IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 22, Issue 3, Ser. II (May - June 2020), PP 50-54
www.iosrjournals.org

The Evolution of Information Security Measurement and Testing

Omoyiola, BayoOlushola
School of Information Systems and Technology, Walden University,Minneapolis, Minnesota, USA

Abstract
Information security has evolved over the years and has become increasingly important to society at large. Similarly, information security measurement and testing have evolved over the years,from the days of BS 7799 to the present day ISO 27001 and others.The measurement and testing techniques have been incredibly beneficial to the world of today. Though it has its limitations, there are opportunities for improvement and future research and development. This paperexplores these themes, highlighting the evolution of information security measurement and testing, the current trends, the benefits and the challenges, gaps, opportunities for improvement, and future research and development. With thesethemes, the discussion examines the evolution ofinformation security measurement and testing.

Keywords:*Information security, Measurement, Testing, Metrics, Management, and Risk*

Date of Submission: 13-12-2019 Date of Acceptance: 17-12-2019

I. Introduction

The field of Information security has grown over the years. It has become increasingly important and significant in the world of today because the governments of federations, institutions, and organizations now see the need to protect their valuable assets and data and mitigate security risks to the barest minimum. Information security leaders of today do brief the executive management regularly and are also now part of the executive management team. These improvements and changes have made it possible for the information security leaders to develop precise objective inputs and to build decisions concerning risk management on scientific and accurate data. Another factor that led to the evolution of security measurement and testing was the fact thatsecurity became a major issue globally, and the need arose for the effective management of security challenges andreduction ofthe security risks in the world (Omoyiola, 2018).The Information security function now uses known practices such as Plan-Do-Check-Act to plan and implement and also check and act to validate the efficiency of controls. The information security department is now mature, and it receives regular support and guidance from top management. Information security is now measurable because it is managed and backed up by finance and regulation. This measurement aids organizational' decision making enhances performance, and increases accountability on IT system security. It helps to evaluate organizational information security performance based on its performance goals. It also helps to track implemented controls for improvement and measures the efficiency of those controls (Tashi, &Ghernaouti-hélie, 2007). With that kind of system in place, measurement creates data, data gives information, which provides knowledge, and knowledge imparts wisdom, which is the practical application of them all. Information security measurement also involves security assessment, security testing, and security audits (internal, external, and third-party). It requires vulnerability assessment, penetration testing (Salas & Martin, 2014). It also covers log reviews, synthetic transactions, code review, and testing, test coverage analysis, interface testing, account management, critical performance and risk indicators, management review and approval, backup verification data, analysis of test output and generation of results (Chapple, Stewart, & Gibson, 2015; Goseva-Popstojanova, Anastasovski, Dimitrijevikj, Pantev& Miller, 2014; Stolfo, Bellovin, & Evans, 2011). Security measurement also includes risk management and measures such as qualitative and quantitative measurements of security (Ahmad, Sahid&Azuwa, 2014; Arora, Hall, Piato, Ramsey, &Telang, 2004; Atyam, 2010; Barabanov, Kowalski, &Yngström, 2011; Dubrisky, 2016). It also covers threat classification (Jouini, Rabai, &Aissa, 2014). It also includes securitymetric dimensions in terms of performance, technical control, compliance, operations, organization information security, information security management, productivity (e.g. return on investment), efficiency, effectiveness, cycle time, user satisfaction and Security Education Training and Awareness (Da Veiga& Martins, 2017; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; Montesdioca&Macada, 2015; Sen &Borle, 2015).

II. Evolution Phases

Information security measurement and testing have evolved over the years, and several standards and frameworks are now in existence. Several researchers have also published it. It all started with the old standards

before the new ones got formed. Some of the old ones do not exist anymore, while the new ones remain. The discussion on the evolution of the frameworks and the research trends are below:

2.1 BS 7799 to ISO 17799 to ISO 27001, and BS 7799-2 to ISO 27002

BS 7799, a standard on information security management systems, was published in 1995 by British Standard Group (BSI). It was later replaced by ISO 17799 after it got adopted by International Organization for Standardization (ISO) and International Electro-technical Committee (IEC) in year 200. Then it was later incorporated into the ISO 27001 framework Borabanov, Kowalski, &Yngström, 2011; ISO/IEC, 2005; Tashi, &Ghernaouti-hélie, 2007). There are other revised versions of BS 7799 because it got revised and updated several times after the ones adopted by ISO came out. BS 7799-2, which is part 2 of BS 7799-1, has also gotten replaced by ISO 27002, the Code of Practice for Information Security Controls (ISO, 2005).

