Management Policies for the Prevention Technique of Social Engineering (SoE) Attacks in the Organization

Nik Zulkarnaen Khidzir, Shekh Abdullah-Al-Musa Ahmed and Tan Tse Guan

Faculty of Creative Technology and Heritage, University Malaysia Kelantan, Malaysia

Summary
Information security in an organization will continue to face SoE attacking threat given the global paradigm in today's digital economy. It is the responsibility of management to address the security issues by forming appropriate security policy for the prevention technique of SoE attacks in the organization. The matter of security implementation is complex and all stakeholders must be involved to understand and commit to the hierarchical relationship of the organization's business objectives to its security policies down to procedures. Standards and guidelines must also be considered for their in security policy for the prevention technique of SoE attacks.

Key words:
SoE ; information security ; policies ; risk management; security policies .

1. Introduction

The prime reason for the SoE attacks is internet connectivity in the organizations. Though the term policy as a general term along with various types of policies , how-ever the meaning of 'security policies' regarding the SoE attacking risk as a specific term . In generic a policy is one of those terms that can mean several things in the information security domain . For example for the prevention technique of SoE at-tacks , security policies on firewalls which refer to the access control and routing list information in the organizations. A well written policy is more than an exercise created on paper to mitigate risk against SoE attacks – it is an essential and fundamental element of sound security practice [1].
A policy , for example , can literally be a lifesaver during a disaster , or it might be a requirement of a government or regulatory function. As a matter of fact , a policy can also provide protection from liability owing to an employee's actions or can form a basis for the control of trade secrets[2].

2. Related Literature Review

When the term 'policies' is used rather than 'policy' the intent is to refer to those policies that are distinct from standards, procedures and guidelines[3]. Figure 3.1 shows that policies are considered as the first and the highest level of documentation for the organization.

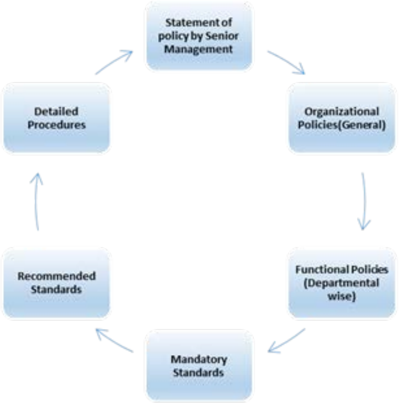

Statement of policy by Senior Management
Organizational Policies(General)
Functional Policies (Departmental wise)
Mandatory Standards
Recommended Standards
Detailed Procedures

Fig. 1 Policy cycle Chart

3. Senior Management Statement of Policy

This is the first step in the policy creation process. Since this article only focus on social engineering attacking risk. So , senior management become the first step in the policy creation for the risk management[4] . In the high level statement of policy that contains the following elements :-

- An acknowledgement of the importance regarding the SoE attacking aware-ness and network port security to prevent this attacks.
- A statement of support for SoE attacking risk throughout the business in organizations.
- A commitment to authorized and manage the definition of the lower level standards, procedures and guidelines.

4. Regulatory Policy

There are security policies for the prevention technique that an organization must implement owing to compliance , regulation or other legal requirements as prevalent in the organizations operating environment , both internal and external [5].
The various entities which the business organization interacts can be financial institute (such as those in

Manuscript received October 5, 2019
Manuscript revised October 20, 2019

banking sector) , public utilities or other types of organizations that operate in the public interest [6] . Regulatory policies are usually very de-tailed and specific to the industry in which the business organization operates. The two main purposes of the regulatory policies are :

- Ensuring that an organizations follows the standard procedures or base practices of an operation in its specific industry .
- Giving an organization the confidence that is following the standard and accepted industry policy.

5. Advisory Policy

These are the security policies for the prevention technique of social engineering at-tacking risk that may not mandated but are strongly recommended [7].

Normally, the consequence of not following them are defined such as Business Conduct Guidelines in an organization – not following these could result in job termination). An organization with such policies want its employees to consider these policies mandatory. Most policies fall under this broad category.

