are the ones refining and creating processes, they are implementing the policies, designing the architecture, writing the rules, etc. Sadly, they are also the ones breaking the rules and attacking the systems. In addition to being targeted by the attackers.

The number one threats today are users who unaware of the risks, threats and their magnitude. Attackers who, used their system as launching pads target these naïve users. Many users today are simply not aware of issues such as social engineering, email attachments, anti-virus updates, P2P applications, instant messaging, etc. All these are platforms for attackers to exploit and channel malicious codes that can spread across the network in just minutes.

We also have another group of people made up of system administrators, power users, developers, network administrators, etc. What's their excuse? "I don't have time for backups, updates, etc". These are savvy but at times ignorant and careless users. We have heard cases on system administrators not changing default passwords, developers not using proper design methodology or deploying software that was not properly tested and so on. These are also avenues for attackers.

Finally, we have the management group who thinks information security is an expensive area and crops a hole into their profits.

Expenditure in this area is often thought of last should there be a balance or only after their system is attacked. They feel this area is not important because it does not generate revenue rather is a liability. Priorities are always given to other more important areas that are considered revenue streams.

Various surveys carried out globally show, human errors are usually the root cause of most security breaches rather than the technology itself. In one of the surveys, "Information Security Breaches Survey 2004" conducted by PricewaterhouseCoopers on behalf of the UK Department of Trade and Industry (DTI), some interesting findings are:

1. One in ten companies have staff with formal information security qualifications.
2. Expenditure on Information Security is increasing but it is still relatively low as seen as a cost rather than as an investment
3. Many organizations have waited until an incident hits them before putting counter-measures in place.

Sadly, there is a lack of awareness on the risk, threats and the magnitude of these risks and threats faced today.

How does awareness fit into this equation? If we have the proper tools and processes, then what is lacking is education. Tools can be bought and processes can be created but people need to be educated, which is an ongoing process that can help solve some if not all of the security breaches. As the saying goes "Security Is Everyone's Responsibility", which is true because defending a fortress requires everyone's participation.

Security awareness is the knowledge of potential risks and threats. It gives users the advantage of knowing the types of security issues and incident members of our organization may face in the day-to-day routine of their functions. The greater the awareness, the greater the defense becomes. Knowing what you are facing will give you the advantage of knowing how to defend before it happens and not after it happens.

As more organizations are seeing the importance of security policies, it is also critical to disseminate it to all its employees and third party who work for or on behalf or the organization. As security policies emphasize on staff's roles and responsibilities, these information must be correctly and comprehensively disseminated through effective and vibrant modes of delivery.

The audience has diverse experiences, backgrounds and job responsibilities. The awareness goal at the decision-making level is to convince the audience that information security and privacy risk reduction is achievable. Awareness goals at the end user level are to help them understand information security and privacy risks and the actions to reduce them. Another end user goal is to create a demand for risk reduction.

The next step is for organizations to start planning for a corporate wide security awareness program, which should be an ongoing exercise. The critical success of any information security program will include people, awareness and personal responsibility.

Firstly, in order to make awareness an effective security tool, is to get management commitment. This is crucial as it involves costs and everyone's involvement to make it successful. To get management commitment is to do a risk and business impact analysis to show the figures should a security breach occur.

Half the battle is won once there is support from the management. Now, a comprehensive plan should be in place for a corporate wide awareness program. The plan should address issues such as:

- Role of the organization in the program
- Role of staffs in the program
- Awareness program scope
- Audience segmentation
- Objectives of the program
- Content of the program
- Effective Modes of delivery

The key objectives towards the implementation of an effective security awareness program are:

1. to identify the key ingredients in a successful training and awareness program.
2. to define, segment and target key groups for focused trainings. Bearing in mind that the corporate wide awareness program should target staff at all levels. This is very important as focused groups will ensure proper implementation and create a balance for a long-term sustainability.
3. to gather and organize a wide variety of techniques and materials for maximum impact. One of the key success factors lies on the mode of delivery. Choosing the right mode is crucial as the impact on the individual will determine the level of awareness.
4. to evaluate the results of your security awareness program. This is to help make future programs better and more successful.