2.2. NIST SP 800-80 to NIST SP-800-55, and NIST SP-800-26 to NIST SP-800-53

NIST SP 800-80, a special publication and guide for developing Performance Metrics for Information Security got published in May 2006 (NIST, 2006). It got withdrawn on November 1, 2008. It was superseded by NIST SP 800-55 Rev 1, which is a unique publication on Performance Measurement Guide for Information Security, which got published in July 2008 (NIST, 2008). There have been other revised versions of NIST SP 800-55 because it has gotten revised and updated sometimes after that publication came out. NIST SP-800-26, a security self-assessment guide for the Information Technology system got published in November 2001. It got withdrawn in December 2007 (NIST, 2001). It was superseded by NIST SP 800-53A, which is a unique publication on security and privacy assessment, which got published in July 2008 (NIST, 2008). There have been other revised versions of NIST SP 800-53A because it got revised and updated sometimes after that publication came out (US Department of Commerce, 2013).

III. Trends of research on information security measurement

Many researchers have conducted research studies on information security measures. As far back as 2003, Dan Geer, Andrew Jaquith, and Kevin Soo Hoo started by laying out a good foundation for people to understand security threats, risks, and cost and how to track progress by addressing them. Later in 2007, Gunnar Peterson and Elizabeth Nichols explained metrics that could measure the security impact that process changes in a particular life-cycle can have on the other phase. They worked on design-time metrics, runtime metrics, deployment time metrics, monitoring of systems availability, reliability and maintainability, and improvement in runtime measurement (Pfleeger, 2012). In 2008, Dan and Julie Ryan conducted a study on security and privacy and how non-effective risk measures could be replaced with helpful one; and measurement of the impact of investment in information security by monitoring of changes in an expected loss. In 2010, Ron Cunningham and Pfleeger released a report on nine compelling reasons why security measurement is hard. Later, David Evans, Steve Bellovin, and Sal Stolfo published an article with a warning for replacement of anecdote-driven security decision making with foundational science, systematic and generalized knowledge, developed universal principles for predictions, and a set of methodologies for testing hypotheses. The foundational science had to do with a measurement that is reliable (Pfleeger, 2012). George Cybenko and Carl Landwehr in 2012 conducted a study on why security progress needs to be measured. Cybenko explained that development in operational cybersecurity is hard to showcase. While Landwehr wrote on the need to improve sound measures of the state of cybersecurity at a national and international scale, and the need for the measurements to be conducted by an unbiased organization because of progress. They explained the mistakes of the past years and how the illegal use of game theory could be misleading. The authors also wrote on lessons learned from a gradual increase in risk perception and the oscillating nature of these data types (Pfleeger, 2012).

IV. Current trends and framework

The current trends and framework of security measurement and testing include but not limited to the Security Performance Measurement framework (NIST SP 800-55), Security and Privacy Assessment (NIST SP 800-53), Risk Management Framework (NIST SP 800-37). Risk Management Guide (NIST SP 800-30), Information Security Continuous Monitoring (NIST SP 800-137), Information Security Management System with PDCA (ISO 27001),Security audit, vulnerability assessment, measurement of SETA (security education training and awareness), Qualitative research and quantitative research such as technical analysis and testing of information systems, mathematical models or statistical computations of risks (E.g. risk analysis), survey, and Economic analysis of investment justification (e.g.Return on Investment analysis), and Security Content Automation Protocol like CVSS, CVE, CWE, OVAL, OCIL, CABEC, CPE, CCE and XCCDF (Jansen, 2009; Montesino&Fenz, 2011). There are also frameworks like ITIL (Information Technology Infrastructure Library), OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), COBIT (Control Objectives for

Information and Related Technology) are used for information security and related risk measurements. Another current trend is that NIST SP 800-53 is usually used with NIST SP 800-37 by organizations. Organizations combine security and privacy assessment with risk management to give a complete package. Combining multiple ISO 27000 standards can also create and maintain a holistic and more robust information security program and framework (Commiato, 2018).

