Security Metrics for e-Healthcare Information Systems: A Domain Specific Metrics Approach

Said Jafari, Fredrick Mtenzi, Ronan Fitzpatrick, Brendan O'Shea
School of Computing, Dublin Institute of Technology, Ireland

Abstract

Information sharing among different healthcare organizations is critical for efficient and cost effective healthcare service delivery. Healthcare organisations with information systems need to be interconnected to ensure information exchange. Interconnectivity increases exposure to risk of damage, loss and fraud. Security and privacy of patients' information are concerns of all healthcare organizations. These concerns hinder the willingness to share data across different organizations. An objective assessment of organisational security posture is required in order to build trust and confidence among different entities in the e-Healthcare ecosystem. Security metrics are a collection of several measurements taken at different points in time, compared against baseline and interpreted to reveal an understanding. Metrics provides insight, improve visibility and accountability, and can reveal the overall security posture of organisation. The current security assessment practices focus either on measuring security programme effectiveness, auditing or assessment of individual information systems components like networks and software. There are discrepancies in the way security is given meaning and quantified in several other approaches. These discrepancies affect their adoption as programmes to derive trustworthy measurable results. Several security assessment practices not sufficiently address measuring the overall security posture of an organization. For those that do, their assessment results are not meaningfully comparable among different organisations. In this paper we present an analysis of selected approaches, identifying their bias, and propose an approach for developing security metrics to be used for assessing security posture of healthcare organizations. The metrics for this approach shall not be tailored to any specific organisation to ensure comparable results.

1. Introduction

The healthcare domain is characterized as being heterogeneous, composed of isolated information systems (IS) that keep patients' information[1]. Despite this setting, patients are continually changing their healthcare providers in their lifetime for various reasons. Thus duplicate and different pieces of information of a single patient resides in different healthcare systems localized in autonomous healthcare organizations [2]. This prevailing situation leads to inefficiency and high cost of healthcare service delivery [2]. To overcome this problem, different healthcare organizations should be able to share patients' information among themselves.

Security and privacy of patients' information are concerns of all healthcare organisations. These concerns do not only hamper the adoption of e-healthcare deployment but also the desire to interconnect isolated e-healthcare systems belonging to different organisations. However, the later case increases exposure to risks of damage, loss and fraud [3]. Intuitively, if organisation A is said to have certain security posture, and organisation B is said to posses a certain security posture different from A, connecting A and B will result into a more vulnerable system than the individual systems. To ensure the interconnected systems results into a moderate secure environment, it is important to assess the security of each organization systemically to reveal the overall security posture.

Security metrics are collections of several measurements taken at different points in time, compared against baseline and interpreted to reveal an understanding [4]. They provide insight, improve visibility and accountability [5, 6], and can reveal the overall security posture of an organisation. The current security assessment practices focuses either on measuring security programme effectiveness (e.g. using National Institute of Standard and Technology (NIST) metrics approach); auditing (e.g. using ISO/IEC 27002:2005); or measuring specific IS components like networks (e.g. using vulnerability scanning, intrusion detection) and software (e.g. using defects counts, complexity measure, attack surfaces) [7-11]. These assessment practices suffer from the following: their metrics are associated with organizational security programme; therefore its results can't be meaningfully comparable across different organizations. Also, auditing does not

provide objective assessment results to be comparable, and the performance measurements of individual IS components like networks or software does not depict the overall security posture of an organization. These discrepancies affect their adoption as programmes to derive trustworthy measurable results. For the interconnected systems to be able to talk to one another without worsening security of the overall ecosystem, each entity security posture should be established with trustworthy and meaningful security indicators in order to bring visibility and build confidence among participating entities. As Schneier [12] stated "*security is like a chain"* therefore "*it is only as strong as the weakest link"*.

In this paper we present an analysis of selected approaches, identifying their bias, and present an approach for developing security metrics for e-healthcare organisations. The metrics from this approach shall be domain specific but generic in nature in that it is not tailored to any specific organizational security programme in order to facilitate its adoption and the comparison of metrics results. The approach is geared to articulate and visualize healthcare specific security concerns to enable stakeholders in this field to grasp an understanding of the security of their systems. The aim is to foster confidence in sharing sensitive patients' information. The rest of the paper is organized into the following manner. Section 2 presents definitions of terminologies used. Section 3 highlights related issues in e-healthcare information security and security assessment and measurement in general. Section 4 presents current approaches of measuring security for the overall organization. Section 5 provides a comparative analysis of selected approaches for a chosen set of properties. Section 6 describes the proposed metrics development approach for healthcare organizations. Section 7 finalizes with the conclusion and further work.

