CyberSecurity MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 29 - (Q4/2011)

ISO / IEC 27001

Implementing ISO/IEC 27001: Choosing an ISMS Consultant
Mobile Devices Asset Classification in ISO 27001 Implementation
Tracing Cyber Criminals Via Full Headers

KDN License number PP 15526/10/2012(031392)

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards"

Gene Spafford

ISSN 1985-1995

CEO MESSAGE

By the end of 2011, CyberSecurity Malaysia has documented up to 15,218 cyber incident cases; that clearly dwarfed reported incidents of the previous year by a massive 88%! Up to February 2012, the incidents have risen to 954. It is important to remind ourselves that these astounding numbers had only represented the reported ones. If anything, this has only further proves that cyber incidents are on the rise – big time.

On another note, the Gartner Predicts 2012 special report anticipates the financial impact of cybercrime will grow by 10 percent each year until 2016, due to the continuing discovery of new vulnerabilities and attack methods by financially-motivated hackers. Unfortunately, this in turn will lead to continued growth in bottom-line financial impact because of the successful cyber attacks.

For CyberSecurity Malaysia, cyber security is never exclusively about securing the Critical National Information Infrastructure (CNII), gateways, Internet backbones and web services. We have long come to terms that nowadays, cyber criminals, hackers and hacktivists will be targeting almost everything under the sun, of all shapes and sizes – as long as they are connected to the cyber space.

Subsequently, incidences such as DDoS attacks or website defacements will prove to be more than just “annoyances”; especially when they later escalate to data breach and theft, such as the one embarrassingly suffered by Sony Corp.'s PlayStation Network and Sony Online Entertainment last April. And we have seen how such attacks did hurt the reputation and credibility of said business entity, which will ultimately incur losses, in terms of damages, infrastructure overhaul, potential revenue and most importantly, its customers’ trust.

This e-Security bulletin publication is one of our many efforts to instill a correct perspective on issues and matters related to cyber security. The society at large must be made aware of the real dangers, risks and tools that exist in the borderless, wireless and, to a certain extent, seemingly lawless virtual world out there.

This is our challenge for the upcoming years ahead. Our efforts shall not be in isolation of the nation’s agenda. We, cyber security professionals will have to work harder towards garnering enough attention to the importance of cyber security and its role in supporting towards the realization of Digital Malaysia, one of the key components of National Transformation Programme. All of which can only be achieved by first ensuring a robust, safe and secure cyber space is in place. Such efforts will not be just for e-commerce but also for businesses in general; and thus cementing the position of cyber security as a significant technology foundation that nobody can afford to do without.

Until next time, have a prosperous and secure year ahead. Thank you.

Thank you and warmest regards,
Lt Col Prof Dato’ Husin Jazri (Retired) CISSP CBCP CEH ISLA
CEO, CyberSecurity Malaysia

EDITOR’S DESK

Greetings,

Security proponents used to say that Information Security is journey rather than a destination. This endeavor requires information security practitioners to be vigilant and always proactive in dealing with today’s cyber threats. In the home front, cyber incidences still remain significant but without big attention as compared to the 2011’s anonymous attack to the Malaysian Government websites. Protecting the Critical National Information Infrastructure (CNII) against cyber attack remains the dominant topic amongst information security professionals.

To comply with the government ruling to mandate all CNIIs to be ISO/IEC 27001 certified by first quarter 2013, many agencies are working very hard in achieving the certification. Many agencies opted to engage Information Security consultants to ensure they are ready for ISMS certification audit. In this issue, we give some tips in selecting an ISMS consultant, what is expected out of them and some characteristics of a credible ISMS consultant.

Mobile devices will remain a ‘cool’ thing to use in our daily life be it gadgets that are provided by the organization or privately owned by individuals of the organization. This new trend is also known as ‘Bring you own devices – BOYD). Use of these devices, bring together with some risk issues when classified information are stored and transmitted via the devices. In this issue, we provide some insight on how to perform asset classifications in line with ISO 27001 implementation.

We presented an insight of how to trace cyber criminal in the article entitled “Tracing Cyber Criminals via Full Headers”. The article highlighted the importance of analyzing the email header to affirm how packets are transferred from point A to Point B and to investigate whether there are any malicious packets delivered in stealthy manner.

In this issue, our guest author would like to feature a paper that dwell in cloud computing particularly in dealing with cloud providers that could not match the security expectation of an organization seeking the cloud services. The author shares with us tips in handling security issues that relates to network security, physical security and blind spot in the communication between any data centre and end-user.

We invite contribution from everyone for our future issue. Thank you and best regards.

Asmuni Yusof
Lt Col Asmuni Yusof (Retired), Editor

TABLE OF CONTENTS

READER ENQUIRY
Security Managment and Best Practices, CyberSecurity Malaysia, Ministry of Science, Technology and Innovation (MOSTI) • E-mail: smbp@cybersecurity.my

PUBLISHED AND DESIGN BY
CyberSecurity Malaysia (726630-U)
Block A, Level 8, Mines Waterfront Business Park, No 3,
Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor Darul Ehsan.

MyCERT 4th Quarter 2011 Summary Report

Introduction

The MyCERT Quarterly Summary Report provides an overview of activities carried out by the Malaysian Computer Emergency Response Team (hereinafter referred to as MyCERT), a department within CyberSecurity Malaysia. These activities are related to computer security incidents and trends based on security incidents handled by MyCERT. The summary highlights statistics of incidents according to categories handled by MyCERT in Q4 2011, security advisories and other activities carried out by MyCERT personnel.

The statisticsprovided in this report reflect only the total number of incidents handled by MyCERT and not elements such as monetary value or repercussions of the incidents. Computer security incidents handled by MyCERT are those that occur or originate within the Malaysian constituency. MyCERT works closely with other local and global entities to resolve computer security incidents.

Incidents Trends Q4 2011

Incidents were reported to MyCERT by various parties within the constituency as well as from foreign sources, which include home users both local and foreign, private sector entities, government sector, security teams from abroad, foreign CERTs, Special Interest Groups including MyCERT's proactive monitoring on specific incidents such as Intrusions.

From October to December 2011, MyCERT, via its Cyber999 service, handled a total of 3,288 incidents representing a 27.35 percent decrease compared to the previous quarter. In Q4 2011, incidents such as Intrusions, Intrusion Attempts and Cyber Harassment showed an increase compared to the previous quarter while other types of incidents had considerably decreased.

Figure 1 illustrates incidents received in Q4 2011 classified according to the type of incidents handled by MyCERT.

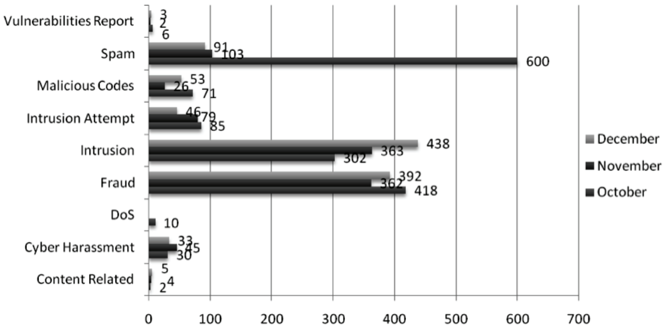

Figure 1: *Breakdown of Incidents by Classification in Q4 2011*

Figure 2 illustrates the incidents received in Q4 2011 classified according to the type of incidents handled by MyCERT and its comparison with the number of incidents received in the previous quarter.

Categories of Incidents	Quarter		Percentage
	Q3 2011	Q4 2011	
Intrusion Attempt	189	209	10.58
Denial of Service	14	1	-92.86
Spam	1646	299	-81.83
Fraud	1355	1153	-14.91
Vulnerability Report	17	11	-35.29
Cyber Harassment	80	105	31.25
Content Related	14	11	-21.43
Malicious Codes	233	142	-39.06
Intrusion	978	1357	38.75

Figure 2: *Comparison of Incidents between Q3 2011 and Q4 2011*

Figure 3: Shows the percentage of incidents handled according to categories in Q4 2011.

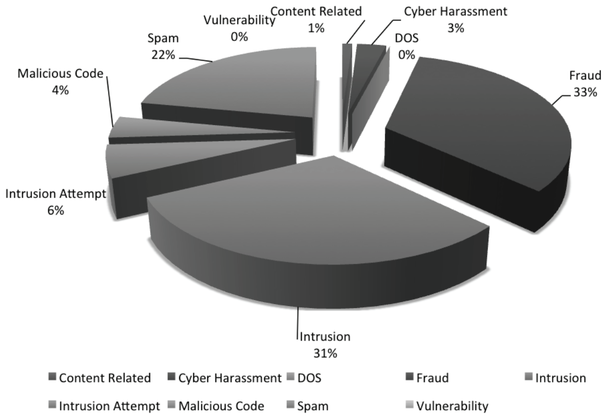

Figure 3: *Percentage of Incidents in Q4 2011*

In Q4 2011, a total of 1,357 incidents on Intrusion representing a 38.75 percent increase compared to previous quarter. Most of these Intrusion incidents are web defacements, also known as web vandalism followed by account compromise. Web defacements are referred to as unauthorised modifications to a website with inappropriate messages or images with various motives by the defacer. This was made possible due to vulnerable web applications or unpatched servers involving mostly web servers running on IIS and Apache with a few others involving other platforms.