Awareness programs should be interesting to capture the audience's attention and make them remember. Some of the things to make it interesting include:

- Use analogies
- Use recent, significant real-world examples and news events
- Explain the importance of your message

- Use scenarios and multifaceted situations (e.g. what would you do if?)
- Use graphics
- Use photos and videos
- Make it interactive

- Make it memorable
- Make it personal
- Make it fresh
- Provide practical, “job-ready” information
- Use known people in examples
- Use animations
- Recognize employees who have done an outstanding job
- Use games and challenges

Another important aspect to remember is that the awareness programs should remain current, as it is an ongoing. As information security policies and privacy regulations change the employees must be informed. Therefore, it is important that current information be disseminated as well.

Information that is disseminated should not be confusing and vague. It should be clear, concise and simple to understand. We should always remember that the audiences are lay people. Therefore, information should be in lay terms.

Information on security issues and user’s roles and responsibilities should be put at prominent places and must be made easily accessible. Educate your users with current news via email or bulletin board postings. Put up posters and have online quizzes. There are many ways and you have to determine what fits in your organization.

In conclusion, the people factor is a very important part of the equation and equipping them with the right security tools is as important. Awareness is a very important process that translates into a security tool for employees. This helps reduce incidents within the organizations and make people be more aware of their roles and responsibilities as employees of the organization in safeguarding their information asset.

SECURITY IS EVERYONE’S RESPONSIBILITY

No	Event	Venue	Date
1	Corporate Security Management 2006	San Jose, Costa Rica	24 – 26 April 2006
2	BAPCO Public Safety Communication and IT Exhibition & Conference,	London, UK	26 April 2006
3	DallasCon 2006 - Information & Wireless Security Conference	Texas, USA	1 – 6 May 2006
4	IT Governance 2006	Kuala Lumpur, Malaysia	9 – 10 May 2006
5	CardTech SecurTech Conference and Exhibition	Louisiana, USA	9 – 11 May 2006
6	SANS Security Conference 2006	San Diego, CA	11 – 16 May 2006
7	International Wireless Communications Expo	Nevada, USA	17 – 19 May 2006
8	Cyber Security Summit	FL, USA	22 – 23 May 2006
9	World Wireless Congress	California, USA	24 – 26 May 2006
10	INSS 2006: 3rd International Conference on Networked Sensing Systems,	Chicago, USA	31 May – 2 June 2006
11	Management of Change Conference	South Carolina, USA	4 – 7 June 2006
12	SUTC 06: Int.nl Conference on Sensor Networks, Ubiquitous and Trustworthy Computing	Taichung, Taiwan	5 -7 June 2006
13	Gartner Security Summit 2006	Washington DC, USA	5 – 7 June 2006
14	ACNS 06: 4th International Conference on Applied Cryptography and Network Security	Singapore	6 – 9 June 2006
15	ICC 06: IEEE International Conference on Communications - Network Security and Information Assurance	Istanbul, Turkey	11 – 15 June 2006
16	IDC's Asia Pacific Security and Continuity Conference 2006	Kuala Lumpur, Malaysia	21 June 2006
17	ACISP 2006: 11th Australasian Conference on Information Security and Privacy	Melbourne, Australia	3 – 5 July 2006
18	19th IEEE Computer Security Foundation Workshop	Venice, Italy	5 – 7 July 2006
19	CRYPTO 2006: The 26th Annual International Cryptology Conference	Santa Barbara, USA	20 – 24 Aug 2006
20	ISC 2006: Information Security Conference	Samos Island, Greece	30 Aug – 2 Sept 2006
21	E-Security Expo and Forum	Kuala Lumpur, Malaysia	5 - 8 Sept 2006
22	Infosecurity Conference & Exhibition	New York, USA	23 – 25 Oct 2006

TRAINING CALENDAR 2006

May 2006

Date	Title	Venue
02 – 03	Information Security Management System (ISMS)	Kuala Lumpur
22 - 26	CISSP CBK Review Course	Kuala Lumpur

June 2006

Date	Title	Venue
19 - 23	Business Continuity Planning (BCP)	Kuala Lumpur
24	CISSP Exam	Kuala Lumpur

July 2006

Date	Title	Venue
17 - 18	Security Awareness	Kuala Lumpur

August 2006

Date	Title	Venue
14 – 18	CISSP CBK Review Course	Kuala Lumpur

September 2006

Date	Title	Venue
11 - 12	Information Security Management System (ISMS)	Kuala Lumpur
16	CISSP Exam	Kuala Lumpur

November 2006

Date	Title	Venue
13 - 14	Security Awareness	Kuala Lumpur

December 2006

Date	Title	Venue
2	CISSP Exam	Kuala Lumpur
4 - 8	Business Continuity Planning (BCP)	Kuala Lumpur
18 – 20	Incident Handling & Response	Kuala Lumpur

The Official (ISC)² CISSP® CBK® Review Seminar and Examination

Why CISSP® Certification?