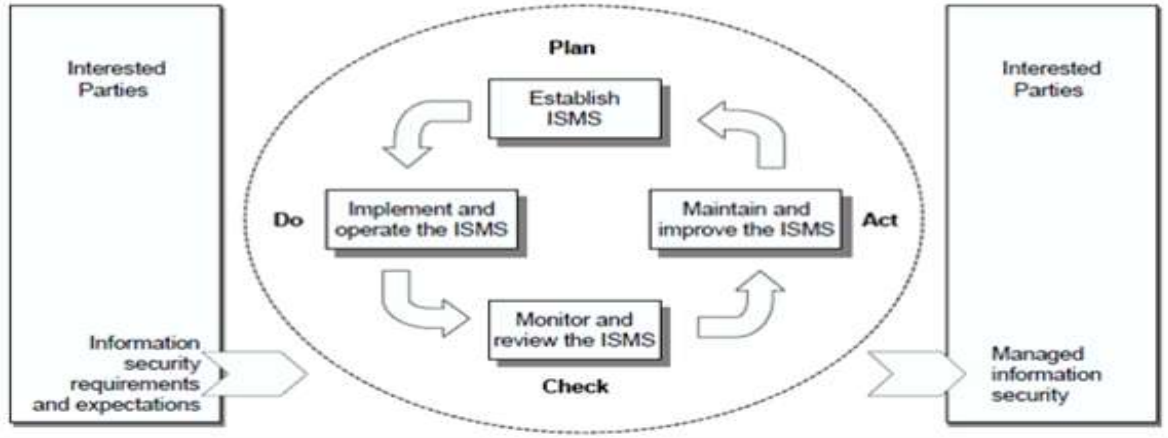

Fig. 1 - ISO 27001 with PDCA

V. Security measurement Models

There are also security measurement models. These models include a balanced scorecard, PDCA model, and four disciplines model.

5.1 Balanced Scorecard

The balanced scorecard is used to measure performance. Hence it is used to measure information security. The information security (IS) metrics get classified according to the balanced scorecard taxonomy, which is Financial, Customer, Internal Business Process, and Learning and Growth (Jacquith, 2010). See the PowerPoint slide for the diagram. The COBIT by ISACA supports the balanced scorecard. Microsoft also supports it (Barabanov et al., 2011). The balanced scorecard enhances planning and management with its planning and management system that aligns organizational strategy with its operations, and to drive the reporting and measurement of performance against strategic goals and objectives. It gets used for high-level classification and examination and a means of communication of results (Barabanov et al., 2011; Microsoft, 2007). A balanced scorecard can be used to measure the performance of security programs such as security education training and awareness, access control, vulnerability assessment, compliance, and business continuity (Microsoft, 2007).

5.2 PDCA model

The PCDA model with Plan, Do, Check, and Act phases,is incorporated into the ISO 270001 standard. See Figure 1 above. At the Plan phase, the objectives and controls get selected, and the information security policy and objectives get established for the management of risk and improvement of the level of risk exposure (Barabanav et al., 2011; Pelaez, 2010). At the do phase, the security controls get implemented for the ISMS in line with the laid down policies and objectives. How to measure security controls are also defined. At the Check phase, process control and performance are check and measured against a set of guidelines (Barabanav et al., 2011; Pelaez, 2010). At the Act phase, preventive and corrective actions are taken based on verification results for the implementation of the continuous improvement of the ISMS. Improvements do get implemented at this phase (Barabanav et al., 2011; Pelaez, 2010).

5,3. Four disciplines model

Apart from the Balance scorecard and the PDCA, there is also the four disciplines model which comprises of Vulnerability management, Identity management, Trust management, and Threat management. At the Vulnerability management phase, the systems get hardened; the firewalls get configured, and the patch management and vulnerabilities get identified. At the Identity management phase, the users get managed; there are provisions and management of account, and there are authentication and authorization of access, and sessions get validated at this point. At the Trust management phase, the security policies and processes get

designed; the procedures are created and modified here, and the controls are also designed and implemented at this phase. At the Threat management phase, events and activities get monitored; a forensic audit gets conducted, and incidents are corrected and managed at this phase (Lindstrom, 2004).

VI. Benefits and Social implications

Information security measurement and testing have several advantages and social consequences.See Figure 2 below.It helps inthe evaluation of information security performance; and for tracking of implemented controls for improvement (Pelaez, 2010; You, Cho, & Lee, 2016). Italso helps to measure the efficiency of controls; also helps in improving accountability to stakeholders; ensuring an appropriate level of support; demonstration of compliance with regulations; enhancing Intelligent and proactive risk management; facilitating decision making, gives competitive advantage, making a business impact; aligning with business goals; and promoting accountability through collection, analysis, and reporting of relevant performance data (Barabanav et al., 2011; Commiato, 2018; Goode, Levy, Hovav & Smith, 2018).