In this quarter, we received a total of 565 .MY domains defaced with the majority involving .COM.MY and .COM domains belonging to the private sector. The defaced domains were hosted on single servers that host single domains as well as on virtual hosting servers that host multiple domains, belonging to local web hosting companies. These web defacements were successfully controlled. MyCERT advised System Administrators on steps to rectify and recover from these defacements.

As was in the previous quarter, MyCERT observed that the majority of web defacements were done using the SQL injection attack technique.

More information about SQL Injection technique and fixes is available at: http://www.mycert.org.my/en/resources/web_security/main/main/detail/573/index.html

Figure 4 shows the breakdown of domains defaced in Q4 2011.

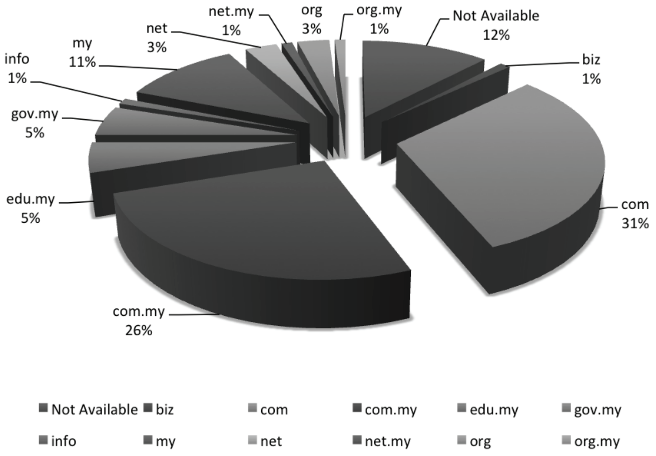

Figure 4: *Percentage of Web Defacement by Domain in Q4 2011*

Account compromise refers to unauthorised access or ownership to another account via stolen passwords or the act of sharing passwords for various malicious motives. The account compromise reported to us mainly involved free-based email and social networking accounts. The compromised accounts will then be used in malicious activities on the net such as in Nigerian scams, impersonation and cyber harassment. Based on our observation, account compromise incidents are mainly due to poor password management practices such as using weak passwords and the act of sharing passwords. As such we advise users to practice good password management to prevent their accounts from being compromised.

Users may refer to the below URL on good password management practises:
http://www.auscert.org.au/render.html?it=2260
http://www.us-cert.gov/cas/tips/ST04-002.html

Fraud incidents had decreased to about 14.91 percent in this quarter compared to the previous quarter. The majority of fraud incidents handled were phishing attacks involving foreign and local brands with the rest of fraud incidents consisting of Nigerian scams, lottery scams, illegal investments, job scams and fraud purchases. The reason for the decrease could possibly be due to more awareness among Internet users of scam activities.

A total of 1,153 incidents were received on fraud activities in this quarter, from organisations and home users. A total of 241 phishing websites involving domestic and foreign brands were reported to us in this quarter with the majority of them belong to local brands. In this quarter, we observed an increase in local Islamic Banking entities becoming target of phishing activities compared to previous quarters. MyCERT handled both the source of the phishing emails as well as the removal of the phishing sites by communicating with the respective Internet Service Providers (ISPs).

Based on our analysis, the majority of the phishing sites were hosted on compromised machines besides phishers hosting them on purchased or rented domains. The machines may had been compromised and used to host phishing websites and other malicious programmes on it.

As was in the previous quarter, incidents on job scams and fraud purchases continue to increase with fraudsters using the same modus operandi.

We continue to receive incidents on cyber harassment in this quarter with a total of 105 incidents representing a 31.25 percent increase compared to the previous quarter. Harassment reports mainly involved cyberstalking, cyberbullying and threatening. Many of cyberharassment victims are people known to the perpetrators such as their friends, relatives, colleagues. etc. Threats via emails, blogs and social networking sites are prevalent in this quarter in which victims are threatened to pay money to individuals they just got to know on the net. If they refuse,their pictures will be exposed or uploaded on porn websites. MyCERT advised users to be very careful with whom they befriend with and never provide their personal details or photos to a third party on the net as details of such materials can be used for malicious activities.

In Q4 2011, MyCERT handled 142 incidents on malicious codes, which represents a 39.06 percent decrease compared to the previous quarter. Some of the malicious code incidents we handled are active botnet controllers, hosting of malware or malware configuration files on compromised machines and malware infections to computers.

Advisories and Alerts

In Q4 2011, MyCERT had issued a total of two advisories and alerts for its constituency which involved popular end -ser applications such as Adobe PDF Reader and Multiple Microsoft Vulnerabilities.

Attackers often compromise end-users' computers by exploiting vulnerabilities in the users' applications. Generally, the attacker tricks the user in opening a specially crafted file (i.e. a PDF document) or web page.

Readers can visit the following URL on advisories and alerts released by MyCERT
http://www.mycert.org.my/en/services/advisories/mycert/2011/main/index.html

Other Activities

In Q4 2011, MyCERT wasinvited to conduct an Incident Handling training session for OIC-CERT Conference participants in Brunei. The training was held from 21 – 25 November 2011 focusing on Incident Handling, network and web security. The participants were mostly from the CERT of their respective countries. MyCERT staff had also presented findings at the Homeland Security Conference in Malaysia on topics concerning CyberSecurity Incidents in October 2011 and also at the Indonesian Information Security Forum on CERT/CC in December 2011. Other presentations were on MyCERT Experience in Handling Child Online Related Issues at Seminar Child Online Protection in October 2011 and a keynote address at the Cloud Computing Conference in November 2011 on Are We Ready to Go Into Cloud Computing? Another keynote address was also given at the ARADO CyberSecurity Seminar in December 2012 on CyberSecurity Trends and Technology.

Another important activity that was held in Q4 2011 was the country's fourth annual Cyber Drill, codenamed **X-MAYA4**, a simulated and coordinated exercise to assess the cyber security emergency readiness of Malaysia's Critical National Information Infrastructure (CNII) to cope against cyber attacks. This year's Cyber Drill scenarios involved two cyber security emergency incidences: web defacement and malware infection in which the players were required to identify the origin of the attacks, take minimising and mitigating steps, and rectify the defacement and/or outbreak.

Conclusion

Basically, in Q4 2011, the number of computer security incidents reported to us had decreased compared to the previous quarter. In addition, most categories of incidents reported to us had also decreased. The decrease is also a reflection that more Internet users are aware of current threats and are taking proper measures against these threats. It could also probably be due to the absence of significant attacks on the net specifically to Malaysian constituency. No severe incidents were reported to us this quarter and we did not observe any crisis or outbreak in our constituencies. Nevertheless, users and organisations must be constantly vigilant of the latest computer security threats and are advised to always take measures to protect their systems and networks from these threats.

Internet users and organisations may contact MyCERT for assistance at the below contact:

E-mail: mycert@mycert.org.my
Cyber999 Hotline: 1 300 88 2999
Phone: (603) 8992 6969
Fax: (603) 8945 3442
Phone: 019-266 5850
SMS: Type CYBER999 report <email> <report> & SMS to 15888
http://www.mycert.org.my/

Please refer to MyCERT's website for latest updates of this Quarterly Summary. ■

CyberCSI 4th Quarter 2011 Summary Report

Introduction

The CyberCSI's Fourth Quarter Summary Report provides an overview of activities undertaken by the Digital Forensics Department (hereinafter referred to as DFD) of CyberSecurity Malaysia for the month of October, November and December 2011. The activities for this quarter are more focused on ASCLD/LAB Accreditation and case analysis received from law enforcement agencies (hereinafter referred to as LEAs) and regulatory bodies (hereinafter referred to as RBs) such as Royal Malaysian Police (RMP), Malaysian Anti-Corruption Commission (MACC), Malaysian Communications and Multimedia Commission (MCMC) and the Securities Commission Malaysia (SC). This summary will also highlight the training sessions and talks given to LEAs, RBs and public based organisations on digital forensics modules.

The 1st Digital Forensic Laboratory Accredited With ASCLD/Lab in Asia

ASCLD/LAB was originally created as a committee of its mother organisation, the American Society of Crime Laboratory Directors (ASCLD) in 1998. It was created as a voluntary programme and remains one today. It offers voluntary accreditation to public and private crime laboratories in the United States and around the world. Accreditation is offered in forensic disciplines for which services are generally provided by forensic laboratories.

