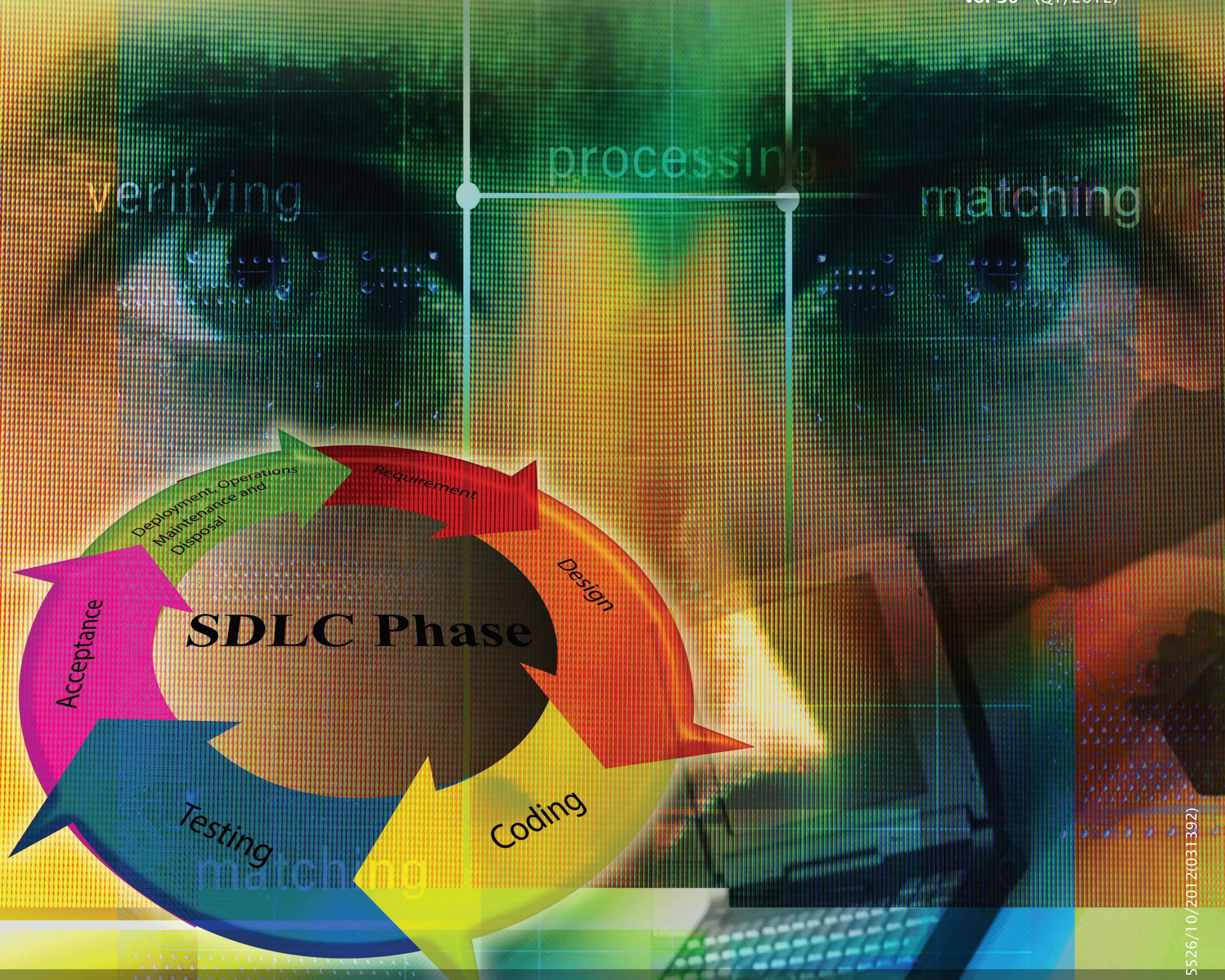
CyberSecurity
MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 30 - (Q1/2012)



Securing Your Software Development Life Cycle
Analysis of Vulnerabilities Report
Benefits of ISO/IEC 27005:2011 Information Security Risk Management

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

"Security is, I would say, our top priority because for all the exciting things you will be able to do with computers.. organizing your lives, staying in touch with people, being creative.. if we don't solve these security problems, then people will hold back. Businesses will be afraid to put their critical information on it because it will be exposed"

Bill Gates

ISSN 1985-1995
9 771985 199003

CEO MESSAGE

For the past few years, we have seen the birth to a gamut of new age cyber threats and how they are encroaching more into every sphere our lives and they come in multi-dimensions. In 2011, we have also seen the emergence of social media and mobile devices etc that has complicated the global cyber security landcape which is further worsened by users' ignorance, technical incompetency, and lack of strategic cyber security collaboration. We take necessary steps to curb this situation, among others knowledge sharing initiatives via e-Security Bulletin. It is expected that 2012 and beyond will be challenging as cyber crime is consistently becoming sophisticated due to the rapid advancement in technology.

In 2011, CyberSecurity Malaysia has received 5,328 online fraud incidents that include various types of Internet scams. That number alone is more than the total number of similar incidents in 2010 and double of those reported in 2009. It is not an exaggeration to say that internet scams i.e. love scams, financial fraud, identity theft etc are fast becoming the crime of choices. For every investigation in the news, there are hundreds that will never make the headline. We learn that criminals can hardly get caught, and even if they do, they can be hardly convicted.

As the technology evolves, the risks posed by cyber threats also continue to grow in both scale and sophistication. New techniques and methods may emerge, and the traditional ones would become obsolete. As such, our attitudes towards cyber security should also evolved and innovated.

The explosion of Internet has also created the phenomenon towards "digital hacktivism". 2011 also witnessed hacktivist groups such as "Anonymous" went rampage, worst than the year before. Indeed, "Anonymous" is a revolutionary group, and it will be more sophisticated in the future. Hence our approach towards combating it has to be equally revolutionary.

Cyber security requires an innovation or perhaps a fundamental shift in approach towards solving the problems; and we have to act fast to stay ahead. 2012 onward, we need to understand the evolving cyber threats and how they work, and to develop the tools and methods to combat them. We should create more robust and resilient cyber space that can withstand attacks, and also help detect and prevent cyber attacks from occurring. We also need talented people with innovative ideas and commitment from both local and global key cyber security players.

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 and welcome to the first edition of eSecurity Bulletin for 2012. Some interesting topics have been lined up in this edition such as security in Software Development Life Cycle (SDLC), principles of security and information security risk management. Also, short but important tips on how to secure your iPad is included. Please spend time to read through the articles.

I would like also to highlight our CyberSecurity Clinic which started its operation in September last year. Some of the services being offered are data recovery (for your hard disk, thumb drive, memory card or server), data sanitization and ICT services. Please visit the CyberSecurity Clinic website (www.cybersecurityclinic.my) for further information.

Last but not least, I want to take this opportunity to thank all contributors for their valuable knowledge sharing. I look forward for more contributions from the security professionals.

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 highlight statistics of incidents according to categories handled by MyCERT in Q1 2012, comprising of security advisories and other activities carried out by MyCERT personnel. The statistics provided 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 Q1 2012

Incidents were reported to MyCERT by various parties within the constituency as well as from foreign sources, which include home users, private sector entities, government agencies, security teams from various countries, foreign CERTs, Special Interest Groups including MyCERT's proactive monitoring on several cyber incidents.

From January to March 2012, MyCERT, via its Cyber999 service, handled a total of 3,143 incidents representing a 4.40 percent decrease compared to Q4 2011. In Q1 2012, incidents such as Denial of Service, Fraud, Vulnerabilities Report and Malicious Code had increased while other incidents showed a decrease.