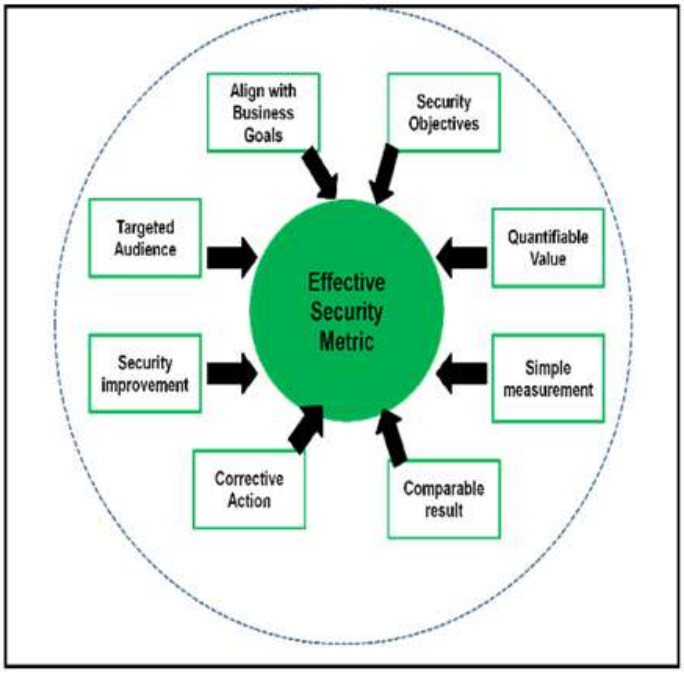

Fig. 2 - Benefits of a security Metric

VII. Limitations and future research

There are limiting challenges, such as the need for more advanced statistical techniques (Pfleeger, 2012). Another is the need for a more advanced risk-based Information Security measurement framework (Arora, Hall, Piato, Ramsey, &Telang, 2004). Other limitations may include time, cost, insufficient top management buy-in, inadequate change management, and when there is a lack of continuous improvement (Commiato, 2018). There is also the human aspect that requires security awareness solutions because the evolution of security technology, its usage, measurement, and testing, alsohas direct overlap with the human side of information security (Furnell& Clarke, 2012). The possibilities and future research include the fact that the measure can get applied to the infrastructure of nations (Grohmann, 2018). Future studies also include research on attack surface and attack graph-based metrics, translation of lower-layer parameters into higher-layer ones, appropriateness of specific data formats, units, and types of measure for particular targets of measurement, alignment of security controls with objectives, capabilities, and the environment (Commiato, 2018).).

References

[1]. Ahmad, R., Sahid, S., &Azuwa, M.P. (2014). Effective Measurement Requirements for Network Security Management.*International Journal of Computer Science and InformationSecurity*, 12(4), 37-44.

[2]. Arora, A., Hall, D., Piato, C. A., Ramsey, D., &Telang, R. (2004). Measuring the risk-based value of IT security solutions. *IT Professional*, 6(6), 35–42. doi:10.1109/MITP.2004.89.

[3]. Atyam, S. B. (2010). Effectiveness of security control risk assessments for enterprises: Assess on the business perspective of security risks. *Information Security Journal*, 19(6), 343–350. doi:10.1080/19393555.2010.514892.

[4]. Barabanov, R., Kowalski, S., &Yngström, L. (2011). Information security metrics: Research directions. 2011 *2nd European Security Conference* (pp.1-16), Örebro, Sweden, June 13-14, 2011.

[5]. Chapple, M., Stewart, J.M., & Gibson, D. (2015). *Certified information system security professional (8th ed.).* Indianapolis, Indiana: Sybex.

[6]. Commiato, A., & Sturgill, M. (2018). Information security standards: Differences, benefits, impacts, and evolution. *ISSA Journal*,16(7), 25–30.

[7]. Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, 70, 72-94. doi:10.1016/j.cose.2017.05.002

[8]. Dubsky, L. (2016). Assessing security controls: Keystone of the risk management framework. *ISACA Journal*, 6, 29 – 32.

[9]. Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, 31(8), 983–988. doi:10.1016/j.cose.2012.08.004

[10]. Goode, J., Levy, Y., Hovav, A., & Smith, J. (2018). Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness. *Online Journal of Applied Knowledge Management*, 6(1), 67–80.