The American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) is the oldest and most well known crime/forensic laboratory accrediting body in the world. ASCLD/LAB has been accrediting crime laboratories since 1982 and currently accredits most federal, state and local crime laboratories in the United States including forensic laboratories in six other countries.

Before laboratories were accredited, ASCLD/LAB established four objectives for its programme. The four objectives have remained unchanged since the inception of the programme. ASCLD/LAB subsequently established a Quality Policy Statement and a Statement of Guiding Principles for Forensic Scientists and Forensic Laboratories.

The objectives of the ASCLD/LAB accreditation programme are:

1. To improve the quality of crime laboratory services provided to the criminal justice system.
2. To develop and maintain criteria which can be used by a crime laboratory to assess its level of performance and strengthen its operations
3. To provide an independent, impartial and objective system by which laboratories can benefit from a total operational review
4. To offer to the general public and to users laboratory services a means of identifying those laboratories which have demonstrated that they meet established standards

We are proud to announce that the Digital Forensics Lab of CyberSecurity Malaysia has officially received an accreditation from ASCLD International on 3rd November 2011. This is a direct recognisition of CyberSecurity Malaysia as the first organisation in Southeast Asia to obtain this certification. It is also an achievement to be proud of as DFD worked hard for three years to obtain the certificate. Some of the cases submitted by the LEAs for analysis will usually be brought to court for arbitration. Analysts involved will appear in court to testify on cases that have been analysed. This certificate is important as it is a measure of DFD credibility, which will be adopted by the courts later.

Digital Forensics and Data Recovery Statistics

Digital Forensics Case Statistics

From October to December 2011, DFD handled

99 cases in digital forensics. Digital Forensics cases comprised cases concerning computer forensics, mobile forensics, audio forensics and video or image forensics submitted by LEAs, RBs and Public.

Figure 1: Illustrates the Digital Forensics cases received from October to December 2011.

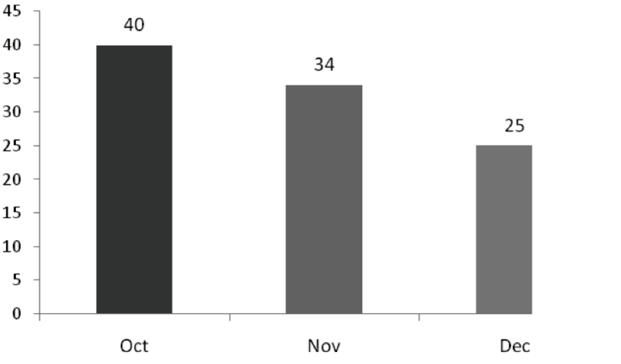

Figure 1: *Cases Breakdown from October to December 2011*

The chart below shows the categories of cases breakdown received by DFD in the period between October – December 2011. There are three (3) major categories that have been classified as of 'highest priority' which is Copyright, Bribery and CCTV/Video Extraction.

Figure 2: Illustrates the breakdown of the categories of cases received by DFD

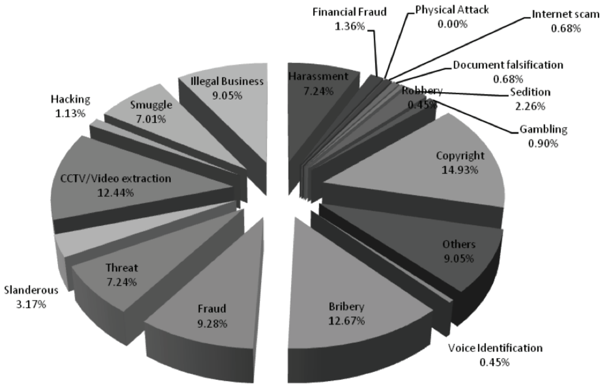

Figure 2: *Breakdown by Categories of Digital Forensics Cases (Oct-Dec 2011)*

Copyright cases were highest contributor with 14.93% cases reported. Infringement (or copyright violation) means the use of materials protected by copyright laws without the consent, it violates one of the original copyright owner's exclusive rights, such as the right to reproduce the copyrighted work or exercise, or create work products based on the copyrighted work.

From the point of law, piracy means copying activity, distribution and use of intellectual property products illegally without the permission of the copyright holder of the intellectual property. Piracy is an offence under the Copyright Act 1987. Intellectual property refers to any product and the work is registered copyright, such as books, music, film, television and radio broadcasts, computer software and industrial design. All intellectual property is protected by the Copyright Act 1987.

Piracy is rampant in Malaysia due to several factors:

1. Lack of awareness among consumers about intellectual property.
2. Pirated product prices far cheaper than genuine products.
3. Misuse of technology such as CD writers and DVD writers on the computer used for piracy.
4. Abuse of the Internet makes it a medium spread pirated products.

Bribery cases were the second highest contributor with 12.67% cases reported. When dealing with these type of cases, DFD provides support to LEAs by analysing emails, text messages, multimedia messages, calls via electronic gadgets such as mobile phones, notebooks, hard disks and thumb drives that has been used as case evidences. DFD also involved in the task force units with consists of various LEAs for Ops 3B. During this operation, the DFD teams focuses solely on corruption and bribery elements within each case. This operation was lead by BNM (Bank Negara Malaysia).

CCTV/Video Extraction category was at third place for this period with 12.44% cases recorded. Here are examples of CCTV cases analysis:

1. Authenticity of video- verify sources of video either genuine or not.
2. Video content analysis- analyze the content in term of any object and activity recorded by CCTV system
3. Facial identification- match CCTV image with photo received
4. Object comparison-compare the object displayed on CCTV with object received.

Example: attire comparison

5. Video frame enhancement- improve the quality of video frame

However, the success rates for the CCTV cases are really depending on the devices quality itself. Currently, majority of the devices received were in low quality and this has impacted the findings as it's impossible to enhance the poor quality video images. There should be awareness to the public to use more reliable devices and strategic CCTV installation area for their safety. DFD will also share with LEA's and RB's on the importance of the matters to ensure investigation can be handled smoothly.

Data Recovery Case Statistics

Figure 3: Illustrates the breakdown of cases received under Data Recovery (Oct-Dec 2011)

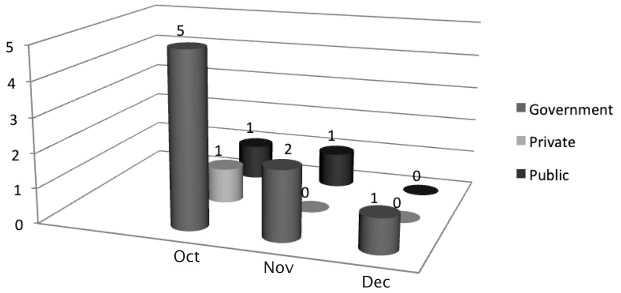

Figure 3: *Breakdown of cases received by Sector under Data Recovery (Oct-Dec 2011)*

Figure 3 show breakdown of cases received from Public, Private and Government Agencies in Quarter 4 of 2011. It can be concluded that cases received from the government sector contributed to the highest majority with 8 cases, followed by public with 2 cases and private with 1 case. Data Recovery cases reduce due to a few factors:

1. The service charges imposed for the data recovery services (starting Jan 2011)
2. Effective from October 2011, Data Recovery service taken over by CyberSecurity Clinics. The objectives of its setting up are:
   - To provide an avenue for consumers to obtain assistance and to resolve issues in relation to cyber security, cyber safety and data privacy from a trusted service provider at competitive cost
   - To serve as a citizen 'touch-point' and to demonstrate the government's commitment to the people by meeting their needs.
3. Outside competitors-the competitors might offer lower price to the public. Public also willing to take risk on data security. This might due to lack of awareness on security of data.

Talk and Training

For year 2011, DFD have been successfully conducted talks and trainings to the related parties such as government bodies and enforcement authorities as well as local universities. Not less than 20 trainings conducted which includes various topics on Digital Forensics area. For 2012 onwards, DFD will continue to serve in giving training to the LEAs and RBs in handling cybercrimes.

DFD offers five (5) trainings to the LEAs, RB, other institutions and public who interested on Digital Forensics such as:-

1. CSMDF Essentials Digital Forensic For Non-IT Background
2. CSMDF01 Digital Forensics for First Responder
3. CSMDF02 Digital Forensic Investigation & Analysis
4. CSMDF03 Data Recovery (Advanced)
5. CSMDF04 Forensics on Internet Application (Advanced)

Conclusion

In total, year 2011 have given many valuable experiences and challenges to the Digital Forensics Department through high profile cases and ordinary cases. Certainly the sweetest moment is when our lab have accredited by ASCLD / LAB (first accredited in Asian) and had successfully helping local authorities to solve their cases.

