
IBIMA
Publishing
mobile

Journal of Information Assurance & Cybersecturity

Vol. 2011 (2011), Article ID 664951, 144 minipages.
DOI:10.5171/2011.664951
www.ibimapublishing.com

Information Security Solutions Status and the Roadmap for Future Requirements

Authors

Said K. Al-Wahaibi[1], Norafida Binti Ithnin[1] and Ali H. Al-Badi[2]

[1] Universiti Teknologi Malaysia, UTM Skudai, Johor. Malaysia

[2] Information Systems Department, College of Commerce and Economics, Sultan Qaboos University, Oman

Abstract

Information Security (InfoSec) Surveys conducted worldwide show that the number and type of

InfoSec attacks is expanding daily. This is verified and validated through a survey discussed in this paper. The paper asks a number of questions

concerning InfoSec issues, outlines a survey designed to answer these questions, and then discusses the results obtained within the framework of those

questions. The survey concludes that, although InfoSec awareness exists, best InfoSec practices are usually not being followed. Consequently InfoSec

threats are increasing enormously despite the existence of tools designed to protect against them. Of particular concern is “human factors”, since user

carelessness and negligence may contribute to the issue and may grant hacker’s access to sensitive assets.

Keywords: Information security survey, Hackers attacks, Hackers attacks countermeasures, Conventional InfoSec solutions status, Future

recommendations for InfoSec solutions.

Introduction

Information systems are facing an enormous increase in information security breaches as

hackers always appear to be ahead in discovering system vulnerabilities and then generate attacks that bypass defense systems, Breach Security Labs

(2009), Symantec (2009), PWC (2008) and Schryen (2007) discuss the this issue in greater details. Compromised security can impact organizations of

many kinds, including governments, businesses, intelligence services, infrastructure, and education so forth. It can disrupt key operations,

reduce productivity and inflict significant economic losses; Anderson (2008), Denning (2009) and Clarke and Knake (2010) show that governments have

enacted laws to address this type of cybercrime. And indeed why shouldn't they, Infoguard (2010) says "It can take a second to steal a national secret; and

it will cost a high price. Ethical hacking brings the message home: If cybercrime is too easy, and the tools to do it are at anybody's fingertips, then it

pays to give more attention to the prevention of this new, often widely underestimated form of crime".

Therefore, improving information security is critical to the operations, reputation, and economic stability of all information systems users. Many

published reports show that hackers are becoming more proficient, and their attacks are becoming extremely destructive, while current InfoSec

protection solutions are not effective against hacker's attacks, which is the reason why these attacks are increasing as highlighted in Maynor et al (2007),

Denning (2008) and Denning and Denning (2010). There must be no doubt that this challenges all organizations, since they will need to proactively

combat the work of unprincipled hackers.

Brancik(2007) mentioned that many hacker's attacks are caused by the insider

which is as high as 80% compared to that from the outsider that is 20%; this is because of the contribution of human factor, where for instance, if legitimate users

do not conduct systems risk and vulnerability analysis, do not use the right protective tools (and do not maintain them up-to-date), or do not use strong

authentication, they may be granting attackers access to their critical assets emphasized in McNab (2004). This is verified and validated through a survey

discussed in this paper. The paper asks a number of questions concerning InfoSec issues, outlines a survey designed to answer these questions, and then

discusses the results obtained within the framework of those questions.

This paper is arranged to first give a brief (in section 2) on the information security survey conducted with respect to the purpose of the survey, the core

issues and the anticipated recommendations; then the scope is given in section 2.1, followed by section 2.2 covering the survey evaluation using both

quantitative and qualitative analysis. After that, the survey results are mapped with the core issues in section 2.3 and conclude in section 3.

InfoSec Survey and the Human Factor

Mohay et al (2003), Savage (2010) and OWASP (2010) show that InfoSec hacking

threats are increasing, and hackers are finding new ways to bypass the wide range of conventional security tools and techniques available (Fire

Walls (FW), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), encryption, Virtual Private Networks (VPN), Network Address

Translation (NAT), subnetting, anti-virus (AV) and anti-spy (AS) ware). Bratus (2007) said “To learn security skills, students and developers

must be able to switch from their traditional conditioning to the attacker's way of thinking".