2. Terminologies

In this section, terminologies relating to security and security metrics are described. A classical definition of security requires maintaining three attributes; confidentiality, integrity and availability. In some recent studies, authenticity, accountability and non-repudiation attributes are also considered [8]. These security attributes are further elaborated:

- Confidentiality: "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"[13].
- Integrity : "Guarding against improper information modification or destruction…"[13].
- Availability: "Ensuring timely and reliable access to and use of information…" [13].
- Authenticity: "Verifying the identity of a user, process or device, prerequisite to allowing access to resources…" [14].
- Non-repudiation is defined as ensuring no false denial of an entity of having participated in all or part of a communication [15].

Other terminologies used in this paper are as follows:

- Safeguards: "Protective measures prescribed to meet the security requirements ..., s*ynonymous with countermeasures*" [14].

In relation to security assessment, the following definitions hold:

- Security posture: "the actual state of a system, entity, or process regarding security, that is, what the system security assessment aims to describe, …" [16].
- Security metrics: "are numbers computed to facilitate decision making .., obtained through collection, analysis, and reporting of relevant performance-related data..." [17].

To elaborate further, security posture is not a static value; it is dynamic and can be meaningfully stated with time interval. Security metrics has to incorporate time aspect to be meaningful. Also metrics as "numbers" refers to the collection of several measurements taken at different points in time, compared and interpreted to reveal a particular trend [4].

This section has illustrated terminologies as used in this paper. The following section highlights uniqueness of healthcare environment in relation to security concerns and discusses general security metrics from literature.

3. Related work

3.1. Security in healthcare information systems

Healthcare organisations are vulnerable to security attacks due to the fact that they contain sensitive patient information. The nature of work requires collaboration among multi-occupations communities (e.g., physicians, nurses, technicians, and administrative staff). These groups of professionals may have different understandings of security. In practice, healthcare professionals do operate in accordance to medical ethics. On the other hand protecting electronic information and their infrastructures requires persistence in obedience of security rules. In extreme cases, the urgency of work

may necessitate bypassing security rules. Ironically, without measurement, ensuring an organizational impression that perceive security with an appreciation and attentiveness that encourages persistent responsible behavior becomes difficult. This environment makes security and privacy issues more challenging to address [18].

New technologies like sensor networks for remote patient monitoring introduces other risks [19, 20]. A stringent protection is required for any organisation processing health information regardless of size, location, or mode of delivery [21].

3.2. The need for security metrics

Security is a relative phenomenon, difficult to be visualized and often involves trade-offs. *Decisions that involve trade-offs among constrained resources requires tools, techniques and measurement to assist in decision making*[22]. The motivation for seeking security metrics comes from different facets. From an economic perspective, organisations wants to know the return-on-investment; how much protection is gained per each additional investment?[23, 24]. Security metrics may provide insight to identify strength and anomalies or weakness in deployed safeguards[25]. This information could be used to enhance proper allocation of resources, planning for safer operating procedures, disaster and recovery planning[26]. Security metrics provides a yardstick through which organisations can compare with one another upon established baseline. This increases confidence and trust for users. *Measurement is the way by which humans understand with more precision the rational world* [27].

3.3. Security assessment and metrics

As far as we are aware, there are no security metrics publicly available for assessing security posture of healthcare organizations. A few security metrics for overall security assessment not tailored to any specific domain have been found. Weiss et al [28] proposed security metrics that build on a risk management approach. In the study, security is quantified and measured in terms of incidents as a result of asset loss by organization in a defined time interval. Total security is reached if nothing is lost. In comparison, an organization is considered more secure than the other if it possesses the same set of assets but lost less than a competitor. It is also regarded as more secure if it possesses more assets but has lost the same. The metric has a number of limitations; among them is a notation of security and selection of security performance indicator. There is vague relationship between security incidents counts and assets loss expressed in monetary value. The indicator S for security of an organization is given by the formula:

$S =$ 100% - [percentage of lost asset] [28].

Lucky of not being attacked may play its part. The countermeasures may not have the capability to know that you have been attacked. Also security is multidimensional [12], its overall measurements results cannot meaningfully be aggregated into a single value. The proposed security equation by itself does not tell much about security, but could be used to supplement other security metrics results.