We foresee 2012 will be another challenging year for DFD. With very dynamic and active works in R&D and manufacturing for new digital equipments and applications, DFD will be exposing to more tough tasks to cope with. However with the enthusiasm and capability plus availability of the up-dated tools, all these challenges hope will make DFD be a better organisation. As always, we will continuously render our services to all our stakeholders.■

Implementing ISO/IEC 27001: Choosing an ISMS Consultant

BY | Asmuni Bin Yusof

Introduction

In protecting their information assets, many organisations have planned to adopt the ISO/IEC 27001 standard to establish a framework to protect their information assets. The standard is also known as Information Security Management System (ISMS) which can be defined as a set of interrelated and/or interacting elements to establish the policy and objectives used to direct and control an organisation with regard to information security, in order to achieve those objectives. Organisations may be interested to adopt the standard due to many reasons such as regulatory compliance, to gain a stronger business advantage, to provide clear roles and responsibilities towards information security, etc. Due to certain complexities in implementing ISMS, organisations have the option to hire ISMS consultants who may assist them in getting the job done.

As in other industries, selecting the right ISMS consultant can be a daunting task. Many consultants claimed that they are worthy to be considered to assist clients in getting their company certified against the ISMS standard. What is the benchmark of a good ISMS consultant? This paper will discuss the traits of a good ISMS consultant which may help organisations to select a credible consultant to assist them in their journey towards ISO/IEC 27001 certification.

Should your company be certified in ISO/IEC 27001?

Before proceeding further, an organisation should ask themselves why they need to get certified against ISO/IEC 27001. Is it because they are abiding to the government's/ regulators' regulation of mandating such certification for their organisations? The true spirit of ISMS certification should be to provide a framework for managing information security issues in a systematic and continuous manner. As information and information systems are the lifeblood of almost all organisations, protecting information assets cannot be left to the IT department alone. It is inevitable that board of directors and top executives take an interest in the protection of information assets of their organisations. Ultimately, ISO 27001 should be utilised as a management tool or system to help you manage all information security risks and opportunities in the spirit of continual improvement.

The point I want to bring home, "Do not plan to get the certification as a means to get a badge on the wall that confirms your company is ISMS certified."

Issues in ISMS Consultancies

We see the mushrooming of ISMS consultancies throughout the country, claiming to possess vast experience in ISMS. In reality, their track records are quite difficult to verify. The services rendered by these consultants are not standardised and some organisations in need of their services are still not clear of what they should be expecting from those consultants. Probably, the criteria for an effective ISMS consultancy service has not been defined resulting in the vast differences in consultation costs/prices. Although overcharging is not desirable, under-pricing is also bad as it might compromise quality of services rendered to clients. At the end of the day, an organisation will have to select a credible consultant/consultancy to assist them in getting the certification completed. They should dictate the selection criteria for choosing an ISMS consultant, and thus, ensuring best value for their money.

Expected Deliverables of an ISMS Consultant

A consultant should be able to establish ISMS in your organisation and set it ready for an ISMS certification. He/She should also equip your staff with sufficient skills to 'drive' the ISMS adoption. At the minimum, organisations should be expecting these items from their consultants:

- Identify information assets and provide recommendations on how to protect those assets
- Gap analysis
- Assist in a Risk Assessment exercise and propose a Risk Treatment Plan
- Preparation of Statement of Applicability
- Review existing Information Security Policies and procedures. Develop new policies and procedures if required
- Review existing IT infrastructure and organisation of information security in the organisation and highlight areas for improvement.
- Provide external and internal Vulnerability Assessment and Penetration Testing for critical systems and services
- Identif and recommend ISMS controls
- Guide to develop Document and Record Management capabilities
- Help to develop Incident Management and Response capabilities
- Help to develop Business Continuity Management capabilities
- Develop Internal Audit teams through training
- Provision of Security Awareness Programme Development and ISMS implementation workshops

The Consultant Company

How do we choose companies that are fit to render ISMS consultancy services? Preferably, their core business is in information security and they are ISO/IEC 27001 certified. We should expect the company to completely understand the value of ISMS and share their experiences in running information security programmes and provide 'tips' in dealing with auditors for Certification Bodies.

The company should also provide evidence in the form of client testimonials on successful ISO/IEC implementations of their previous ISMS projects.

Traits of a Credible Consultant

The followings are some of the traits of a good ISMS consultant:

1. **Being an Information Security Professional.** To be able to advice on information security matters, a consultant should have a good background on information security and should have some experience in planning and executing information security programmes in their company. To assist organisations to gauge the potential of a consultant, they should insist for a consultant with some internationally recognised information security certification such as Certified Information Security System Professional (CISSP), Certified Information Security Manager (CISM) and Certified Information System Auditor (CISA). You should demand these requirements as many important controls to protect information assets will involve analysing and proposing

the right technical controls. The validity of the certifications possessed by the holders can be easily verified from the certifiers.

2. **Experience in ISMS Implementation.** Preferably, a potential consultant should hold a certification on ISMS Implementation. It will be more worthy if the consultant has prior experience in implementing ISMS projects. The experience is much needed especially in consulting critical issues such as getting top management buy in, across-organisation commitments, identifying risks, business impact analysis, continuous development and improvement matrix. Inexperience consultants may not be able to deliver these crucial tasks.
3. **Certified ISO/IEC Lead Auditor.** It is paramount for an ISMS consultant to have credible information security auditing capability. He/she should be able to consider security controls in the perspective of a certification body. The consultant should possess a valid certificate in ISO 27001 Lead Auditor.
4. **Registered to Relevant Bodies.** To ensure that the chosen consultant is credible, an organisation may want to dictate that the consultant is registered to the relevant auditing or certification boards. You should expect the consultant is registered to the relevant auditing authorities such as the International Register of Certified Auditors, Professional Evaluation and Certification Board (PECB) and the International Register of Certificated Auditors.
5. **Knowledge of the Industry you are in.** Preferably, the potential consultant should have some knowledge of the industry you are in. For example if your company is in the communication sectors, a consultant should understand issues in running the communication business such as bandwidth and quality of service issues. For energy sectors, knowledge of industrial control systems should be necessary.
6. **Thorough understanding of the ISO/IEC 27001.** Although it is difficult to gauge the capabilities of a consultant through any tender selection process, you should be able to do so when you have the opportunity to meet the consultant. The potential consultant should possess a thorough knowledge of the ISO/IEC 27001:2005 standard and other ISMS related standards.

Conclusion

Selecting an ISMS consultant is not a trivial matter as it may affect the outcome of your ISMS certification. The consultant should have vast experience in information security and with substantial experience in ISMS consultancy. An organisation should determine the agreed deliverables to ensure a timely ISMS certification. An organisation should also get the best out of the consultancy services to ensure their ISMS drivers are ready to take over the 'steering wheel' when the contract ends.

An organisation should expect a substantial amount of knowledge transfer. Hence, someone from the organisation must have knowledge of ISMS so as to be able to at least check the performance of the consultant.

Remember, "The actual journey starts when your organisation achieve the ISMS certification." ■

References

1. ISO/IEC 27001 – Information technology – Security Techniques – Information security management systems - Requirements

2. ISMS Implementation Guide, http://www.atsec.com/.../ISMS-Implementation-Guide-and-Examples.pdf accessed on 28 Feb 2012.

3. ISO/IEC 27001 for Small Businesses Practical Advice

Mobile Devices Asset Classification in ISO 27001 implementation

BY | Ahmad Ismadi Yazid B. Sukaimi

Introduction

Information in mobile devices is an asset. Just like other important business assets, is essential to an organisation's business and consequently needs to be suitably protected. The use of mobile devices involves the sharing of its functions between official and personal use of the data in the same device. Thus, the security risk of the data in these devices is often ignored because it is mobile, portable and the necessity to use it all time. In analysing the risk, consider this hypothetical scenario. There is a malware outbreak with root access privilege for the Android mobile operation system. The malware is distributed by installing spoof Angry Bird application via email. The installed malware will copy all the contact information and send the data throughout short messaging system. It will also switch on the GPS, Bluetooth to drain out the battery usage. What is the risk level of the malware outbreak to the top management officers' Android mobile devices issued by the company?

Mobile Devices Risk Assessment

There are existing researches on mobile devices security. Mulliner [11] studies stated that there are needs to establish study for mobile devices security and he demonstrated it by using a Windows mobile environment. Mulliner's work has been a reference to Woongryul Jeon et al (2011) study [8], which describes that it is important to establish the framework. In the paper he demonstrated the theory by experimenting on smart phone security. He also pointed out that it is important to establish a vulnerability framework focusing on mobile devices. Ledermuller [1] studies on mobile device risk assessment also mentioned about there is a need to establish vulnerability assessment framework specific for mobile devices. He introduced a novel approach for mobile risk analysis using a categorisation method.