Figure 1 illustrates incidents received in Q1 2012 and classified according to the type of incidents handled by MyCERT.

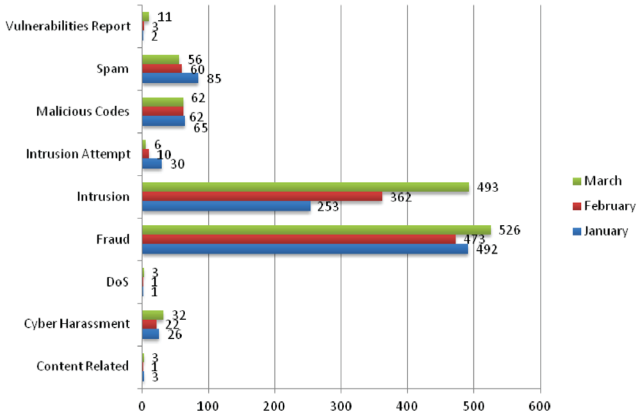


Figure 1: *Breakdown of Incidents by Classification in Q1 2012*

Figure 2 illustrates incidents received in Q1 2012 and classified according to the type of incidents handled by MyCERT as well as a comparison with the number of incidents received in the previous quarter.

Categories of Incidents	Quarter		Percentage
	Q4 2011	Q1 2012	
Intrusion Attempt	209	46	-77.99
Denial of Service	1	5	400
Spam	299	201	-32.77
Fraud	1153	1491	29.31
Vulnerability Report	11	16	45.45
Cyber Harassment	105	80	-23.80
Content Related	11	7	-36.36
Malicious Codes	142	189	33.09
Intrusion	1357	1108	-18.34

Figure 2: *Comparison of Incidents between Q4 2012 and Q1 2012*

Figure 3 shows the percentage of incidents handled according to categories in Q1 2012.

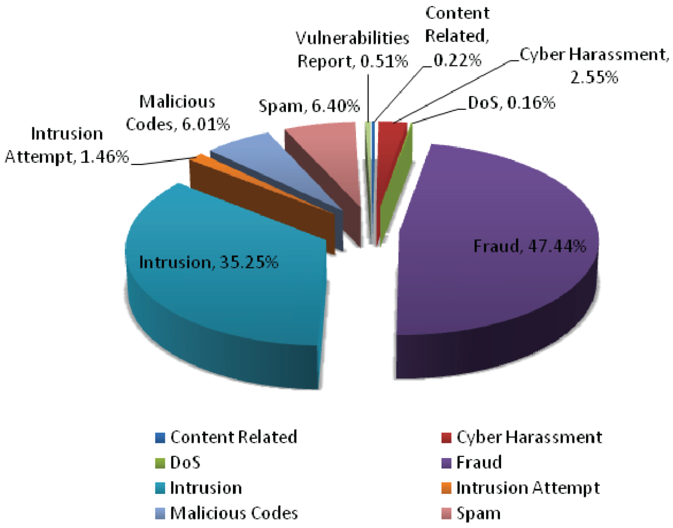


Figure 3: *Percentage of Incidents in Q1 2012*

In Q1 2012, a total of 1,108 incidents were received on Intrusion representing an 18.34 percent decrease compared to the previous quarter. The Intrusion incidents reported to us were mostly web defacements or known as web vandalism followed by account compromises. Based on our findings, the majority of web defacements were due to vulnerable web applications or unpatched servers involving web servers running on IIS and Apache.

In this quarter, we received a total of 689 .MY domains defaced belonging to various sectors such as private and government sites hosted on servers belonging to local web hosting companies. MyCERT responded to web defacement incidents by notifying the respective Web Administrators to rectify the defaced websites by following our recommendations.

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

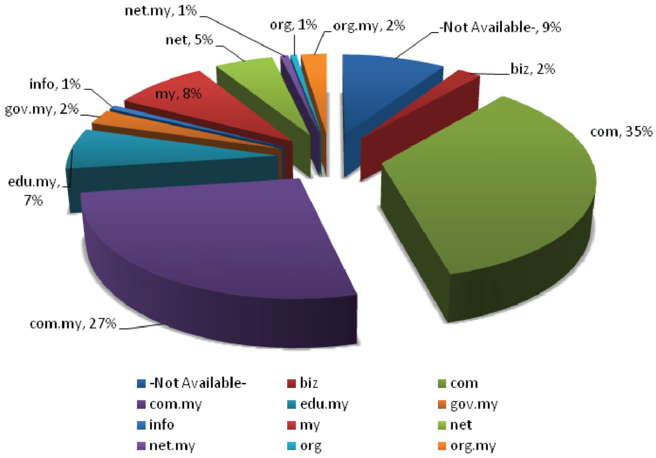


Figure 4: *Percentage of Web Defacement by Domain in Q1 012*

Account compromise incidents continue in this quarter as was in the previous one with an increase of 68 incidents compared to 57 in Q4 2011. Account compromise incidents has become a trend nowadays in which unscrupulous individuals take advantage of various techniques to compromise legitimate accounts. The increase in Internet banking and usage of social networking sites combined with lack of security awareness had contributed to the increase in account compromise incidents. Account compromise incidents reported to us involved mostly free based email accounts and social networking accounts. These incidents could have been prevented if users practised good password management such as using strong passwords and properly safeguarding them.

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

Incidents involving fraud had increased to about 29.31 percent in this quarter compared to the previous quarter. Fraud incidents continue to be a trend in this quarter and is one of the most frequently reported incidents to Cyber999. In fact, fraud has become a global trend involving phishing, Nigerian scams, lottery scams, illegal investments and job scams as it provides attractive financial returns to the perpetrators.

A total of 1,153 incidents were received in this quarter, from organisations and home users. Phishing incidents involving foreign and local brands still prevail in this quarter along with other types of frauds. Incidents on job scams also increased targeting other industries such as hospitals and specialist centres.

We continue to receive incidents on cyber harassment in this quarter. However, the number had dropped to about 23.80 percent with a total of 80 incidents. Harassment reports generally involved cyberstalking, cyberbullying, threatening done via emails and social networking sites. A new trend we observed in this quarter is luring victims into posing nude in front of video cams while chatting with the perpetrators via Skype or MSN Messenger. The captured nude pictures of these victims will then be used to threaten the victims to pay some amount of money failing which the pictures will be publicly exposed on social networking sites. We advised users to be very precautious with whom they communicate or chat on the Internet especially with unknown individuals.

In Q1 2012, MyCERT had handled 189 incidents on malicious codes, which represented a 33.09 percentage increase compared to the previous quarter. A few of the malicious code incidents we handled were active botnet controllers, hosting of malware or malware configuration files on compromised machines and malware infections on computers.

Advisories and Alerts

In Q1 2012, MyCERT had issued a total of ten advisories and alerts for its constituencies involving popular end-user 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 into opening a specially crafted file (i.e. a PDF document) or a 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.

Conclusion

In conclusion, the number of computer security incidents reported to us in this quarter had decreased slightly compared to the previous quarter. However, several categories of incidents reported to us continue to increase. The slight decrease could be a positive indication that more Internet users are aware of current threats and are taking proper protection measures against them. No severe incidents were reported to us in 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. ■

Benefits of ISO/IEC 27005:2011 Information Security Risk Management

BY | Noor Aida Idris, Lt Col Asmuni Yusof (Retired)

Introduction

The increasing numbers of cyber security incidents has resulted in managing information security as one of the top agendas in many organisations. Organisations have to keep up-to-date with information security risks introduced by new and advanced technologies, in addition to their own reliance with such new technology since organisational information now resides in a digital world as well as in physical mediums.