6. Informative Policy

These are policies that exist simply to inform the reader . These are no implied or specific requirements , and the audience for this information could be certain internal entities (within the organization) or external parties [8]. Having discussed the term ‘policy’ in general , let us now turn to ‘security policy’. A security policy is a statement produced by the senior management of an organization , or by a selected policy board or committee to dictate what type of role security plays within the organization . Security policy against the SoE attacks can be defined as a codified set of process and procedures applied to secure the fulfillment of its obligations and continuation of its activities even in the presence of possible interferences . Security policies against SoE attacks are most often referred to in the context of information technology(IT) , telecommunication(TC) or information and communication technology (ICT) . Moreover they are often erroneously though , associated exclusively with deployment of computer hardware or software , to the point of the configuration being called security policy against SoE attacks . The definition given in the International Organi-zations for Standardization (ISO) standard 17799 in a slightly different are risk management and should set a clear policy direction and demonstrate support for and committed to , information security through the issue and maintained of an information security policy across the SoE attacking risk factors in the organization [9] . Below figure 4.2 showing the building block of risk management for the prevention technique of SoE attacks .

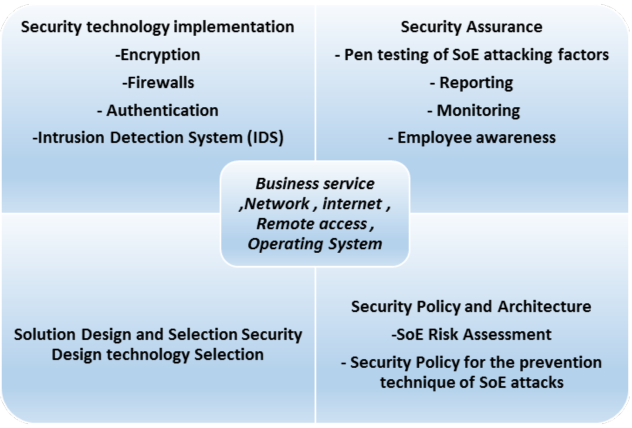

Security technology implementation
-Encryption
-Firewalls
- Authentication
-Intrusion Detection System (IDS)
Security Assurance
- Pen testing of SoE attacking factors
- Reporting
- Monitoring
- Employee awareness
Business service ,Network , internet , Remote access , Operating System
Solution Design and Selection Security Design technology Selection
Security Policy and Architecture
-SoE Risk Assessment
- Security Policy for the prevention technique of SoE attacks

Fig. 2 showing the building block of management system for the prevention technique of SoE attacks .

7. Social Engineering Attacking Risk Factors Scenario in Financial Sectors

In the financial sector , almost every bank has created a comprehensive document that lays down a number of security related guidelines and strategies for banks to follow in order to offer Internet banking . The guideline broadly talk about the types of SoE attacking risk factors associated with Internet banking , the technology and security standards , legal issues involved and regulatory and supervisory concerns . Any bank that wants to offer Internet banking must follow these guidelines and ad-here to them as a legal necessity[10] . Recent InfoSec survey indicate that the banking and finance sector companies , most serious about security regarding social engineering attacks and regarding social engineering attacks and regularly revise their security policies following periodic IS audit .

8. Methodology

There should a mechanism that works well for the management system for the prevention technique of SoE attacks , whose objective is to provide a systematic approach to managing sensitive information in order to protect it . It encompasses employees , process and information[1] . Showing in the figure 4.4 . In this article it is showing that some basic measures must be applied to secure the information sys-tem . Social engineering threats must be managed and controlled and established a global policy , that is , a broad security policy , with management involvement helps to do this . While doing this , four levels of documentation emerge , as depicted in Figure 3.1