For a company that adopts ISO 27001 in the organisation, mobile devices issued by the company can be a challenging factor from a security point of view. The organisation needs to perform a risk assessment in order to determine the organisation's mobile devices exposure to risks and determine the best ways to manage those risks. There are many ways of performing a risk assessment, and all that ISO 27001 requires is that [2] 'An appropriate risk assessment shall be undertaken'. It is left to the organisation that implements ISO 27001 to determine what is 'appropriate'. The challenge is to perform it on mobile devices. According to LederMuller [1], determination of risk within the methodology is based upon the standard formula, which the risk is calculated from the multiplication of the asset value, threats and vulnerabilities. The worth of an asset can be a result from various dimensions. It can be estimated in terms of money, and also from a security impact [2] as confidentiality, integrity and availability. The studies introduced six steps to be followed for mobile devices risk assessment.

- RA_Step 1 - Evaluation of asset value categories
- RA_Step 2 - Calculation of a single asset value
- RA_Step 3 - Evaluation of threats
- RA_Step 4 - Calculation of a single threat value
- RA_Step 5 - Answer vulnerability questions.
- RA_Step 6 - Calculation of risk level

Evaluation Of Asset Value

When a company issues mobile devices to employees, it become officiall assets to the company and also shares the same risks with other computers and peripherals. The risk is even greater since it is small and mobile in nature and has the same access to the company's network infrastructure. The values of company issued mobile assets will be determined using ISO/IEC 27001 Information Security Management System (ISMS) implementation [3] controls and controls objectives. There are 11 domains and 133 controls for the certification. Necessary controls should be identified based on risk assessment information and the organisation's overall approach in mitigating risks. Selected controls should then be mapped to the standard and scope of implementations.

Selecting Control and Control Objective

Mobile devices need to be evaluated as assets where there is a specific asset management domain and control objectives defined to perform the evaluation. The control objectives and controls [3] listed below are directly derived from and aligned with those listed in ISO/IEC 17799:2005 Clauses 5 to 15.

Each mobile device must undergo the same control procedures with other digital assets such as inventory, ownership record and usage. Because there is a very fine line in differentiating the usage of mobile device between official and personal use, this is the most challenging aspect for monitoring purposes. For mobile devices, detailed records for incoming and outgoing calls, Short Messaging System (SMS) and Multimedia Messaging System (MMS) can be obtained from the service provider. For email systems, the logs can be obtained from the mail server itself. For other applications such as web browsing, social networking, online games and others, no audit trail can be done unless we have access to the operating system of mobile devices. The logs of applications installed in mobile devices can become the baseline for its asset value. The next challenge is to identify the applications that will be installed by the users. The asset value may change accordingly to the functionality of the applications where the company now has no control since the devices are controlled by the users.

A.7 Asset management		
A.7.1 Responsibility for assets		
Objective: To achieve and maintain appropriate protection of organisational assets.		
A.7.1.1 Inventory of assets	Control: All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.	To detect deviations from the distributions of the number of visits of a random walk to a certain state.
A.7.1.2 Ownership of assets	Control: All information and assets associated with information processing facilities shall be 'owned' by a designated part of the organisation.	To determine how far the tested sequence can be compressed.
A.7.1.3 Acceptable use of assets	Control: Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.	To determine whether the number of zeros and ones in a sequence are approximately the same as would be expected for a truly random sequence.

Table 1: *Control and Controls Objective*

Information Classification

Information in mobile devices can be categorised by labelling such services using information classification policies as specified by an ISMS implementation. Then, the information classification will be converted into mathematical data for scoring calculation. Information classification defined by an organisation is based on needs and agreements. The classification of the information will be determined in terms of its values, legal requirements, sensitivity and criticality to the organisation. The inventory should also reflect the sensitivity and security priority assigned to each information asset. An Information Classification label should be developed based on their sensitivity and security needs, i.e. Top Secret, Secret, Confidential, Restricted and Public. Each of these classification categories designates the level of protection needed for a particular information asset. Some asset types, such as personnel, may require an alternative classification scheme that would identify the information security processes used by the asset type. Classification categories must be comprehensive and mutually exclusive to the organisation. Below are information classification explanations to be adapted for mobile devices categorisation.

A. Top Secret

It is the highest category of a company's information classification. An unauthorised disclosure, loss of integrity and unavailability of information that has been classified as TOP SECRET would cause **serious** adverse impact to the organisation. If the Information ends up with a third party, it can only be done with a formal authorisation from the owner and/or after signing a non-disclosure agreement. This is for "read only" purposes and shall not be taken out from the premises. Information shall be labelled with the right handling policy.

B. Secret

It is the second highest category of a company's information classification. An unauthorised disclosure, loss of integrity, unavailability of information classified as SECRET would cause **severe** adverse impact to an organisation. Information shall be accessed by the employee only with explicit authorisation. Information shall be extended to third parties only with formal authorisation from the owner and/or after signing a non-disclosure agreement and for "read only" purposes. It shall not be taken out from the premises. Information shall be labelled and handled with the right handling policy.

C. Confidential

It is the third highest category of a company's information classification. An unauthorised disclosure, loss of integrity, unavailability of information classified as CONFIDENTIAL would cause **significant** adverse impact to an organisation. Information shall be accessed by the employee only with explicit authorisation. Information shall be extended to third parties only with formal authorisation from the owner and/or after signing a non-disclosure agreement and for "read only" purposes. It shall not be taken out from the premises. Information shall be labelled and handled with the right handlin.

D. Restricted

It is the fourth highest category of a company's information classification. An unauthorised disclosure, loss of integrity, unavailability of information classified as RESTRICTED would cause **minor** adverse impact to an organisation. Information shall be accessed by the employee only with explicit authorisation. Information shall be extended to third parties only with formal authorisation from the owner and/or after signing a non-disclosure agreement and for "read only" purposes. It shall not be taken out from the premises. Information shall be labelled and handled with the right handling policy.

E. Public

It is the lowest category of a company's information classification. An unauthorised disclosure, loss of integrity, unavailability of information classified as PUBLIC would not cause **any** impact to an organisation. Information shall be accessed by any employee of the company. Information can be extended to external parties with no requirements in place.

Mobile Device Asset Category

According to LederMuller [1], determination of risk within the methodology is based upon a standard formula, where the risk is calculated from the multiplication of the asset value, threats and vulnerabilities. The worth of an asset can be measured from various dimensions. It can be estimated in terms of money and from a security impact perspective ranging from confidentiality, integrity and availability. LederMuller [1] study introduces Mobile Devices Risk assessment using an asset categorisation methodology. The technique is identifying applications from mobile devices and categorise them by functionality.

1. Asset Category
2. E-Mail (corporate)
3. E-banking
4. E-health
5. Remote access (corporate)
6. Remote access (private)
7. Voice communication

8. Stored business documents
9. Physical device
10. Personal information (online synchronised)
11. E-Mail (private)
12. Social networking
13. Messaging
14. Personal information
15. Web access (browser)
16. Stored documents
17. Maps & Navigation
18. News client
19. Utilities

Identifying Asset Value

The next step is to label the information inside mobile devices using the Information Handling label. The table below describes the asset value of a mobile device issued to a company's management team. The evaluating methods listed here should be considered but should not be limited to the questions below:

1. What is the information insidmobile devices?
2. What happened to the information if the asset is missing?
3. Can the information be retrieved from the device?
4. Can the devices communicate to the corporate network?
5. Who is the owner of the device?

By answering the given questions, the evaluator can identify the optimum information handling for each group of mobile device asset category. Each category can be a single application or multiple applications, which will share the same information handling label. The table below shows mobile devices information handling label for a management officer with a mobile device issued by the company.

Asset Category	Information Handling Label	Value
E-mail (corporate)	Top Secret	5
E-banking	Top Secret	5
E-health	Top Secret	5
Remote access (private)	Confidential	3
Voice communication	Confidential	3
Stored business documents	Top Secret	5
Physical device	Top Secret	5
Personal information (online synchronised)	Top Secret	5
E-mail (private)	Top Secret	5
Social networking	Confidential	3
Messaging	Top Secret	5
Personal information	Confidential	3
Web access (browser)	Confidential	3
Stored documents	Top Secret	5
Maps & Navigation	Top Secret	5
News client	Confidential	3

Table: *Asset Value By Information Handling Label*

From the classification of the application category information, the information in the mobile device can be classified as Top Secret and has the highest value of 5. This value will be incorporated later for calculating the risk value of mobile devices during the company risk assessment process for ISO 27001 implementation.

The table below is the data collected for each user in different categories, namely the management and corporate user where they were supplied with mobile devices. The normal user; on the other hand, obtained their devices personally. The issue is that whether the normal users are able to connect their devices to the corporate network which will result in their mobile devices status to be the same as the corporate user. If the corporate email is using POP or IMAP services, the normal user can connect to the corporate network with their mobile devices easily and share the same risks with other corporate users.