Information security management was introduced to ensure organisations were able to secure their most valuable information assets, which concerns critical business information. By proactively protecting information assets and managing information security risks, organisations can reduce the likelihood and/or the impact on their information assets from a wide range of information security threats. Today, there are various mechanisms being practised by different organisations in managing information security. Among which is via information security management systems based on ISO/IEC 27001: 2005 Information Security Management Systems (ISMS) - Requirements.

ISO/IEC 27001 is one of the published standards in the ISO 27000 family that provides the general requirements for implementing information security management systems. This standard provides organisations with means for protecting their information (in terms of confidentiality, integrity, availability) and providing clients, partners and regulators, assurance of compliance to an internationally recognised set of information security requirements. It is a risk-based approach that provides a holistic and structured way in managing information security for organisations.

Risk management is an important concept through information security management. Information security risk management is needed to ensure the confidentiality, integrity and availability of information assets is preserved by organisations. According to (Humphreys, 2008), risk management is the key to information security governance by an organisation and to the protection of its information assets. If the organisation is unaware of the risk(s) it faces, it will not deploy or implement security controls; thus fail to protect its most critical assets. Several guidance are available to assist organisations manage their information security risks, one of it is ISO/IEC 27005:2011 Information Security Risk Management. The objective of this paper is to convey benefits of implementing information security risk management based on ISO/IEC 27005:2011 Information Security Risk Management.

Introduction to ISO/IEC 27005:2011- Information Security Risk Management

ISO/IEC 27005 contains description of information security risk management processes and activities, which provide guidelines to organisations to manage their information security risks. This standard, which was first introduced in 2005, has been revised recently and re-published in 2011. The standard is one of the standards which play a significant role for the successful implementation of ISMS.

Benefits of ISO/IEC 27005

In the authors' opinion, there are several key advantages when organisations refer to ISO/IEC 27005 for implementing information security risk management. Firstly, this standard can be used by any type of organisation. Secondly, this standard supports the requirements of information security risk assessment specified in ISO/IEC 27001. And thirdly, this standard, which has been revised to align with three other risk management standards, can be used by organisations that wish to manage their information security risks in similar fashion to the way they manage other risks.

This standard is applicable to any type of organisation

One of the attractions of ISO/IEC 27005 is the risk management processes described in the standard which is applicable to all organisations, no matter the size or type. As a matter of fact, the information security risk management processes defined by the standard can be applied not just to the organisation as a whole, but to any discrete part of the organisation (e.g. a department, a physical location, a business service or a critical function), any information system, existing or planned or particular aspects of control (e.g. business continuity planning).

Information security risk management described in ISO/IEC 27005 consists of five processes which are: context establishment, information security risk assessment, information security risk treatment, information security risk acceptance, information security risk communication and consultation and information security risk monitoring and review. These five processes are illustrated in Figure 1.

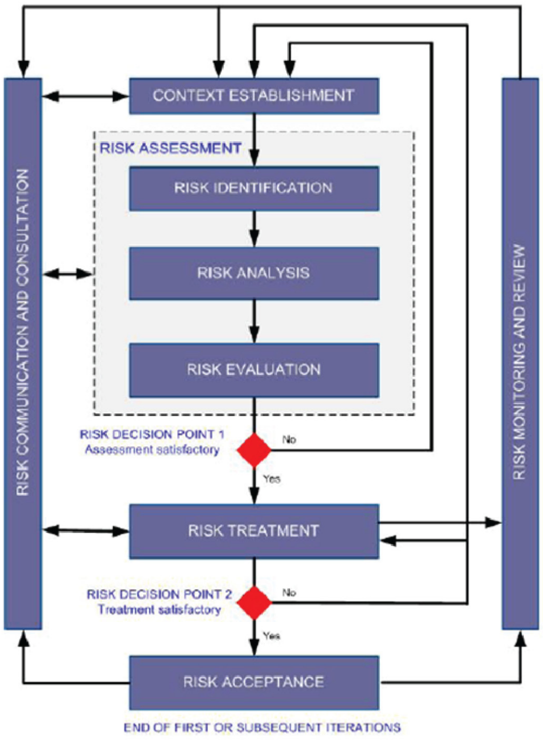


Figure 1: *ISO/IEC 27005 Information Security Risk Management Processes*

The standard supports risk assessment requirements specified in ISO/IEC 27001

Another key benefit offered by the ISO/IEC 27005 standard is that it supports the information security risk assessment requirements specified in ISO/IEC 27001. Thus, organisations that wish to be certified against ISO/IEC 27001 certification may refer to ISO/IEC 27005 when implementing the information security risk assessment.

The mapping of clauses in ISO/IEC 27005 with risk assessment requirements in ISO/IEC 27001 is discussed in detail below:

a) Clause 7 – Context establishment
In ISO/IEC 27005, the context of risk management for an organisation is established first. In establishing context for risk management, both external and internal context for setting the basic criteria necessary for information security risk management, defining the scope and boundaries, and establishing an appropriate organisation operating the information security risk management. The context establishment process is in line with ISO/IEC 27001:2005 clause 4.2.1 c) Define the risk assessment approach of the organisation.

b) Clause 8 – Information security risk assessment
The context establishment process is followed by a risk assessment process. There are three sub processes included in a risk assessment process which are risk identification, risk analysis and risk evaluation. Risk assessment process determines the value of the information assets, identifies the applicable threats and vulnerabilities that exist (or could exist), identifies the existing controls and their effect on the risk identified, determines the potential consequences and finally prioritises the derived risks and ranks them against the risk evaluation criteria set in the context establishment. The information security risk assessment process is in line with ISO/IEC 27001:2005 clause 4.2.1 d) Identify the risks and e) Analyse and evaluate the risks.

c) Clause 9 – Information security risk treatment
Next is the risk treatment process. The information security risk treatment process involves planning to treat the identified risks. There are 4 options available for risk treatment: risk modification, risk retention, risk avoidance and risk sharing. Selecting the risk treatment options should be based on the outcome of the risk assessment, the expected cost for implementing these risk treatment options and the expected benefits from these options. The information security risk treatment processes is in line with ISO/IEC 27001:2005 clause 4.2.1 f) Identify and evaluate options for the treatment of risks.

d) Clause 10 – Information security risk acceptance
The decision to accept the risks and responsibilities for decisions are made and formally recorded in the information security risk acceptance process. This process is important to ensure that the upper management is aware of the risks and also on the plans to treat the risks. The information security risk acceptance process is in line with ISO/IEC 27001:2005 clause 4.2.1 g) Select control objectives and controls for the treatment of risks and h) Obtain management approval of the proposed residual risks.

e) Clause 11 – Information security risk communication and consultation
The risk communication and consultation process involves activities to achieve an agreement on how to manage risks by exchanging and/or sharing information about those risks between the decision-makers and other stakeholders. The information security risk communication and consultation process is in line with ISO/IEC 27001:2005 clause 4.2.4 c) Communicate the actions and improvements to all interested parties with a level of detail appropriate to the circumstances and, as relevant, agree on how to proceed.

f) Clause 12 – Information security risk monitoring and review
On-going monitoring and review of current information security

risks are important because risks are not static. New threats and vulnerabilities may arise at any point in time; likelihood or consequences may change abruptly without any indication. Thus, constant and continuous monitoring on the risks is necessary to detect these changes. By conducting regular monitoring and review may also ensure that the risk management context, the outcome of the risk assessment and risk treatment plans remain relevant to the organisation. The information security risk monitoring and review process is in line with ISO/IEC 27001:2005 clause 4.2.3 d) Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks.