This InfoSec survey was conducted to directly look at:

1. Information security knowledge and daily practices,

2. How normal people handle InfoSec matters,

3. The level of InfoSec awareness,

4. How human factors lead to security breaches.

The aim was also to see whether implementing InfoSec solutions based on behavioral analysis and hacker's countermeasures would give better

protection against newly emerging InfoSec threats as compared with conventional tools. The survey was therefore

designed to indirectly measure:

1. Whether the concept of a "total security solution" is realistic, and if a model

driven InfoSec solution would prove to be more robust and more effective than conventional approaches;

2. The human factors issue, how it accounts for the success or failure of InfoSec solutions, and whether it has connections

with reverse engineering hacking techniques;

3. Whether InfoSec protection solutions based on behavioral analysis and

counter measures of hacker's techniques form a base line for a total InfoSec protection.

Survey Scope

The survey was conducted using a questionnaire, which comprised 15 questions. The questions

covered training, risk assessments and security policy, applying this policy (if it exists), best InfoSec practices, verifying the effectiveness of current

InfoSec tools, and users' future solution recommendations.

The surveyed sample comprised 100 Information

Technology respondents from different organizations (government 30%, private sector 30% and military 40%); respondents came from

different backgrounds, levels of education and job responsibilities. Of those surveyed, 10 were face to face interviews with senior IT/InfoSec staff, and 90

were sent by email and hard copy to other staff.

Responses were accumulated and classified by scoring one point for

each check received for each given question.Thus the maximum score possible for any one question (given one reply

per question and one reply per respondent) was 100.

Statistical analysis software (SPSS) was used to analyze the data collected, see

Figure 1 for summary statistical results. This showed that the majority of responses scored between 10 and 35 with a mean of 25.16, a standard deviation

of 16.37, and a variance of 268.141. Table 1 (below) shows response frequencies, there being a maximum of 64 for Q14 (Yes), and a minimum of

zero for Q1 and Q4 (Don't care).

Table 1: Infosec Survey Results

Please see Table 1 in full PDF version

Survey Evaluation

The results in Figure 1 and Table 1 reveal interesting information concerning how InfoSec is understood

and used in the organizations surveyed.

It was noted that 72% of surveyed respondents have had no InfoSec training,

15% of respondents update their InfoSec knowledge regularly, and 22% never update their knowledge at all. Systems risk assessment and

vulnerability checks were always performed by only 12% of the surveyed respondents. Security policies were defined for and followed by 46% of

respondents, 22% did not have a security policy.

From Q1 & Q4 respectively it was noticed that the "Don't care" choice scored

0% on the training and the InfoSec policy questions. This suggested that users do care, and have the intention of improving their

InfoSec capabilities, if they get the chance.

Fifty two percent of respondents said they had good authentication and

access controls, whereas 22% didn't have strong authentication. Q6 and Q7 showed that 24% had multiple protection tools active all the time, but only

10% actually set up and updated their systems regularly.

Q7 to Q12 showed human factor shave a major impact

on the number and type of hacker’s attacks, because of careless or unknowledgeable users. Examples of dangerous practices are highlighted by

8% of respondents, who surf or download from unknown or distrusted sites/storage media, and 3%, who open attachments from unknowns or reply to

hoaxes (showing poor awareness of the issues). Examples of good practices are shown by 3%, who encrypt their information and outgoing emails, and

6%,who scan outgoing emails for information leakage. The survey also showed that 28% have a disaster recovery plan, test it regularly, and back up

their important information.

Financial issues are illustrated by Q15, responses showing that

those surveyed think their corporate InfoSec spend is in the low to medium range, it is clearly not much better than those of Q8 to Q12, in fact, it complements those

answers. It is important to note that this result is consistent with the results of a 2008 UK Government Survey on Security Breaches on IC3 (2009)].