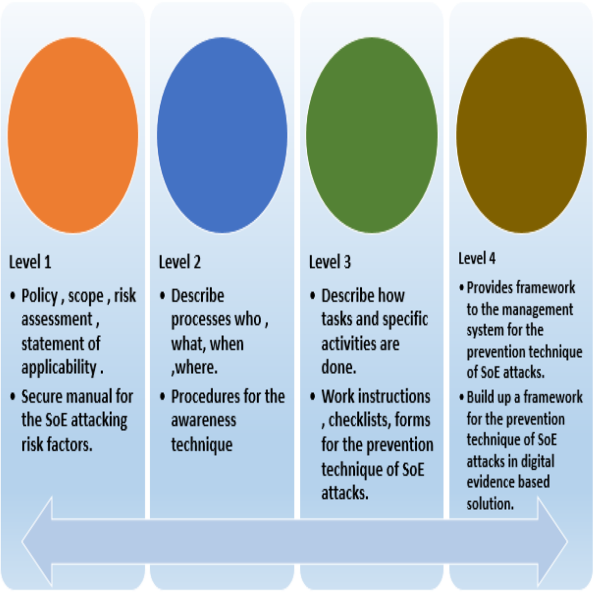

Level 1
• Policy , scope , risk assessment , statement of applicability .
• Secure manual for the SoE attacking risk factors.
Level 2
• Describe processes who , what, when ,where.
• Procedures for the awareness technique
Level 3
• Describe how tasks and specific activities are done.
• Work instructions , checklists, forms for the prevention technique of SoE attacks.
Level 4
• Provides framework to the management system for the prevention technique of SoE attacks.
• Build up a framework for the prevention technique of SoE attacks in digital evidence based solution.

Fig. 3 Documentation level of Management policies for the prevention technique of SoE Attacks

Since in this article describing the management process of the prevention technique of SoE attacks[2] . And to identify the nature of possible threats of SoE attacks . One of the best practices is to establish a set of measure called ‘controls’ . Controls are meant to ensure the security and beyond that to also ensure the privacy and confidentiality of information stored in the systems[3]. It is then necessary to continually evaluate the controls with the auditing process.

9. Organizational Responsibilities for the Management of Prevention Technique of Soe Attacks

Basically in this article describing the management policies for the prevention technique of SoE attacks in the organizations. Ideally ‘best practices’ begins at the top and percolate down in the organization. The senior management team members of an organization are the strategies with version and long term view. This exemplify their asset protection intent with the well-set policies directed toward this[4] . One of the important tasks for the top management in an organization is to make their employees aware of the SoE attacks . This starts with the formation of ‘ security policies’ as we see in this article . Security policies , standards and procedures stand in a certain hierarchical relationship in alliance with the organization’s overall business goals . This illustrated in figure 4.5 . There are a few important points to be noted with respect to figure 4.1 .Frist of all , to be understood and effective , policies of the prevention technique of SoE attacks must be traceable back to the corporate objectives .

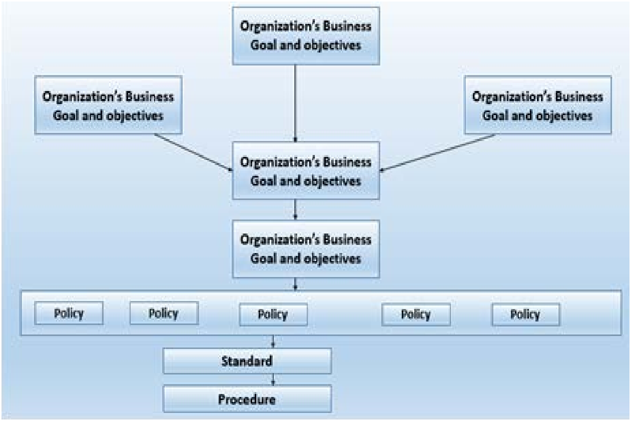

Organization's Business Goal and objectives
Organization's Business Goal and objectives
Organization's Business Goal and objectives
Organization's Business Goal and objectives
Organization's Business Goal and objectives
Policy
Policy
Policy
Policy
Policy
Standard
Procedure

Fig. 4 Hierarchy of security policies , standards and procedures

Typically , the management works together with the chief security officer (CSO) and chief information officer (CIO) taking their technical assistant to find the most possible way a social engineering attacker to get into the system[5]. So, after per-forming a network scan of its business operations environment, an organizations may arrive at a conclusion that they operate a high level of risk in its mitigate the risk of SoE attacks in the organization and must follows strategy[5] . Thus a management role lies in defining business strategies , guidelines and processes / procedures as well as considering the volume of data , systems , sub processes and persons. So , planning to be performance.

