ISSN: 2661-3719(Print); 2661-3727(Online)

透过多维社会技术来评估信息世界的安全性能

卡卡里·休斯、胡珀·鲁斯、托马斯·杨、谢丽尔·斯图尔特、蒂亚拉埃洛夫
University of Science and Security, Bibra Lake, NT 0384, Australia

摘　要：衡量信息安全绩效是各大企业中信息安全管理系统的重要组成部分。过去的研究主要集中在建立定性测量方法上。由于这些可能导致模棱两可的结论，因此出现越来越多让定量指标作为替代方案的建议。然而，关于定量方法的文献仍然很少。因此，对信息安全绩效评估的研究具有挑战性，特别是因为许多方法尚未在组织环境中进行测试。本文通过多维社会技术方法来验证中型企业的真实环境中，信息安全管理系统的性能评估。结果表明，信息安全具有战略定义和合规性，但措施主要在技术和运营层面实施，其战略管理仍不发达。我们发现最大的问题与信息资源和风险管理有关，其中与信息安全测量相关的活动被证实是关键问题之一。虽然企业确实具备一定的信息安全性能，并且意识到信息安全的重要性，但他们目前的做法仍难以跟上技术与安全趋势的快节奏。
关键词：信息安全、网络安全、网路漏洞、企业反应、安全意识

A real-world information security performance assessment using a multidimensional socio-technical approach

Carcary Hughes, Hooper Ruth, Thomas Young, Cheryl Stewart, Tiara Eloff
University of Science and Security, Bibra Lake, NT 0384, Australia

Abstract　Measuring the performance of information security is an essential part of the information security management system within organisations. Studies in the past mainly focused on establishing qualitative measurement approaches. Since these can lead to ambiguous conclusions, quantitative metrics are being increasingly proposed as a useful alternative. Nevertheless, the literature on quantitative approaches remains scarce. Thus, studies on the evaluation of information security performance are challenging, especially since many approaches are not tested in organisational settings. The paper aims to validate the model used for evaluating the performance of information security management system through a multidimensional socio-technical approach, in a real-world settings among medium-sized enterprises. The results indicate that information security is strategically defined and compliant, however, measures are primarily implemented at technical and operational levels, while its strategic management remains underdeveloped. We found that the biggest issues are related to information resources and risk management, where information security measurement-related activities proved to be particularly problematic. Even though enterprises do possess certain information security capabilities and are aware of the importance of information security, their current practices make it difficult for them to keep up with the fast-paced technological and security trends.
Keywords: Information security, cyber security, breaches, business response, security awareness

引言

(ISMS)

(ISM)

ISM　　ISMS　　ISMS

/

(ISec)　　ISMS　　ISec

ISec　　ISec

ISMS (90%) (86%)
(85%)
50%) .
(67%) (67%) (67%)
(56%)
ISec (SME) ISec

二、优先考虑或降低网络安全的原因

37% —— 2016
(29%)
12

29%
22%
ISec

三、网络安全漏洞

(72%)
(33%) (27%)
(17%)

ISP 10×10M

一、网络安全的重要性

(74%)
(31%) (43%) 2016
cber

6%

—— ——

2016
11%
24%
45%
200
69% 49%

(98%)

(28%)

(20%)

(15%) (6%)

(26%)

(13%)

四、信息安全意识评估

“ ”

——

五、讨论

Posthumus VonSolms (2004)

——

——

5 7

(Belton and Stewart) (2002)

结论

ISP 10×10M

ISec

ISec

ISM ISec

ISec

ISec

(1)

- ; (2)

(3)

(4)

(5)

(6)

ISec

ISec

参考文献

1. Hansche S. Designing a security awareness program: Part 1, in-formation. Systems Security January/February 2001:14–22.

2. MartinsA, Eloff JHP.Measuringinformationsecurity, <http://philby.ucsd.edu/wcse291_IDVA/papers/rating-position/Martins.pdf>;2001 [accessed August 2004].

3. Stanton JM, Stam KR, Mastrangelo P, Jolton J. Analysis of end usersecurity behaviours. Computers and Security 2005; 24 (2):124–33.

4. Vargas LG, Dougherty JJ. The analytic hierarchy process andmulticriterion decision making. American Journal of Mathe-matical and Management Sciences 1982; 19 (1):59–92.

5. McKissak J, Hooper V, Hope B. An Organisational Model for Information Security Assessment. In:Brown I, editor. PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON INFORMATIONMANAGEMENT AND EVALUATION. Cape Town: Academic Publishing; 2010. pp. 218–227.

6. Patel SC, Graham JH, Ralston PAS. Quantitatively assessing the vulnerability of critical informationsystems: A new method for evaluating security enhancements. Int J Inf Manage. 2008; 28: 483–491.

7. Cokins G. Performance Management: Finding the Missing Pieces (to Close the Intelligence Gap).Hoboken: Wiley; 2004.

8. Ribas CE, Burattini MN, Massad E, Yamamoto JF. Information Security Management System: A CaseStudy in a Brazilian Healthcare Organization. Proceedings of the International Conference on HealthInformatics (HEALTHINF-2012). Algarve: Science and Technology Publications; 2012. pp. 147–151.

9. Rhee HS, Ryu YU, Kim CT. Unrealistic optimism on information security management. Comput Secur.2012; 31: 221–232.

10. European Union Agency for Cybersecurity [ENISA]. ENISA Threat Landscape Report 2017. 2018.