Easy alignment with other risk management standards

Another advantage for organisations that choose ISO/IEC 27005 when implementing information security risk management is that they can align the way they manage other risks, such as enterprise-wide risks, with information security risks. This is due to ISO/IEC 27005 being revised recently to reflect changes in three risk management standards which are:

- ISO 31000:2009 - Risk management - Principles and Guidelines;
- ISO 31010:2009 - Risk management - Risk Assessment Techniques; and
- ISO Guide 73:2009 - Risk Management Vocabulary.

As an example, organisations that have adopted ISO 31000 for managing their enterprise-wide risks may find that they can manage their information security risks in a similar fashion. Thus, lesser time and resources may be used when embarking on the journey of adopting ISO/IEC 27005 for information security risk management and implementing ISMS based on ISO/IEC 27001.

Conclusion

Information security risk management is one of the requirements in ISO/IEC 27001 ISMS. As stated earlier, ISO/IEC 27005 is an essential companion for implementing ISMS based on ISO/IEC 27001. The advice and guidance contained in the standard is useful for any organisation intending to manage their information security risks effectively. The three advantages described in this paper can be enjoyed by organisations managing their information security risks based on ISO/IEC 27005.■

References

1. *ISO/IEC, "Information Technology – security techniques – information security risk management systems", ISO/IEC 27005 International Standard, 2011.*
2. *ISO/IEC, "Information Technology – security techniques – information security management system – Requirements", ISO/IEC 27001 International Standard, 2005.*
3. *International Organization for Standardization website, www.iso.org, accessed on 23 March 2012.*
4. *ISO27001 Security website, www.iso27001security.com, accessed on 23 March 2012.*
5. *Humphreys, E. 2008. Information security management standards: Compliance, governance and risk management, information security technical report 13 (2008) 247–255.*
6. *Humphreys E. 2010. Information Security Risk Management – Handbook for ISO/IEC 27001, BSI Standards.*

Securing Your Software Development Life Cycle

BY | Norahana Salimin

> **"When an organisation incorporates security in its SDLC, inevitably it benefits from products and applications that are secure by design."**

Introduction

Quality software does not really mean secure software. Building security into software development is often seemed as a major pain in the neck. In certain cases, security is treated as an obstacle to the successful completion of a software project. That's the reason why security is usually considered as the last factor. The emergence of worldwide cyber-attacks especially in Malaysia [1], where the attackers were targeting software (mostly web applications) used by government agencies, critical national information infrastructure (CNII) and high profile corporations, raised a pertinent question. How seriously did the government and the corporate sector viewed security? How do they ensure that sensitive data belonging to ordinary citizens or customers are not exposed or stolen? There are possibilities that corrective actions may have been taken to resolve the situation. However, what about preventive measures to ensure that lightning does not strike twice? This is where securing the software development life cycle (SDLC) comes into the picture as an attractive preventive measure.

Securing SDLC

Software Development Life Cycle (SDLC) [2] is a process, model and methodology of creating or modifying an information system. According to the International Information Systems Security Certification Consortium, Inc. (ISC)² [3], secure SDLC phases comprised of Requirement, Design, Coding, Testing, Acceptance, Deployment, Operations, Maintenance and Disposal. Initially, developers must have firm concepts of software security. With a solid knowledge in security concepts, only then can it be applied to the phases outlined in SDLC. This paper discusses the best practices on securing the phases of SDLC.

Requirement

The requirement phase or secure requirement is defined as the outline of security controls and the integration of those security controls into the development process. Policy, standards, patterns and practices (PnP), external regulatory and compliance requirements must be included into the security requirements. Confidentiality, integrity, availability, authentication, authorisation and auditing of data must also be included. A way to gather these security requirements is by referring to the modelling methodologies of used and misused cases where understanding the threats against a system will produce the countermeasures to protect the system.

Design

Secure concept in the design phase is basically about structuring the software from a security perspective. Performing a threat modelling exercise will identify the surface attacks and security criteria that will be valuable in structuring the software in terms of security. Security criteria must be met before a particular software is released for deployment. The principles of security design are many. Among them are those having the least privilege, separation of duties, complete mediation, defence in depth, fail safe, weakest links, single point of failure, etc. The technologies being used to match these designs are identity and authentication management, information flow control, audit management, data protection, digital rights management, computing environment and integrity management.

Coding

Secure coding involves the usage of coding and testing standards, applying security testing tools such as fuzzing and static-analysis code scanning and the review of source codes. Knowing common software vulnerabilities and countermeasures such as injection, cross site scripting, buffer overflow and broken session management is a must to ensure these vulnerabilities are covered during coding. Defensive coding practices can be applied such as type safe practises, memory management, error handling and locality. Source code versioning is also important to ensure verified codes are not overwritten by unverified source codes. To ensure codes are not being tampered, digitally signing source codes is now a good practise.

Testing

Secure testing is conducted when software functionalities are complete and ready to enter testing trials. These trials must not be ignored. Black box test is focused on testing without knowledge regarding the design of the software. White box test on the other hand is testing with the required knowledge. Fuzz testing is executed by injecting random data to observe the behaviour of the software while defensive coding testing is the examination of common vulnerabilities in the software.

Acceptance

The acceptance phase is secured by ensuring that the software in question meets the necessary requirements before being deployed. In the pre-deployment stage, the completion criteria and risk acceptance levels needs to be outlined. Software documentation should be in place. In the post-release stage, independent testing, validation and verification of the said software by third parties such as obtaining a Common Criteria certification may be applied.

Deployment,Operations,Maintenance and Disposal

The deployment, operations, maintenance and disposal phase concerns on vulnerabilities that have not been countered by the software and future vulnerabilities that may be discovered during deployment. Software that is delivered to customers should be digitally signed to avoid being tampered with. Installation of software should be securely deployed with the help of an installation manual. Configurations should be hardened to avoid incorrect system implementations. The secure usage of software or system operations should be documented in the operation manual. Patch management and support management should be implemented to gather information from users on errors they encountered, as this may be the source for attackers to launch an attack.

When software is to be replaced or retired, several processes need to be in place to ensure it is executed in a secure manner. If a replacement system exists, the replacement should be operational before retirement takes place. Approval from the management is required before any act of removal or replacement is carried out. Only then the system's access controls are terminated or removed to prevent unauthorised access. Finally, the retired system or software services are to be shut down to reduce the attack potential, securely delete configurations and data from the server and eventually uninstalling the system.

Initiatives to improve security on SDLC

For a child, early childhood education such as preschool and kindergarten is the best method to foster a greater learning development. The same concept applies with our security environment. The 'kindergarten' for most software developers is the higher learning institutions. These institutions can play an important role in the initiative to secure product lifecycles. It can be achieved by emphasising more security aspects in the syllabus to teach future developers the importance of security as a whole. Collaboration between the academic world and security experts from the industry can also speed up the transfer of knowledge since it has become more familiar with the current trends and approaches on the how-to methodologies. With these efforts, our future developers will have a security-in-mind attitude while developing their software, thus reducing the potential of designing unsecured software.

CyberSecurity Malaysia [4], as the national cyber security specialist centre and an agency under the purview of the Ministry of Science, Technology and Innovation (MOSTI) provides ICT security specialist services and continuously monitors threats to national security. In translating the responsibility into implementation, CyberSecurity Malaysia is pioneering the initiative in securing ICT products, regardless of the state of being i.e. software, hardware or firmware. Furthermore, this initiative was established to promote secure product development for developers. The initiative was implemented by establishing a product evaluation scheme in Malaysia.