	Asset value		
Asset category	**Management User**	**Corporate User**	**Normal User**
E-mail (corporate)	5	5	0
E-banking	5	5	2
E-health	5	5	2
Remote access (corporate)	5	5	0
Remote access (private)	5	2	2
Voice communication	5	2	2
Stored business documents	5	3	3
Physical device	5	3	3
Personal information (online synchronised)	5	2	2
E-mail (private)	4	2	2
Social networking	4	2	2
Messaging	3	2	2
Personal information	3	2	2
Web access (browser)	3	2	2
Stored documents	1	2	2
Maps & Navigation	1	1	1
News client	1	1	1
Utilities	1	1	1

Base on the information handling scoring for each mobile devices category, the asset value of the mobile devices can be calculated. By having an information value of 5, which shows the highest risk value, it will affect the security measures, handling and usage of the mobile devices. The owners of the mobile devices must also understand the risks of using the device inside and outside the premises. The differentiating factor of official and personal usage must be identified clearly.

Conclusion

Mobile devices asset value can be determined by giving scores for each categorisation. Even though the value of the asset shows the highest ranking of information security label, we cannot escape from using mobile technology to access office communication systems. By knowing the value of a mobile phone, the user and the company can find out what security measures are appropriate to the asset itself. This step can set the level of risk faced by a company if the mobile equipment is exposed to threats and leads to loss of information. The risk of having mobile devices connected to the corporate network now can be managed by identifying the true value of the asset which will be used later for completing the mobile device risk assessment. ■

References

1. *[1] Thomas Ledermuller, Nathan L. Clarke.2011. Risk Assessment of mobile devices. Trust, Privacy and Security in Digital Business:8th International Conference, Trustbus 2011, Toulouse, France, August 29 - September 2, 2011, Proceedings*
2. *[2] MAMPU. UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA. Jabatan Perdana Menteri Malaysia (2007). ISMS RISK ASSESSMENT GUIDELINE.*
3. *[3] Kamat, M. (2009). Guideline for Information Asset Valuation. Forum American Bar Association, (c).*
4. *[4] Vulnerability Assessment tools .2011. Information Assurance Technology Analysis Center*
5. *[5] NIST Risk Management Framework. FISMA. National Institute of Standards and Technology. Online at http://csrc.nist.gov/groups/SMA/fisma/framework.html*
6. *[6] Stoneburner, G., Goguen, A., & Feringa, A. (n.d.). Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology. Nist Special Publication.*
7. *[7] Etsi, C. R., Brookson, C., & Uk, B. I. S. (2009). Security for ICT - the Work of ETSI Authors : European Telecommunications, (1)*
8. *[8] Woongryul Jeon, Jeeyeon Kim, Youngsook Lee and Dongho Won. A Practical Analysis of Smartphone Security. Lecture Notes in Computer Science, 2011, Volume 6771/2011, 311-320, DOI: 10.1007/978-3-642-21793-7_35*
9. *[9] Enck, W., & Mcdaniel, P. (2008). Understanding Android ' s Security Framework. Security, (October).*
10. *[10] Ongtang, M., Mclaughlin, S., Enck, W., & Mcdaniel, P. (2009). Semantically Rich Application-Centric Security in Android. Intents.*
11. *[11] Mulliner, C.R.: Security of Smart Phone, Master's Thesis of University of California (June 2006)*

'Right-Sizing' Security in the Cloud: A Risk-Based Approach for Providers

BY | George Chang

Introduction

Recent stories on network interruptions and system break-ins made many organizations hesitant about transferring data, applications and/or processes to the Cloud. Just last year, Malaysian Government websites were hacked by hacker group Anonymous, leaking thousands of private user information to the public.

These incidents prompt experts and customers to wonder whether security becomes a greater issue with cloud computing compared with other forms of hosting. Not really. Even if the different service models and technologies applied in enabling cloud services do introduce new risks. For an organization, opting for cloud computing means losing control over its IT environment, while retaining the liability for it. And so, even if the responsibility for operations is handed over to a third party.

Cloud services share the same challenges as any average application in the private datacenter. The level of protection is equal to security measures such as physical, network, system and information security. It may also involve access policies, rules of conduct for employees and processes.

Any organization should ask whether their cloud provider is able to match or surpass their own level of protection. The profitability resulting from scalability, uniformity and standardization, is one of the most attractive benefits of cloud computing. However, cloud providers must offer services that are flexible to satisfy the largest customer base possible while balancing security measures that constraints such flexibility. This renders cloud providers unable to offer the equal level of security of a traditional IT environment.

If cloud providers cannot offer trusted security measures, then sound agreements must be made in regards of responsibility. In Software as a Service (SaaS) environments, security measures and their scope are formulated in contracts. In the Infrastructure as a Service (IaaS) model, the security of the underlying infrastructure, and the layers based on it, come under the responsibility of the IaaS provider. The remainder of the chain, such as the operating systems, applications, and data leveraging the infrastructure, is the responsibility of the customer. The Platform as a Service (PaaS) model is positioned somewhere in between SaaS and IaaS. The security of the platform is part of the responsibilities of the PaaS provider; however, the customer is responsible for securing the applications developed on that platform.

It is important to assign responsibilities in the event incidents or disaster occurs. There should be redundant back-up servers at a remote location to maintain operations and fail-over systems to temporarily transfer services to another cloud provider. This does not only apply to cloud providers but also enterprises.

Network security

If information security in the private data center requires strict rules and measures, same goes for the Cloud. The cost savings of a SaaS application are worthless if data and reputation are compromised. The cloud provider must warrant the security of the Cloud, but also the one of the network and the physical environment. It is important to select a cloud provider that has a solid track record, expertise and best solutions in networking and system security. One that is able to review all security risks, test system protections, and control or avert threats. At last, network security should protect all virtual access points to the cloud. Cloud providers must employ well-managed security rules to block attacks, protecting all virtual access points to the cloud. They should be able to search and stop emerging threats before it becomes a real danger.

Physical security

Social engineering is on the rise as a means to break through the physical or network security perimeters. People attempt to obtain the trust of employees by telephone or in person in order to gain access to the datacenter or to lure employees into sharing information they can in turn use to hack data systems. Consequently, in addition to technical measures, the cloud provider must define and enforce rules of conduct and social guidelines for employees. A great way to test compliance with these rules is by hiring the services of an 'ethical hacker', who will try to gain access to the physical and digital environments on behalf of the customer.

When thinking about physical security, it is also advisable to look at the specific solutions the cloud provider has in place for disaster recovery. Where is data stored when it is not in use? Is the data encrypted and available in a redundant remote location?

Blind spot

One feature of cloud computing is that multiple users leverage the same application or hardware. This so-called 'multi-tenant' environment implies that multiple organizations' information is present on one physical system. It is therefore critical to ensure that the systems are segmented correctly and that their data and applications are fully separated from each other. However, virtual environments operate differently than traditional servers. The latter monitor all traffic transported on the spot, through a physical Ethernet switch or router. In a virtual environment, data is streamed through a virtual adapter, without ever passing through any physical device. This creates a blind spot in the communication between the datacenter and the end user, and consequently a potential security issue. Setting up a physical or virtual security appliance between the cloud provider and the private organization may prove to be a smart solution, as it will help provide the right mix of performance and control across the traffic streams.

Conclusion

In conclusion, there are many different ways to approach the Cloud: via the SPI service models (Software-as-a-Service, Platform-as-a-Service, of Infrastructure-as-a-Service), the public versus private cloud, internal versus external hosting, and a large number of hybrid solutions in between. Given the number of options, there is no standard list of security measures that covers all possible events exhaustively. So, before moving forward, organizations should apply a risk-based approach towards the Cloud and make sure that the necessary security measures required do not impede the expected efficiency and cost benefits of their cloud solutions. ■

....

George Chang *is Fortinet's Regional Director for Southeast Asia & Hong Kong. Fortinet is a leading provider of network security appliances and the worldwide leader in Unified Threat Management or UTM. Fortinet integrates multiple levels of security protection (such as firewall, antivirus, intrusion prevention, VPN, spyware prevention and antispam) to help customers protect against network and content level threats.*

Tracing Cyber Criminals Via Full Headers

BY | Sharifah Roziah Binti Mohd Kassim

Introduction

Presently, cyber criminals are actively using emails as a medium for launching cyber crimes on the Internet. This is especially prevalent in cases involving email correspondences as seen in the Nigerian scam, phishing, cyber harassments, cyber bullying, cyber stalking, malware and spam. However, many are not aware that the full headers of any email can actually be used by investigators to detect, trace cyber criminals and eventually curb cyber crimes on the net. The question is, how an investigators or an analysts go about doing so? Before we delve further in the answer, we need to understand what a full header is.

Definition of Email Header

All emails arrive in standard Headers or accurately termed as Brief Headers. A Brief Header has basic information about an email such as FROM, TO, SUBJECT, DATE/TIME. An example is provided below:

Brief Header

A brief header will look like the example below with the following information:

Date: Fri, 8 May 1998 10:05:21 +0800 (MYT)
From: ass@pc.jaring.my
To: john@ace.cdc.abu.com
Subject: happy holiday

The above brief header provides basic information about the date, time the email was sent, the sender of the email, the recipient and subject matter of the email. However, the above information is not sufficient for investigators analysing cases related to emails. The FROM (sender) information in an email can be forged or spoofed.