Another significant survey finding was indicated by Q13 and Q14, which showed that 54% of respondents have experienced an increase in

InfoSec threats, despite their use of the latest protective tools (that is the second highest value). Sixty four percent of respondents think

implementing InfoSec solutions based on behavioral analysis and hacker's countermeasures would give better protection than current

protection tools (the highest value in the survey), compared to 6% who said they would not (No). Both of these two values were marked by

SPSS as the highest and the lowest values respectively.

Figure 1: Descriptive Statistics of the Infosec Survey Using SPSS

Please Fig 1 in full PDF version

Mapping Core Issues to Survey Questions

In this section, the four core issues above are mapped with the survey question results, to

give the final and the most important findings of the survey.

The first issue was the status of conventional InfoSec

solutions and their effectiveness. This relates to survey questions Q5 to Q7, Q10, and Q13 to Q15. From these it was concluded that conventional InfoSec solutions

are not effective against hacker's attacks.

The second issue was whether the concept of a "total security solution" is

realistic, and whether a model driven InfoSec solution would prove to be more robust and more effective than conventional approaches. This issue

relates to the questions Q5 to Q7 and Q10 to Q14. Responses indicate that the concept of a "total security solution" is not feasible, however, a model driven

InfoSec solution would prove more effective and efficient than conventional solutions.

The third issue concerns human factors, how they impact the success or failure of InfoSec solutions, and whether there is any connection with reverse

engineering hacking techniques. This issue maps to all questions (Q1 to Q15). These showed that human factors have a significant impact on the

success or failure of InfoSec solutions. This is because conventional solutions rely on the users' "good will", which is never achieved fully. On the other hand,

reverse engineering hacking techniques, including behavioral analysis, reduce human factors.

The final issue concerns whether Info Sec protection solutions based on behavioral analysis and counter measures of hackers techniques form a

base line for a total InfoSec protection. This issue was mapped to questions Q5 to Q7 and Q10 to Q14. Here there was a positive answer, because

countermeasure hacker's techniques would analyze and determine hacking processes and behaviors, which is the core of detection and blocking of

breaches. But, not fully a total InfoSec protection as the second survey question denied its existence.

Survey Summary

The survey showed that people have experienced an increase in InfoSec threats, despite the fact

that they often exercise good InfoSec practices and behavior. The top most information security threat comes from hacker's attacks for whatever the

reason is. This implies that there is a research need for more effective InfoSec solutions against hacker's attacks. Answers on the survey question number

14 gave a recommendation for InfoSec countermeasures solutions based on hacker's behavioral analysis; this answer got the highest

score on the survey. There are studies and references that give good guidelines for anti-hacker solution with respect to the type of tools and counter hacker

techniques and policies as covered in Fadia (2006), Erickson (2008) and Lockhart (2004). InfoSec awareness is a dominating part in overcoming the

human factor and the insider issue as stressed by Brancik(2007); that is dealing with human error whatever the reason is, while the best practices

gathers past experience from all sources and utilize it in the best possible way to countermeasure hacker's attacks, Jones and Gallo (2007) and Yuill et al

(2006) give good counter hacking approaches. Counter hacker tools should be carefully identified and selected to fit for purpose such as

access control, Fire Wall, Intrusion Detection Systems, Intrusion Prevention Systems, encryption (files, storage media, mails and links

using SSL, SSH, IPsec, SET), Virtual Private Networks, Network Address Translation, anti-virus and anti-malware knowing that there exist security unit

that combine number of security tools into one unit; these tools are detailed in Kanneganti (2008), McClure et al (2005), Shema et al (2006) and

Smith and Marchesini (2008).

References

Anderson, R. J. (2008). Security Engineering: A Guide to Building Dependable

Distributed Systems, 2nd edition, *Wiley Publishing Inc*., Indianapolis, Indiana

Brancik, K. (2007). Insider Computer Fraud: An In-

depth Framework for Detecting and Defending against Insider IT Attacks, 1st edition, *Auerbach Publications*.