The established scheme [5] is now known as the Malaysian Common Criteria Evaluation and Certification (MyCC) scheme. The Information Security Certification Body (ISCB) and the Malaysian Security Evaluation Facility (MySEF) were established under CyberSecurity Malaysia to execute certification and evaluation processes separately. The standards [6] that are being used are Common Criteria (CC) and Common Methodology for Information Technology Security Evaluation, which are international standards that are widely used for independent security evaluation in ICT products. When a developer enters into a CC certification, CyberSecurity Malaysia MySEF will evaluate not only the product but also the SDLC phases of the product to ensure it was executed in a secure process. However, the depths of verifying the SDLC processes will depend on the evaluation assurance level (EAL) chosen by the developer for their product. The benefit of a CC certified product is that the developer will have some level of assurance that their product was properly tested and verified by a third party on its security features. The other benefit is that the developer's potential customers (government agencies or corporations) may favour a CC certified product because of a certain level of confidence in the security functionalities.

Conclusion

The initiatives taken by developers to secure overall software lifecycle and the extra initiatives taken to promote secure product development and usage by the government and higher learning institutions will eventually reduce the possibility of a successful attack and exploitation. This will then ensure that only hack-resilient software is created. Securing software lifecycles are not an all-in-one solution because it also very much depends on the hosts, networks and the people using the stated software. However, at least, security flaws are detected at an early stage and thus, reduce software vulnerabilities from being exploited. With all these joint initiatives, we will at least have some assurance that our information and ICT environment are secure from cyber-attacks.■

References

1. *Malaysia Government Websites Disrupted, http://www.bloomberg.com/news/2011-06-16/malaysia-government-websites-attacked.html*
2. *System Development Life Cycle, Wikipedia, http://en.wikipedia.org/wiki/Systems_Development_Life_Cycle*
3. *CSSLP Candidate Information Bulletin, Inc., (ISC)² portal, https://www.isc2.org/cib/default.aspx*
4. *CyberSecurity Malaysia's Web Portal, http://www.cybersecurity.my*
5. *Malaysian Common Criteria Evaluation and Certification (MyCC) scheme portal, http://www.cybersecurity.my/mycc/*
6. *Common Criteria Web Portal, http://www.commoncriteriaportal.org/*

Analysis of Vulnerabilities Report

BY | Sharifah Roziah Binti Mohd Kassim

Introduction

Vulnerability is referred to as security vulnerability or a flaw in a software or application that makes it infeasible even when the product is used properly. The presence of vulnerabilities in software or application provides opportunity to attackers to exploit it and compromise a system. Vulnerabilities reports refer to reports or incidents regarding vulnerabilities that are present in a system, software or application.

Vulnerabilities Report is sub classified into the followings:

- Misconfiguration: A problem exists with certain misconfigurations which may allow root access or system compromise from any account on the system and might lead to information leak, data manipulation and many more.
- Web: User or complainant report vulnerabilities which are related to websites.
- System: User or complainant report vulnerabilities on any specific system.

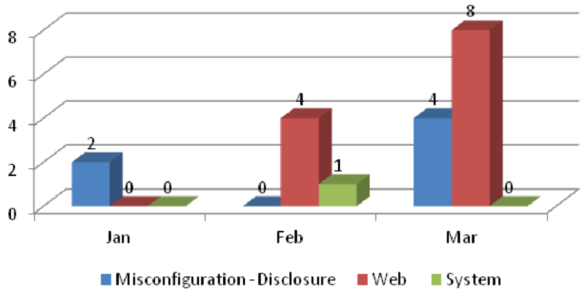
Vulnerabilities Reports are basically received from third parties and very seldom from the owner of the systems or web themselves. Third parties include those from CyberSecurity Malaysia on pro-active monitoring and information received from trusted sources such as from security mailing lists and other Computer Emergency Response Teams.

Vulnerabilities Reports received must be validated first by checking if the reported vulnerability actually exists. Once validated, Incident Handlers will inform the respective owners of the vulnerability and provide recommendations for rectification.

Analysis

Type of Vulnerabilities	Jan	Feb	Mar
Misconfiguration - Disclosure	2	0	4
Web	0	4	8
System	0	1	0
TOTAL	2	5	12

Table 1: *Vulnerabilities Report Q1 (Jan - Mar) 2012*



Graph 1: *Vulnerabilities Report Q1 (Jan - Mar) 2012*

Out of the 19 incidents, six incidents involved misconfigurations, 12 involved websites and one involved system as shown in Table 2 and Graph 2 below.

Type of Vulnerability	Total
Misconfiguration - Disclosure	6
Web	12
System	1

Table 2: *Total Incidents on Sub Categories of Vulnerabilities*

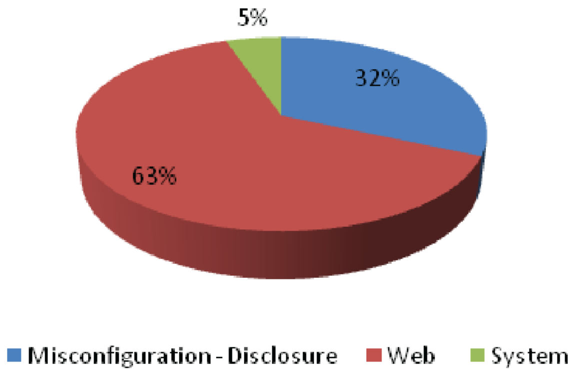


Table 2: *Percentage of Incidents by Sub Categories of Vulnerabilities*

From the graph above we can see that the majority of vulnerabilities incidents involved web with a total of 63 percent compared to other sub categories. This is followed by misconfigurations at 32 percent and systems at 5 percent.

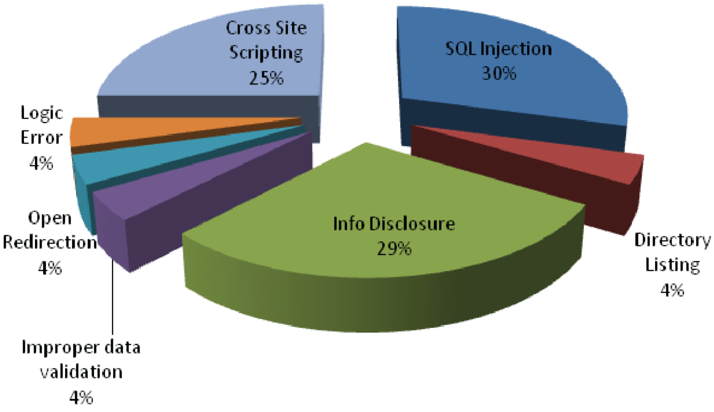
Researchers at WhiteHat Security have discovered that the duration of an average site exposed to vulnerabilities is about 270 days before they are remediated. The big time gap actually gives more opportunity for attackers to exploit the vulnerable websites. Vulnerabilities in web are mostly due to vulnerable web applications due to improper input validation and sanitisation, improper error checking and handling.

Web Application Developers can follow general good practises in securing their web applications where inputs are properly validated and sanitised and errors are properly checked and handled.

Various types of vulnerabilities were discovered based on the incidents received which were SQL Injection, Directory Listing, Info Disclosure, Improper Data Validation, Open Redirection, Logic Error and Cross Site Scripting. The number of incidents received on the above vulnerabilities can be referred at Table 3 and Graph 3 below.