- Allocate resources.
- Assign responsibilities.
- Document the process
- Provide tools.
- Ensure training for prevention of SoE attacks .
- Plan the process

A convincing sample collection methods was done regarding the experience of SoE attacks in the organization, there were total 87 questionnaire were distributed in the organization and 39 returns , so 44% response rate .However the experience of SoE attacking risks , respondent response were regarding suspicious mail or unexpected called , 30% had shown such experienced and 69% had shown not this type of experience.

Regarding unexpected mail 41% had not get any this type whether 58% had this experienced.

Questionnaire were asked whether employee noticed any unauthorized person without proper id worked in organization 30% respond that had never seen any type of people but 25% had this type of experience.

Even what would be the decision would they take , so the response were 15% said blocked the number, 7% were respond that cancel the call, 9% were delete the mail , 20% were respond contract with security expert and 27% were respond about block the number .So the respondent table 1.1 would be as below . Table 1.1 : Showing the respondent response table

Experience of SoE attacks_1	***f***	***Rel f***	***cf***	***Percentile***
No	13	0.33	39	100
Yes	26	0.66	26	66
Total	39			
Experience of SoE attacks_2	***f***	***Rel f***	***cf***	***Percentile***
No	12	0.30	39	100
Yes	27	0.69	27	69
Total	39			
Experience of SoE attacks_3	***f***	***Rel f***	***cf***	***Percentile***
No	16	0.41	39	100
Yes	23	0.58	23	58
Total	39			
Experience of SoE attacks_4	***f***	***Rel f***	***cf***	***Percentile***
Block the mail	12	0.30	39	100
Contract with security expert	10	0.25	25	64
Delete the mail	6	0.15	17	43
Cancel the call	3	0.07	11	28
Block the number	8	0.20	8	20
Total	39			

10. Conclusion

In the present global digital economy , information flows more often than not through the complex IT infrastructure present[8][9]. To be efficient at managing , operating and protecting this IT infrastructure, there is a need for having a common set of guidelines for the use and access of information assets . Therefore in this article focusing the policies , guidelines and standards for the prevention technique of SoE attacking risk in the domain of information security [4].

In the global context for IS and the SoE attacking risk factors of threat to information security , it is clear that many business processes do not work without reliable IT systems confidentiality and thus integrity and availability of information are of high importance in today's business life[10] . The complexity of security administration in managing large networks is , now a days , a big issue . Owing to factors such as globalization and reason of regulatory nature, organization's are now more serious about SoE attacks . International companies seeking to outsource their work and insist on security assurance/ security certification. They insist on adherence to laws , standards and business practices prevalent in their respective countries. Not surprisingly , the top software services companies , IT enabled services companies and BPO out sits are going in for security certification such as BS 7799 or ISO 17799. Thus , regulatory requirements become one more derive for increased security awareness .

Acknowledgments

Thanks to University Malaysia Kelantan, as done the survey for collecting data.

References

[1] Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237-248.

[2] Algarni, A., Xue, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. European Journal of Information Systems 26(6), 661-687.

[3] Applegate, S.D. (2009). Social Engineering: Hacking the Wetware! Information Security Journal: A Global Perspective, 18(1), 40-46.

[4] Brill,A., Pollit, M., & Whitcomb, C. M. (2006). The Evolution of Computer Forensic Best Practices: An Update on Programs and Publications. Journal of Digital Forensic Practice, 1(1), 3-11.

[5] Brotby, W. K. & Hinson, G. (2013). PRAGMATIC Security Metrics: ApplyingMetametrics to Information Security .CRC Press.

[6] Buskirk, E.V. & Liu, V.T. (2006). Digital Evidence: Challenging the Presumption of Reliability. Journal of Digital Forensic Practice, 1(1), 19-26.