[11]. Goseva-Popstojanova, K., Anastasovski, G., Dimitrijevikj, A., Pantev, R., & Miller, B. (2014). Characterization and classification of malicious Web traffic. *Computers & Security*, 42, 92-115. doi:10.1016/j.cose.2014.01.006

[12]. Grohmann A. (2018). Evolution of the cybersecurity framework. *ISSA Journal*, 16(7), 25–30

[13]. ISO/IEC (2005). ISO/IEC 2700:2005. Geneva, Switzerland: International Standard Organization.

[14]. ISO (2005). ISO/IEC 27002:2005. Retrieved from https://www.iso.org/standard/50297.html

[15]. Jacquith, A. (2010). Creating meaningful information security metrics. Retrieved from: https://searchsecurity.techtarget.com/magazineContent/Creating-meaningful-information-security-metrics

[16]. Jansen, W. (2009). Directions in security metrics research. NIST Internal Report, 7564, 1-21. doi:10.6028/NIST.IR.7564

[17]. Jouini, M., Rabai, A., &Aissa, B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, 32, 489-496. doi:10.1016/j.jprocs.2014.05.452

[18]. Lindstrom P. (2004). Security measures and metrics. Retrieved from: http://spiresecurity.com/poster/Spire%20Poster%20-%20Four%20Disciplines.pdf

[19]. Microsoft (2007). Balanced scorecard for information security: Introduction. Microsoft Corporation. Available at http://technet.microsoft.com/en-us/library/bb821240.aspx

[20]. Montesdioca, G.P.Z. &Macada A.C.G. (2015). Measuring user satisfaction with information security practices. *Computers & Security*. 48, 267-280. doi:10.1016/j.cose.2014.10.015

[21]. Montesino, R. &Fenz, S. (2011). Information security automation: How far can we go? *Availability, Reliability, and Security (ARES), 2011 Sixth International Conference on Availability, Reliability, andSecurity* (pp.280-285), Vienna, Austria, August 22-26, 2011, IEEE. doi:10.1109/ARES.2011.48.

[22]. NIST (2001). Security self-assessment guide for information technology systems. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-26/archive/2001-11-01

[23]. NIST (2006). Guide for developing performance metrics for information security. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-80/archive/2006-05-04

[24]. NIST (2008). Guide for assessing the security controls in federal information systems and organizations: Building effective security assessment plans. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53a/archive/2008-07-01.

[25]. NIST (2008). Performance measurement guide for information security. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-55/rev-1/final.

[26]. Omoyiola, B. O (2018). Overview of biometric and facial recognition techniques. *IOSR Journal of Computer Engineering(IOSR-JCE*). 20 (4), 1-5.doi: 10.9790/0661-2004010105

[27]. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176. doi:10.1016/j.cose.2013.12.003.

[28]. Pelaez, M.H.S. (2010). Measuring effectiveness in information security controls. *SANS Institute*. Retrieved from: https://www.sans.org/reading-room/whitepapers/basics/paper/33398.

[29]. Pfleeger, S. L. (2012). Security measurement steps, missteps, and next steps. *IEEE Security & Privacy*, 10(4), 5–9. doi:10.1109/MSP.2012.106.

[30]. Salas, M.I.P. & Martins, E. (2014) Security testing methodology for vulnerabilities detection of xss in web services and ws-security. *Electronic Notes in Theoretical Computer Science*, 302, 133-154. doi: 10.1016/j.entcs.2014.01.024.

[31]. Sen, R., &Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, 32(2), 314-341. doi:10.1080/07421222.2015.1063315.

[32]. Stolfo, S., Bellovin, S. M., & Evans, D. (2011). Measuring security. *IEEE Security & Privacy*, 9(3), 60–65. doi:10.1109/MSP.2011.56.

[33]. Tashi, I., &Ghernaouti-hélie, S. (2007). Security metrics to improve information security management. 2007 *6th Annual Security Conference* (pp.4701- 4712), Las Vegas, NV, April 11-12, 2007.

[34]. US Department of Commerce (2013). Security and privacy controls for federal information systems and organizations. *NIST Special Bulletin* (800-53), 4, 1-462. doi: 10.6028/NIST.SP.800-53r4.

[35]. You, Y., Cho, I., & Lee, K. (2016). An advanced approach to security measurement system. *Journal of Supercomputing*, 72(9), 3443-3454. doi: 10.1007/s11227-015-1585-7.