	Jan	Feb	Mar	TOTAL
SQL Injection		2	5	7
Directory Listing	1			1
Info Disclosure	1	2	4	7
Improper data validation		1		1
Open Redirection			1	1
Logic Error			1	1
Cross Site Scripting			6	6

Table 3: *Figure on Different Types of Vulnerabilities*



Graph 3: *Percentage of Incidents on Different Types of Vulnerabilities*

Based on analysis, the most popular vulnerability reported is SQL Injection vulnerability representing 30 percent compared to other vulnerabilities. This is followed by Information Disclosure representing 29 percent and Cross Site Scripting which is at 25 percent. Directory Listing, Open Redirection, Logic Error and Improper Data Validation each is at four percent.

An open redirect is an application that takes a parameter and redirects a user to the parameter value without any validation. This vulnerability is used in phishing attacks to get users to visit malicious sites without them realising it. Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications (such as web browsers through breaches of browser security) that enables attackers to inject client-side script into web pages viewed by other users. SQL injection is an often used technique to attack databases through a website. This is usually done by including portions of SQL statements in a web form entry field or GET requests in an attempt to get the website to pass a newly formed rogue SQL command to the database (e.g. dump the database contents to the attacker).

Administrators may refer to the URL below for recommendation on fixing SQL Injection vulnerabilities:

http://www.mycert.org.my/en/resources/web_security/main/main/detail/573/index.html

Information disclosure enables an attacker to gain valuable information about a system. The disclosure could be due to unintentional acts, misconfigurations or due to vulnerabilities.

Directory listing is referred to as a web server that is configured to display the list of all files contained in this directory. This is not recommended because the directory may contain files that are normally not exposed through links on the web site. A user can view a list of all files from this directory possibly exposing sensitive information. Logic error is a bug in a programme that causes it to operate incorrectly, but not to terminate abnormally (or crash). A logic error produces an unintended or undesired output or other behaviour, although it may not immediately be recognised as such. Improper data validation is when software does not validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in an altered control flow, arbitrary control of a resource, or arbitrary code execution.

Common incidents related to vulnerabilities found in Q1 2012:

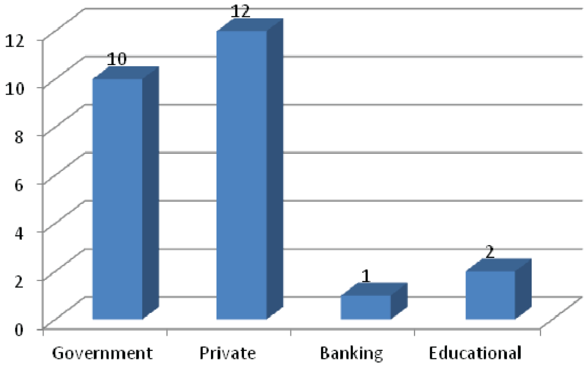
1. Directory Listing on web server due to misconfiguration on the web server which allows directory listing on any folders handled by the web server.
2. Information disclosure or data leak which enables anyone to view database information belonging to the website.
3. Email account passwords belonging to users in an organisation's had been leaked/disclosed and posted on public websites such as at pastebin.
4. Misconfigurations that allow any user to view file configurations of a system or web.
5. Vulnerable websites allows users to change the value of their total amount of payment that had been valued/passed by a website to payment gateways during payment processes. By right, websites should not allow users to modify the value or payment parameters as the value is a fixed value set by the website.
6. Vulnerabilities found in the web applications allowing remote users to view phpmyadmin settings.
7. Information disclosure by government staffs on public/free discussion groups the likes of YahooGroup.
8. Cross site scripting is a web application vulnerability allowing a remote attacker to trick users in executing malicious scripts via their websites.

Out of the 19 incidents received on Vulnerabilities Report, a total of 25 websites and systems were reported. These websites and systems belonged to various sectors ranging from government agencies, financial institutions and private and educational entities as shown in

Table 4 and Graph 4.

Sectors	TOTAL
Government	10
Banking/Financial Institutions	1
Private Sector	12
Educational	2

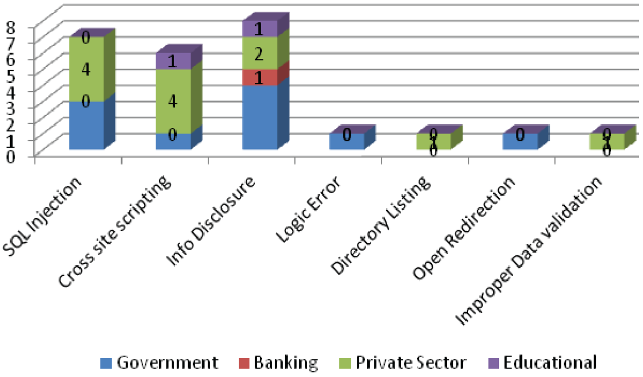
***Table 4:** Figure on total incidents based on Sectors*



***Graph 4:** Total Incidents on Vulnerability Reports based on Sectors*

A total of 12 vulnerable websites were found to belong to private sector firms, followed by 10 website involving government agencies, two websites involving educational institutions and one website involving a banking firm.

Out of the figures above, Information Disclosure vulnerabilities were mainly detected in the government sector websites which were at four websites, followed by private sector with two websites. Banking and educational sector recorded one website each that were vulnerable to Information disclosure, as can be referred to in Graph 5. SQL Injection and Cross Site Scripting vulnerabilities were mainly found in websites belong to the private sector with four websites on SQL Injection and another four websites on Cross Site Scripting, followed by the government sector with three websites vulnerable to SQL Injection and one website vulnerable to Cross Site Scripting.



***Graph 5:** Break of Type of Vulnerability Based on Sectors*

Conclusion

In conclusion, the number of incidents received in this quarter on Vulnerabilities Report was considered low with a total of 19 incidents. Though the number was not alarming, System Administrators must be vigilant on vulnerabilities that may be present in their systems and applications. The repercussions from these vulnerabilities can be severe to the affected organisations even due to a small misconfiguration in their systems such as disclosure of sensitive information to the public belonging to the organisation. The disclosed information can be further manipulated by irresponsible parties for malicious purposes on the net. As such, System Administrators must always make sure their systems and applications are regularly patched/updated and checked/fixed for any errors or misconfigurations. In addition, they are advised to regularly monitor their logs to detect any anomalous activities in their systems.■

References

1. *http://infosecisland.com/blogview/12417-Report-Websites-Remain-Vulnerable-to-Attacks.html*
2. *http://www.mycert.org.my*
3. *http://www.sans.org*

Security Challenges Emerge with IPv6

BY | George Chang

"Most systems that are not IPv6 enabled have the ability to handle a work-around, which is to wrap an IPv6 packet with an IPv4 header. They read the header, but they cannot read the contents of the packet itself."

No doubt, the global launch of the Internet Protocol, IPv6 on June 6, 2012 ushers in a new era in the evolution and widespread adoption of Internet infrastructure around the globe. As the successor to the current Internet Protocol, IPv4, IPv6 is critical to the Internet's continued growth as a platform for innovation and economic development.

The world already has had a small taste of what is to come in June of last year during World IPv6 Day. Spearheaded by the Internet Society, the effort galvanized more than 1000 Web sites, tech companies and ISPs to collectively switch to IPv6 for a total of 24 hours in an effort to "test drive" the protocol to predetermine and mitigate any possible glitches that might occur during an actual launch.

On June 6, 2012, top tech organizations and Web leaders such as Google, Facebook and Yahoo!, among others have made the leap to the updated Internet protocol, IPv6, in an official worldwide launch. Yes, this time, IPv6 is here to stay.

And the transition has become increasingly necessary. The current IPv4 protocol, which can handle around 3.7 billion addresses, has simply run out of address space, thanks in part to the mobile device explosion. Meanwhile IPv6, for all intents and purposes, has unlimited address capacity to accommodate a rapidly growing global Internet and mobile infrastructure.