Full Header

Besides the brief header which contains basic information, a more detailed information can be extracted from it called the full header. This has detailed technical information about an email. All email programmes can be set to show only brief headers or full headers and it is up to a particular user to set the programme as to whether to view only brief headers or full headers.

Full headers will have information such as the mail's server data that the email passed through on its way to the recipient. It also contains the IP addresses of the recipient and the sender. Additionally, it has the name of the email programme and the version used in completing the process. This is essential for analysis and for investigation purposes on cases involving email abuse, spamming, mail bombing, etc. This information is not available in a brief header. Thus, it is important for investigators to have full headers for cases involving email abuse, worm infected emails, harassment, forgeries and other email related cases.

What is in Full Header?

Full headers contain the names and IP addresses of all the hosts/servers that have relayed a message from the sender until it reaches the recipient. Each host/server that forwards the message along its route adds a line of information to the headers. The information provided in the full headers allows an investigator to discover the origin of an email based on the originating IP address. It is important to trace the originating IP address of an email in order to find out the actual sender of the email as the "From:" line on the email header can be spoofed, or faked.

It is also important for investigators to obtain the full header from the original recipient of the email. The full header cannot be retrieved from forwarded copies of the original message. As such, the original recipient of the concern email must keep the email for investigation purposes.

How to Read a Full Header

Here is an example of a full header. The Received information in the full header is very important in finding out the origin of the email and the route it took to reach the recipient. From the full header we can also find out if the email is forged, spoofed or intercepted.

Normally, for tracing purposes, full headers are read bottom to top. The last Received line in a full header will tell the origin of the email which is the source computer/ machine where the email was sent. On the other hand, the top Received line would tell the email server where the email originated which will eventually route to the recipient email server before the email finally reaches the recipient.

Let's look at the example below:

```
Return-Path: ass@elay13.jaring.my
Delivered-to: johnace.cdc.abu.com
Received: from relay13.jaring.my
(relay13.jaring.my [192.228.128.124])
by ace.cdc.abu.com (8.7.1/8.7.1)
with ESMTP id KAA18533
for <john@ace.cdc.abu.com>  ;
Fri, 8 May 1998 10:01:01 +0800
Received: from (j19.kch18.
jaring.my [161.142.54.153])
by relay13.jaring.my (8.8.8/8.8.7)
with SMTP id KAA21792
for  john@ace.cdc.abu.com ; Fri, 8
May 1998 10:05:21 +0800 (MYT)
Message-Id: <199805080205.
KAA21792@relay13.jaring.my>
Date: Fri, 8 May 1998
10:05:21 +0800 (MYT)
From: ass@pc.jaring.my
To: john@ace.cdc.abu.com
Subject: happy holiday
```

We will analyse the full header by reading from bottom to top:

1. *Subject: happy holiday*
   The subject line gave us an idea of what the mail is all about.

2. *To: john@ace.cdc.abu.com*
   The 'To' line listed clearly the email address/es of the recipients of the mail.

3. *From: ass@pc.jaring.my*
   The 'From' line showed who sent the mail and his/her email address. This 'From' information can easily be faked/ forged.

4. *Date:Fri,8May199810:05:21+0800(MYT)*
   The Date line lists the date and time this mail was originally sent. It was sent according to the sender's local time zone.

5. *Message-Id: <199805080205. KAA21792@relay13.jaring.my>*
   The message-Id line was intended primarily for tracing mail routing and uniquely identifying each mail.

6. *Received: from (j19.kch18.jaring.my [161.142.54.153]) by relay13.jaring.my (8.8.8/8.8.7) with SMTP id KAA21792 for john@ace.cdc.abu.com ; Fri, 8 May 1998 10:05:21 +0800 (MYT)*
   The email originated from (j19.kch18.jaring.my [161.142.54.153]). Note the originating IP address of this email is 161.142.54.153. A whois lookup of the IP 161.142.54.153 will show that the IP address is registered under Jaring (service provider) as below:

   ```
   inetnum: 161.142.0.0
   - 161.142.255.255
   netname: JARING-NAT
   descr: JARING
   Communications Sdn Bhd
   country: MY
   ```

   The above result indicated no possible spoofing or forgery as the IP address indeed belonged to jaring.my. The email is relayed via server relay13.jaring.my using Sendmail version 8.8.8/8.8.7. (Whenever the actual programme name is left out, as it is here, Sendmail is assumed) with SMTP id KAA21792 for recipient john@ace.cdc.abu.com. The "SMTP id KAA21792" is an internal ID number assigned to the message. This ID number is only of use by the ISP's mail service; it can be used to look up the message in their log files.

7. *Received: from relay13.jaring.my (relay13.jaring.my [192.228.128.124]) by ace.cdc.abu.com (8.7.1/8.7.1) with ESMTP id KAA18533 for <john@ace.cdc.abu.com> ; Fri, 8 May 1998 10:01:01 +0800*
   The email is then received from relay13.jaring.my (relay13.jaring.my [192.228.128.124]) by the recipient's mail server which is ace.cdc.abu.com using their Sendmail version 8.7.1/8.7.1 with ESMTP id KAA18533 for <john@ ace.cdc.abu.com>.

8. *Delivered-to: john@ace.cdc.abu.com*
   The email is then delivered to the recipient by his mail server.

9. *Return-path: ass@relay13.jaring.my*
   Return path is the path where the sender will receive his reply from the recipient.

Findings

From the above full header, we can conclude that the email originated from IP 161.142.54.153. On further analysis, the IP address 161.142.54.153 matches the hostname j19.kch18.jaring.my. A Whois search of the above originating IP address indicated the IP address indeed belonged to Jaring Communications. There is no conflict between the IP address, the hostname and the Whois result. As such we can say from this findings that the full header is not intercepted or forged as there are no indications of forgery or interception.

```
========WHOIS==========
IP: 161.142.54.153

inetnum: 161.142.0.0
- 161.142.255.255
netname: JARING-NAT
descr: JARING
Communications Sdn Bhd
country: MY
=======================
```

Once the originating IP address has been traced, the investigator will need to go to the ISP and make an official request to the Corporate Affairs Department requesting for the identity of the person who sent the above email. A copy of the full header must be accompanied together with the request as evidence for the ISP. The ISP will facilitate for further investigation until tracing of the identity of the perpetrator is done. Once the identity is traced, he/she will be prosecuted.

Looking for Forgery or Interception From the Full Header

In a full header, there will be several IP addresses, hostsnames and mail server information. Normally, perpetrators or email abusers will add the name of another mail server to the headers in their attempt to trick recipients and forge themselves. In order for investigators to ensure the information in the full header is not forged, they can do a DNS lookup or Reverse DNSlookup to verify the hostname and the IP address that it belongs to.

After completing the DNS lookup and if the hostname and IP address does not match then this may indicate that the information in the full header has been forged. There is also a possibility of interception if there is a presence of an unknown third party IP address other than the IP address that belonged to the sender and recipient of the email. In addition, investigators can also do a Whois lookup to check and verify the location of the IP address.

Forged or intercepted email full headers cannot be used as valid evidence by law enforcement agencies for tracing or prosecuting perpetrators.

Conclusion

In conclusion, full headers are an important element or a crucial piece of evidence for investigating the source of cyber crimes or cyber attacks that were conducted via email. Untampered or unforged full headers can be produced in a court by investigators for prosecution of cyber criminals. They are very useful for tracing or prosecuting perpetrators on the net and eventually curb the rise cybercrimes on the net. This will help to minimise cyber crime activities on the net. Victims who are being abused, harassed or scammed via emails are encouraged to report the matter to the relevant ISPs, CERTs or to law enforcement agencies for further investigation. They must keep the particular email message together with its full header in their PC for further investigation or for tracing purposes and for future record purposes. ■

References

1. *http://kb.iu.edu/data/akij.html*
2. *http://www.mycert.org.my/en/resources/email/email_header/main/detail/509/index.html*
3. *http://www.emailquestions.com/full-email-headers/244-do-i-read-full-headers-email.html*
4. *http://support.google.com/mail/bin/answer.py?hl=en&answer=29436*
5. *http://www.policypatrol.com/spam-filter-article.htm*

E-SECURITY NEWS HIGHLIGHTS FOR Q4 2011

QR CODES ARE BEING USED TO SPREAD MALWARE

Just when you thought that keystroke logging by an iPhone was your biggest mobile security concern, the folks at Kaspersky Lab are saying that you need to be careful with QR codes. The incident took place in Russia, and involved a mobile app called Jimm. Instead of downloading the app, the code contained malware that fired off a series of expensive SMS messages ($6 each), racking up unwanted charges.

http://www.geek.com/articles/mobile/qr-codes-are-being-used-to-spread-malware-20111021/