Bratus, S. (2007). "What Hackers Learn That the Rest of us Don't," *IEEE Security & Privacy*, July/August 2007, 5(4).

Breach Security Labs., (2009). 'Web Hacking Incidents Report 2009,' *Breach Security Inc*. (USA). [Retrieved November 02, 2009], available at

[http://www.breach.com/resources/whitepapers/index.html].

Clarke, R. A. & Knake, R. (2010). "Cyber War: The

Next Threat to National Security and What to Do About it," Ecco, (USA).

Denning, D. E. (2008). "The Web Ushers in New

Weapons of War and Terrorism," *Scientific American*. August 18, 2008.

Denning, D. E. (2009). "Barriers to Entry: Are

They Lower for Cyber Warfare?," *IO Journal*, April 2009.

Denning, P. J. & Denning, D. E. (2010). "Discussing

Cyber
Attack," *Communications of the ACM*, 53(9).

Erickson, J. H. (2008). The Art of Exploitation, 2nd

edition. *William Pollock* (USA).

Fadia, A. (2006). The Unofficial Guide to Ethical Hacking, 2nd edition,

Thomson Course Technology (Canada).

IC3 (2009). "IC3 2008 Annual Report on Internet Crime Released,”

[Retrieved June 3, 2011], IC3 (USA). available at [http://www.ic3.gov/media/2009/090331.aspx].

Infoguard AG. (2010). "Seminar on Ethical Hacking and Cyber Crime," *Infoguard* (Switzerland). available at [http://www.infoguard.co

m/ae/index.php?nav=108,126], [Retrieved June 3, 2011].

Jones, W. & Gallo, A. (2007). "A Process-Based

Approach to handling Risks," *IEEE – IT Professional*, March/April 2007, 9(2).

Kanneganti, R. & Chodavarapu, P. (2008). SOA Security, 1st edition, *Manning Publications CO*. (USA).

Lockhart, A.
(2004). Network Security Hacks, *O'REILLY*.

Maynor, D., James, L., Spammer-X, Bradley, T.,

Haines, B., Baskin, B., Das, A., Bhargava, H., Faircloth, J., Edwards, C., Gregg, M. & Bandes, R. (2007). 'Emerging Threats Analysis,' Syngress Force.

McNab, C. (2004). "Network Security Assessment," *O'REILLY*.

McClure, S., Scambray, J. & Kurtz, G. (2005). "Hacking

Exposed: Network Security Secrets and Solutions," 5th edition, *McGraw-Hill/ Osborne* (USA).

Mohay, G., Anderson, A., Collie, B., de Vel, O. & McKemmish, R. D. (2003). Computer and Intrusion Forensics, *Artech House inc.*

OWASP, (2010). "WEB Defender and OWASP top ten," Breach Security Inc. [Online], [Retrieved May 12, 2010], available at [https://www.owasp.org/i

ndex.php/Category:OWASP_Top_Ten_Project]

PWC, (2008). "BERR Survey on Security Breaches," UK Government,

[Online], [Retrieved June 3, 2011], available at: [http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html],

Savage, M. (2010). "Under Attack," *Information Security*, [Online], May 2010, [Retrieved June 3, 2011], available at: [http://viewer.media.bitpi

pe.com/1152629439_931/1272910610_295/0510_ISM_eM.pdf].

Schryen, G. (2007). "Anti - Spam Mesearures,” *Springer*.

Shema, M., Davis, C. & Cowen, D. (2006). Anti-

Hacker Tool Kit, 3rd edition, *McGraw-Hill/ Osborne* (USA).

Smith, S. & Marchesini, J. (2008). "The Craft of

System Security," *Addison Wesley*.

Symantec. (2009). "Global Internet Security Threat Report," *Symantic*, (USA).

Yuill, J., Denning, D. & Feer, F. (2006). "Using Deception to Hide Things from Hackers: Processes, Prnciples and Techniques,”

Journal of Information Warfare, 5(3). 26-40.