However, with the launching of the IPv6 protocol worldwide, researchers and IT professionals are anticipating some challenges, especially on the security front.

For one, the relative newness and lack of knowledge around the IPv6 protocol will inevitably pave the way for misconfigurations, compatibility issues and other implementation gaffes. There is not the institutional knowledge around IPv6 the way there is around IPv4, which has been around for decades and enjoys an extensive knowledge base.

But perhaps the biggest security

issue is that many security networking devices are equipped with capabilities that allow them to forward IPv6 traffic, but not inspect it. And, because IPv6 is enabled by default on many platforms in networks today – such as Windows 7 – IPv6 compliant systems are already installed in their networks.

Most systems that are not IPv6 enabled have the ability to handle a work-around, which is to wrap an IPv6 packet with an IPv4 header. They read the header, but they cannot read the contents of the packet itself. They cannot do their normal deep packet inspection, and they just forward the packet. Only when they have a dual stack implementation would they be allowed to simultaneously allow network security functionality to both process and fully inspect packets from both the IPv4 and IPv6 protocols.

Several vendors have this functionality it – not all – and that's one of the risks facing network security professionals today. People have to make sure that their security product can inspect IPv6 traffic. If it can just forward IPv6 traffic, it could be forwarding malicious content.

Even with a dual stack implementation, however, organizations need to determine if they have the same feature set enabled for the IPv4 protocol as they do for IPv6. If not, the network security devices could be overlooking critical pieces of malicious traffic that could potentially compromise their network.

Some of the policies in IPv4 and technologies you rely upon may only work in IPv4 and not IPv6, which means gaps in your security coverage. In this case, however, knowing is not even half the battle. Upgrading networking security infrastructure to accommodate IPv6 is no small undertaking and will likely take years to be phased in completely. Subsequently, many organizations, facing potentially costly and time consuming hardware upgrades, are not planning to embrace IPv6 any time soon.

Yet enterprises cannot shy away from the issue for too long as a lot more IPv6 traffic will hit their networks after the 6 June launching. When IPv6 is going to be 5 to 10 percent of your data – rather than a fraction of a percent – upgrade avoidance becomes much harder to justify. Enterprises and CIOs need to start pondering over the problem soon.■

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.*

Principles of Security

BY | John Hopkinson

The “Principles of Security” must be kept in mind and should underlay all security guidelines and activities. They are particularly important, and should be used for guidance, when the rules (laws, policies, etc.) are absent, not clear, or are in conflict. The following Principles of Security does not tell you what to do, but they provide guidance in deciding what actions you need to take.

Sensitive Information

All organisations have information, the disclosure or compromise of which, by whatever means, may have undesirable consequences. It has long been established that structured physical protection of sensitive information is a necessity. With the growing dependence on information technology, it follows that structured protection must exist within those resources.

Proven Environment

Until proven secure by a responsible authority, no environment shall be assumed to be secure. The assumption of security poses a greater threat than the absence of security. For example, it cannot be assumed that the complexities of commercially supplied hardware or software afford any level of protection.

Individual Accountability

Any person who possesses, or through the use of information technology system(s), processes sensitive information, shall be responsible for the safeguarding of that information and shall be accountable therefore. Any person who uses an information technology system which processes sensitive information shall be responsible for ensuring that any actions related to the processing and/or sanitisation do not serve to degrade or otherwise compromise the integrity of the information technology system. The use of information technology systems are intended to augment human capabilities, but is not intended to replace, circumvent, or otherwise render obsolete, the basic concept of individual accountability.

Least Privilege

Any person, or surrogate information technology resource or feature, shall only be granted that privilege necessary to perform their assigned task or function.

Need-To-Know

Any person shall only be given access to a specific information technology resource if such access is required in the completion of assigned tasks. Only individuals authorised to access sensitive information shall be allowed access to information technology systems:

- that process sensitive information
- have processed sensitive information in the past but have not been appropriately sanitised.

Segregation of Responsibility

Responsibilities must be segregated so that, as far as possible, no one person has total control over a particular resource or process. To avoid total control, dual responsibility should be implemented so that manipulation of that resource cannot be accomplished without the knowledge of another person.

Security Effectiveness

Security is only as good as the knowledge and attitude of the people who use it.

Weak Link Syndrome

Overall security is only as good as the weakest link. These weak links can be exploited by unauthorised parties with malicious intent.

Mutual Acceptance

If a group of people or an individual wishes to communicate with others, the communication must be acceptable by all parties privy to it. The chain of communication is constantly at risk even when information is held in trust.

Levels of Protection

The levels of protection must be implemented gradually so as to be commensurate with the sensitivity of the information processed.

Continuity of Protection

All security principles, policies and mechanisms for their implementation in an information technology environment must be invoked at all times unless specific dispensation has been granted by an appropriate authority. In such a circumstance, a time period must be stipulated.

Protection Implementation

Unless deemed impossible or unnecessary by an appropriate authority, protection features must be implemented to provide multiple levels or rings of security.

Assurance of Protection

Automatic and/or manual protection techniques must be employed regularly to verify that all security mechanisms are invoked and operating properly.

Controls

No control, or a combination thereof, will ever provide total protection. Acceptance of some measure of risk is unavoidable. All controls must satisfy the following:

- The risk that is being addressed must be described
- The risk should be capable of being monitored for change of magnitude
- The risk should be quantified, so that the magnitude of risk to be accepted is identified

Risk Acceptance

Risk acceptance is a valid and an appropriate technique for the provision of cost effective security. Risk acceptance may only be used by a competent authority, generally this refers to the Owner.

Security Failure

In all cases of security failure, or doubt arising as to the appropriate action that needs to be taken, the guiding principles are “Default to the Most Secure”. Only in exceptional circumstances shall the competent authority moderate this principle. A decision to moderate must be confirmed periodically in writing.

Human Fallibility

Individuals who have been screened should be able to be trusted. However, people are fallible and therefore mechanisms and services must be in place to help prevent people from making mistakes.■

Mr. Hopkinson *has extensive experience in the security field in both the military and commercial sectors. As a researcher in information technology security, he focused on assurance, risk analysis, risk management, and security metrics. He develops strategies with regard to standards and consortia activities, and action plans to fulfil those strategies. He assists organizations in developing their security strategies and plans to implement those strategies.*

Keep your data safe: Top 4 tips on Securing iPad

Just in case you have never heard of an iPad, it is a tablet computer from Apple Inc. Its size and weight which fall between smart phones and laptop computers make it a popular device nowadays. The latest model - iPad 3 had been launched recently with exciting features and new specifications.

If you have already bought the latest Apple iPad or planning to buy one for yourself soon, here is some good advice from **Axelle Apvrille, Fortinet's Senior Mobile Anti-Virus Researcher**:

- If connected to 3G: keep an eye on your subscription bill, in particular related to sending SMS or Internet usage. This is what mobile malware use the most, so if something is wrong, check your apps and report any issue to AV vendors and/or your operator. Suspicious samples can be sent for analysis to submitvirus@fortinet.com.

- Don't have your passwords stored by the browser. Rather, use a well-known/well-rated password safe application.

- Do not let applications use your current location or any other private data, unless you really want them to use the information. The less information you grant, the less risky it is.