CARRIER IQ ROOTKIT LOGS EVERYTHING ON MILLIONS OF PHONES

If you use an Android, BlackBerry, or Nokia smartphone then you may be at risk of being illegally wire tapped by Carrier IQ--a provider of performance monitoring software for Smart Phones. Earlier this month Trevor Eckhart announced that he found software, made by Carrier IQ, that may be logging your every move on your mobile phone and he called it a "rootkit"--a software that hides itself while utilizing privileged access like watching your every move.

http://www.computerworld.com.my/resource/security/carrier-iq-rootkit-logs-everything-on-millions-of-phones/

NEW JERSEY TRAINS NEW CLASS OF LAWYERS TO PROSECUTE CYBERCRIME

Seeing that there was a “serious lack” of prosecuting attorneys proficient in the laws dealing with cybercrime, Molinelli took advantage of asset forfeiture regulations that allow a certain percentage of seized assets be used for education to put toward training that would beef up the skills of the people who could help put cybercriminals in prison.

http://www.hstoday.us/briefings/correspondents-watch/single-article/new-jersey-trains-new-class-of-lawyers-to-prosecute-cybercrime/3757b41b64e0dc8fa0aa46cfdd773576.html

APPLE ITUNES FLAW 'ALLOWED GOVERNMENT SPYING FOR 3 YEARS

A British company called Gamma International marketed hacking software to governments that exploited the vulnerability via a bogus update to iTunes, Apple's media player, which is installed on more than 250 million machines worldwide. The hacking software, FinFisher, is used to spy on intelligence targets’ computers. It is known to be used by British agencies and earlier this year records were discovered in abandoned offices of that showed it had been offered to Egypt’s feared secret police.

http://www.telegraph.co.uk/technology/apple/8912714/Apple-iTunes-flaw-allowed-government-spying-for-3-years.html

DDOS ATTACKS SPELL ‘GAMEOVER’ FOR BANKS, VICTIMS IN CYBER HEISTS

The FBI is warning that computer crooks have begun launching debilitating cyber attacks against banks and their customers as part of a smoke screen to prevent victims from noticing simultaneous high-dollar cyber heists.The bureau says the attacks coincide with corporate account takeovers perpetrated by thieves who are using a modified version of the ZeuS Trojan called “Gameover.”

http://krebsonsecurity.com/2011/11/ddos-attacks-spell-gameover-for-banks-victims-in-cyber-heists/

EUROPEAN NATIONAL LAWS TO BE REPLACED BY EU DATA PROTECTION REFORM

75% of Europeans are worried about how social networking sites use their private information. The European Union wants to create one "level playing field" when it comes to data protection, and plans to update laws dating back to 1995, long before Facebook and other social networking sites even existed. EU Justice Commissioner Viviane Reding said that presently companies that operate in several member states must comply with different laws and different decisions taken by data protection authorities in 27 member states. She added, "They need... a 'one- stop-shop' when it comes to data protection matters--one law and one single data protection authority for each business; that of the member state in which they have their main establishment."

http://security.cbronline.com/news/european-national-laws-to-be-replaced-by-eu-data-protection-reform-291111

POLICE TO SET UP CYBER CRIME UNIT

A new police Cyber Crime Unit is to be set up to protect Britain against the growing threat of attacks on the internet and in electronic communications. Alongside the law enforcement unit, a new Joint Cyber Unit at the Government's GCHQ eavesdropping centre will develop the UK's military capabilities in cyberspace, Cabinet Office minister Francis Maude announced.

http://www.independent.co.uk/news/uk/crime/police-to-set-up-cyber-crime-unit-6267831.html

THE GROWING IMPACT OF FULL DISK ENCRYPTION ON DIGITAL FORENSICS

"The increasing use of full disk encryption (FDE) can significantly hamper digital investigations, potentially preventing access to all digital evidence in a case. The practice of shutting down an evidential computer is not an acceptable technique when dealing with FDE or even volume encryption because it may result in all data on the device being rendered inaccessible for forensic examination. To address this challenge, there is a pressing need for more effective on-scene capabilities to detect and preserve encryption prior to pulling the plug.

http://www.bespacific.com/mt/archives/028804.html

Training Programs

Professional Development Schedules in CyberSecurity Malaysia Calendar 2012

No.		Program Duration	Standard Fees (RM)	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Fundamental/Introduction															
1	Essentials Digital Forensics for Non-IT Background	2 days	1500		9-10										
2	Digital Forensics for First Responder	2 days	1500				5-6								
3	MyCC 1.0 - Understanding Security Target, Protection Profile & Supporting Evaluation	1 day	790		20					23					
4	Introduction to ISO 27001 & ISO 27002:2005 Information Security Management System	1 day	650	9	10	5	6	7	11	6	6	3	5	5	7
5	Business Continuity Management for Essentials	1 day	1000		20		23		25			24			
6	Data Encryption for Beginners	1 day	790						4					19	
7	Cryptography for Beginners	1 day	890					21				10			
8	CSM Security Essential Training	2 days	1590		27-28			7-8						5-6	
9	Google-Fu Power Search Technique	2 days	1400			5-6				9-10					
10	Wireless Security	2 days	1350					9-10							
11	Customize Training Package for groups and companies (Fundamental Courses Item 1-10)	1-5 days	Negotiable												
Intermediate															
1	Malaysia Common Criteria (MyCC 2.0) - Foundation Evaluator Training	3 days	3290		21-23					24-26					
2	Incident Response & Handling for Computer Security & Incident Response Team (CSIRTS)	3 days	3590					14-16						31(Nov)-2(Dec)	
3	Cryptography for Information Security Professional	3 days	3590					22-24				11-13			
4	ISO 27001 Implementation	3 days	3200	10-12	13-15	6-8	9-11	8-10	12-14	9-11	7-9	4-6	8-10	6-8	10-12
5	Google-Fu Googling to the Max	2 days	1600			7-8				11-12					
6	Incident Handling and Network Security Training Workshop (IHNS)	3 days	3590			26-28						3-5			
7	ISMS Internal Auditor (ISO 27001)	2 days	2850			12-13			11-12		13-14			5-6	
8	Customize Training Package for groups and companies (Intermdiate Courses Item 1-6)	1-5 days	Negotiable												
Specialization															
1	Digital Forensics on Data Recovery	2 days	1800								8-9	24-25			
2	Forensics on Internet Application	1 day	900											20	
3	Risk Management	3 days	3900												
4	Legal, Regulations, Investigations & Compaliance Fundamentals of Infromation Security Law & Practise	1 day	1200			20									
Professional Certification															
1	Certified Information System Security Professional (CISSP) CBK Review Seminar	5 days	4705		13-15		9-13						1-5		
2	System Security Certified Practitioner (SSCP) CBK Review Seminar	5 days	4372			13-16		9-13	6-10	11-15			8-12		5-9
3	Certified Secure System Lifecycle Professional (CSSLP)	5 days	4180			7-11	16-20						15-19		
4	SEC504: Hacker Techniques, Exploits & Incident Handling	6 days	USD4400						18-23						
5	SEC542: Web App Pen Testing and Ethical Hacking	6 days	USD4400			19-24									
6	AUD 507 - Auditing, Networks, Perimeters and Systems	6 days	USD4400												
7	SEC560: Network Penetrating Testing and Ethical Hacking	6 days	USD4400										8-13		
8	Digital Forensics Investigation & Analysis	4 days	3850							16-20					
9	Business Continuity Management Professional Certification (BCLE2000)	5 days	8900			5-9		7-11		9-13			1-5		3-7
10	Professional in Critical Information Infrastructure	3 Weeks	USD6000											19(Nov)-7(Dec)	
11	Cyber Warrior	5 days	4850			19-23			18-22						17-21
12	Cyber Defender	5 days	4890			12-16			11-15						3-7
13	ISO 27001 Lead Auditor	5 days	5000	16-20	20-24	19-23	23-27	21-25	25-29	16-20	13-17	24-28	15-19	26-30	17-21
14	Forensics Investigation Advance	5 days	USD4085	9-14											
Examination															
1	CISSP Examination	6 hrs	USD599		25			12				8		3	
2	SSCP Examination	6 hrs	USD300		25			12				8		3	
3	Certified Forensics Investigation Analyst (CFIA)		580												
4	Kryterion Test Center			19		29		17		13		26		27	
5	Cyber Warrior - Operation D-Day (fully hands on examination)	3 hrs	1200			26			25						28

*Subject to change

Venue

CyberSecurity Malaysia, Training Centre, Level 4, Block C, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia. | Tel: +603 - 8946 0999 | Fax: +603 - 8946 0844 (ISPD)

People First, Performance Now

MOSTI Ministry of Science, Technology and Innovation

Best Brand Internet Security 2008 & 2009

ISMS SIRIM CERTIFIED TO ISO/IEC 27001:2005 CERT NO.: AR4656

STANDARDS MALAYSIA MS ISO/IEC 17025 TESTING SAMM NO. 456 (MyCERT LABORATORY)

MSC MALAYSIA Status Company