The CISSP Certification is an independent and objective measure of professional expertise and knowledge within the information security profession. In June 2004, the International Organization for Standardization's (ISO) United States representative, ANSI (American National Standards Institute), has granted certification accreditation in the area of information security under ISO/IEC 17024 for CISSP credential.

If you plan to build a career in information security - one of today's most visible professions - and if you have at least four full years of experience, then CISSP Certification should be your next career goal.

HOW CISSP® BENEFITS YOU

The CISSP® credential is a key differentiator in the selection process for information security positions, new assignments or promotions. When you achieve the CISSP® designation:

- You indicate you have measured up to a globally accepted professional and ethical standard.
- You have recognition and acceptance as a career professional.
- Your career opportunities are significantly enhanced.
- You have demonstrated knowledge of and competence in the 10 domains of the information system security common body of knowledge (CBK).
- You possess an internationally recognized credential.

HOW CISSP® BENEFITS YOUR ORGANIZATION

Organizations staffed with CISSPs gain a competitive edge. Because the personnel protecting their data are the best in the business, these organizations demonstrate to customers, suppliers, and employees alike, the importance they place on security. Additionally, the CISSP® designation reflects a properly and consistently trained IT professional staff.

Are You Certified?

Learn from the world renowned experts, and get certified via the Official (ISC)® CISSP® CBK® Review Seminars and Examination!

The Official (ISC)² CISSP® CBK® Review Seminar

Most practitioners specialize in only one or two of the CBK domains, and typically have varying degrees of knowledge in the others. Knowledge of all 10 domains is required to pass the exam. For this reason (ISC)² has developed this intensive, five-day review seminar that will broaden your understanding of all 10 domains and that will help you succeed on the CISSP exam.

The Seminar provides:

- extensive work from CISSPs, (ISC)² instructors and Subject Matter Experts in developing material and presentation;
- 100% revised, updated or new material;
- a practice exercise with 100 questions that are representative of the actual exam;
- a personal critique of your results to help you focus on the topics where you need more study;
- a comprehensive student guide that addresses all materials covered by the course.

40 Hour Course Outline

The course material, covering the 10 CISSP domains of the CBK, is redesigned and updated for every Review Seminar to reflect the latest information system security issues, concerns, and countermeasures. The following domains are covered in the seminar modules.

- **Security Management Practices**
- **Security Architecture and Models**
- **Access Control Systems and Methodology**
- **Application Development Security**
- **Operations Security**
- **Physical Security**
- **Cryptography**
- **Telecommunications, Network, and Internet Security**
- **Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)**
- **Law, Investigations, and Ethics**

HOW TO DECIDE IF YOU NEED THE CBK REVIEW SEMINAR

To test your knowledge of the 10 domains, you can download the free Official (ISC)² CISSP® CBK Study Guide from the (ISC)² website. It will help you to evaluate your strong and weak areas and to determine if you should attend the CBK Seminar.

2006 SEMINAR in Malaysia
22 – 26 May 2006
14 – 18 August 2006

Venue: Hilton, Petaling Jaya
Duration: 40 hours in 5 days
Time: 08:30 - 17:30
Course Fee: RM 3800

2006 EXAMINATION in Malaysia
24 June 2006
16 September 2006
2 December 2006

Venue: UCTI – University College of Technology & Innovation (APIIT), Technology Park Malaysia, Bukit Jalil, Kuala Lumpur
Exam Fee: US$ 499 (Received 16 days prior to exam date)

http://www.isc2.org

https://www.niser.org.my/cissp

CISSP CBK Review Seminar Class of 2005








REPORTING INCIDENTS TO MyCERT

Tel	:	60 3 8996 1901
Fax	:	60 3 8996 0827
Via email	:	mycert@mycert.org.my
Via 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

NISER
National ICT Security and Emergency Response Centre

MyCERT
Malaysian Computer Emergency Response Team