- Don't jailbreak your iPad, unless you strictly need a jailbroken app or feature. If you do jailbreak it, be sure to change the root password.■

Fortinet *is a leading provider of network security appliances and the worldwide leader in Unified Threat Management (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.*

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 (for advocaters, majistrates, prosecutors, judges and any others)	2 days	1500		9-10										
2	Digital Forensics for First Responder	4 days	3200				3-6								
3	Malaysia Common Criteria (MyCC 1.0) - Understanding Security Target, Protection Profile & Supporting	1 day	790		20					23					
4	Introduction to ISO 27001 & ISO 27002:2005 Information Security Management System	1 day	650	9	10	5	6		11	9	6	3	8	5	10
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						7-8	
11	Forensics on Internet Application	1 day	900											20	
12	Customize Training Package for groups and companies (Fundamental Courses Item 1-12)	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(Oct)-2(Nov)		
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	23-25	8-10	12-14	10-12	7-9	4-6	9-10	6-8	11-13
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	Digital Forensics on Data Recovery	2 days	1800									24-25			
8	Network Security Assessment Training NEW!	2 days	1300											27-28	
9	Server and Desktop Security Assessment Training NEW!	2 days	1300							17-18	14-15	11-12	16-17	13-14	11-12
10	Web Application Security Assessment Training NEW!	1 day	750									11		13	
11	Customize Training Package for groups and companies (Intermdiate Courses Item 1-8)	1-5 days	Negotiable												
	Specialization/Specific Domains														
1	Risk Management NEW!	2 days	1800									19-20			
2	Business Impact Analysis NEW!	2 days	1800									24-25			
3	ISMS Internal Auditor Course (ISO 27001) NEW!	3 days	2850		20-22	12-14	3-5	21-23	19-21	17-19	14-16	18-20	16-18	20-22	18-20
	Professional Certification														
1	Certified Information System Security Professional (CISSP) CBK Review Seminar	5 days	4705				16-20						1-5		
2	System Security Certified Practitioner (SSCP) CBK Review Seminar	5 days	4372				23-27						8-12		
3	Certified Secure System Lifecycle Professional (CSSLP)	5 days	4180				7-11						15-19		
4	SEC504: Hacker Techniques, Exploits & Incident Handling	6 days	USD4400						18-23						
5	Digital Forensics Investigation & Analysis	4 days	3850							16-20					
6	Business Continuity Management Professional Certification (BCLE2000)	5 days	8900			5-9		7-11		9-13			1-5		3-7
7	Professional in Critical Information Infrastructure Protection	3 Weeks	USD6000											19(Nov)-7(Dec)	
8	Cyber Warrior	5 days	4850			19-23			18-22						17-21
9	Cyber Defender	5 days	4890			12-16			11-15						3-7
10	ISO 27001 Lead Auditor (External Auditors)	5 days	5000						25-29	16-20			15-19	26-30	17-21
	Examination														
1	CISSP Examination	6 hrs	USD599		25			12							
2	SSCP Examination	6 hrs	USD300		25			12							
3	Certified Forensics Investigation Analyst (CFIA)		580												
4	Kryterion Test Center			19		29	13	17		13		26		27	
5	Cyber Warrior - Operation D-Day (fully hands on examination)	1 day	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

Ministry of Science, Technology and Innovation

Best Brand Internet Security 2008 & 2009

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

MS ISO/IEC 17025 TESTING SAMM NO. 456 (MySEF LABORATORY)

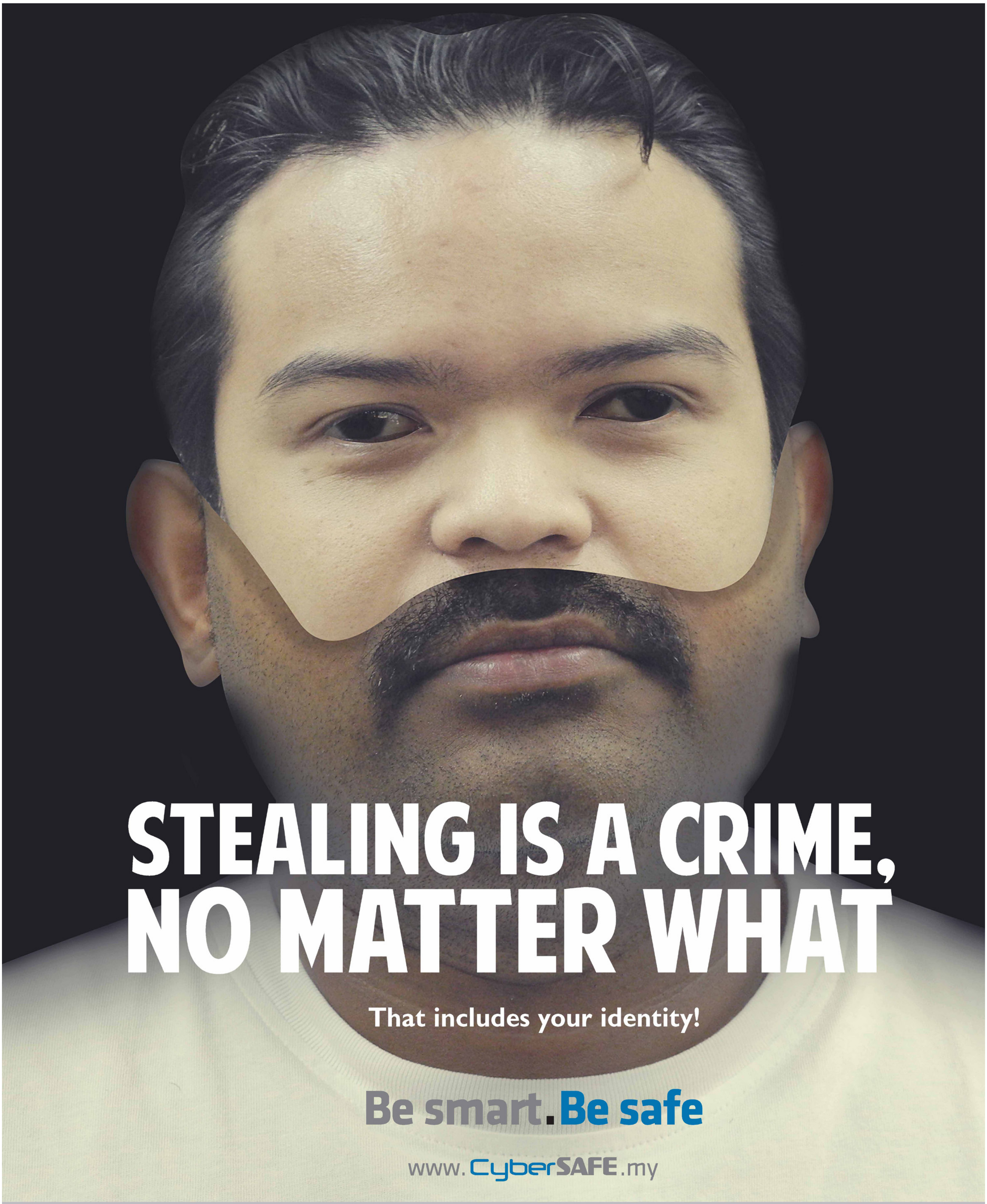
Status Company

CyberSecurity MALAYSIA

An agency under MOSTI

1Malaysia
People First, Performance Now

MOSTI
Ministry of Science, Technology and Innovation



STEALING IS A CRIME, NO MATTER WHAT

That includes your identity!

Be smart. Be safe

www.CyberSAFE.my

Best Brand Internet Security 2008 & 2009

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

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

MSC MALAYSIA Status Company

Corporate Office:
CyberSecurity Malaysia, Level 8, Block A, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor Darul Ehsan | Tel: +603 - 8946 0999 | Fax: +603 - 8946 0888
Email: info@cybersecurity.my | Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my