[7] Cheung, S. K. S. (2005). Information Security Management for Higher Education Institutions. Intelligent Data analysis and its Applications, 1(2-3), 55-68.

[8] Mohamed, N., Nawawi, A., Ismail, I. S., Ahmad., S.A., Azmi, N.A. & Zakaria, N.B. (2013). Cyber fraud challenges and the analysts competency: Evidence from digital forensic department of Cyber Security Malaysia. Recent Trends in Social and Behaviour Sciences - Proceedings of the 2nd International Congress on Interdisciplinary Behavior and Social Sciences, 581-583.

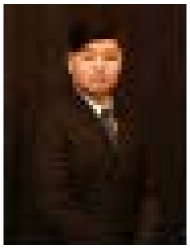
[9] Molok, N.N.A., Ahmad, A. & Chang, S. (2018). A case analysis of securing organisations against information leakage through online social networking. International Journal of Information Management, 43(4), 351-356.

[10] Myyry,L.,Siponen,M.,Pahnila,S.&Vartiainen, (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems, 18(2), 126-139.

Shekh Abdullah-Al-Musa Ahmed, currently studying as a PhD Research Fellow (with International ZAMALLAH Scholarship) at Faculty of Creative Technology and Heritage in University Malaysia Kelantan (UMK) . His main supervisor is Ts. Dr. Nik Zulkarnaen Khidzir and co-supervior is Dr. Tan, Tse Guan . He received the Bachelor of (Hons)

In Computing from UCSI U , Malaysia and Master of Engineering In information System Security from Bangladesh University of Professionals (BUP).

Nik Zulkarnaen Khidzir, Certified Professional Technologist (Malaysia Board of Technologist); Senior Lecturer Faculty of Creative Technology and Heritage ; Currently appointed as Research fellow and Head of Division at Global Entrepreneurship Research and Innovation Centre (GERIC), UMK, Universiti Malaysia Kelantan has been involved in ICT industry and academia for the past 18 years. He graduated in Computer Science Degree and Diploma Specialize in Software Engineering. Master's degree specialized in Information Privacy and ICT Strategic Planning. His PhD in Information Security Risk Management provide him a skill for research and consultation works. His research interests are Advanced Method for Educational Technology, Multimedia and Visual Communication Interaction in Islamic Perspectives, Software Engineering, Cybersecurity Risks, Information Security Risk Management, Business and Education Computing/e-commerce and Creative Computing and Multimedia related project. He also obtained several formal entrepreneurship education and qualification such Profesional Certificate Entrepreneurship Leader, Swanseas University UK; Postgraduate Diploma in Entrepreneurship Educators, Executive Certificate in Business Management and Entrepreneurship, UUM; and Certified Entrepreneurship Coach, UMK/GERIC. Throughout his years of experiences in industry, he also involved in telecommunications, digital Multimedia content development, and System Integrator and ICT solution provider as System Analyst, Database Administrator, Certified Software Tester, Software Designer, Assistant Project Manager (ICT-related project). Also involved in research and consultation as well as training program development for academia and industry. He actively involved in organizing local and international conferences. Also become as proceeding conference and journal reviewer local and international. Pertaining his research interest and contribution to the body of knowledge, he has published several articles in indexed proceedings and high impact journals. He is a member of the IACSIT, IEEE and PECAMP. He received various recognition and awards in research and innovation competition at national and international level.



Tan Tse Guan is currently a senior lecturer in Creative Technology at the Faculty of Creative Technology and Heritage at Universiti Malaysia Kelantan, Malaysia. He received the Bachelor of Computer Science (Hons) in Software Engineering, the Master of Science in Artificial Intelligence and the Doctor of Philosophy in Computer Science from Universiti Malaysia Sabah, Malaysia, in 2006, 2008 and 2013, respectively. His research interests include Creative Technology, Artificial Neural Networks, Coevolutionary Computing, Evolutionary Computing, Game Artificial Intelligence and Multiobjective Optimization.