The approach described in [29] proposed a security programme maturity model using ISO/IEC 17799 standard, a predecessor of ISO/IEC 27002, by incorporating separately the notion of existence and quality. It defines security posture as an improvement to the maturity model which essentially modify maturity model based on the quality of implementation of each element. Existence of quality factor in the programme is an attempt to alter security assessment from existence to effectiveness of the process. The proposed programme permits the adoption of security standard with little or no customization. This is generally useful in ensuring uniform deployment of controls and generally can improve the process of auditing. It suffers from ensuring the reproducible assessment results due to lack of formula in reaching the results.

Table 1. Sample of quality measure the from security maturity model

Programme maturity element	If maturity element is implemented, then ..		
	Low-quality threshold	Medium-quality threshold	High-quality threshold
Information asset classification, labeling and handling procedures developed	Procedures developed but not implemented	Assets partially classified	Pervasive classification throughout the entire organization

(Source: [30])

Other assessment approaches are based on best practices. The standard ISO/IEC 27002 [8], contains eleven security controls with a total of 39 security categories. The recommended controls are to be implemented based on requirements identified from a risk assessment. The standard is intended to ensure uniform security management practices and help build confidence in inter-organizational activities. As extended to healthcare, BS EN ISO 27799 [21] standard provides general guidance for

implementation of ISO/IEC 27002 in healthcare domain. This standard specifies a set of detailed controls for managing health information security and provides a minimum requisite level of security appropriate for each individual healthcare organisation. Both standards contain guidelines for security controls for organizations to adopt. These guidelines are presented in generic-technology-neutral fashion. They lack interpretation details of the suggested controls, put much focus on requirement enumeration and no account on measurement of its quality and applicability [25, 30]. It also becomes difficult to ensure reproducible objective results [25, 28].

In this section, metrics that measure the security posture of the entire organization are discussed. These metrics generally suffer in that they are not meaningful, objective and reproducible. The next section discusses the metric development approach recommended by NIST.

4. Security metrics development

Currently, security metrics for assessment of security posture of organizations are still definitional [31]. NIST SP 800-55 revision 1 standard [7], is the security metric standards available so far. NIST's metrics are tailored to specific security programme formulated and implemented by an organization. They should support security related decision making on proper allocation of resources, monitor and provide relevant performance trends of security enforcement. The type and granularity of metrics is dependant on the maturity of the security programme. These metrics essentially measure the effectiveness of the security programme of individual organizations. Its meaningfulness is dependant on how well the security programme was developed. To put in other words, it is necessary to assure the completeness of the security programme before delving into development of its metrics to avoid the bad side of metrics. Also if the metrics are for measuring programme effectiveness then there is a danger to inhibit metrics results comparison across different organizations. For meaningful comparison, the compared organisations must have the same security programmes of the same maturity level, it is difficult to guarantee these conditions. NIST's metrics are based of security performance goals and objectives, which may differ from one organization to another. Examples of NIST's metrics are shown in Table 2.

Table 2. Examples of NIST's metrics

Category	Metric
Vulnerability Management	%ge of high vulnerability mitigated within organizationally defined time periods after discovery.
	Number of high vulnerability mitigated across the enterprise during he time period.
Access Control	%ge of remote access points used to gain unauthorized access.
Awareness and Training	%ge of information system security personnel that have received security training.
Audit and Accountability	Average frequency of audit records review and analysis for inappropriate activity
Configuration Management	%ge approved and implemented configuration changes identified in the latest automated configuration
Identification and Authentication	%ge of users with access to share accounts
Incident Response	%ge of incidents reported within required time frame per applicable incident category
Physical and Environment	%ge of physical security incidents allowing unauthorized entry into facilities containing information systems

(Source: [7])

Herrmann [6], described security metrics as tools that eliminate guessing about the security and privacy posture of the organization. They promote visibility and accountability. Like the NIST approach, the existence of a security programme is assumed and the metrics assess programme effectiveness. Emphasis is made on ensuring clear definition of goals and objectives as well as pre-stated use of the metrics.

The NIST approach cannot provide generic metrics to be used across different organizations for comparison purposes. Another approach should be devised that could derive measurement results that are credible and comparable. In the next section, a comparative discussion on the selected three approaches is presented.

5. Discussion

Table 3 compares approaches discussed above in terms of philosophy or view on security, focus on measurement, degree of quantification and motivation as a means to depict a trend and gaps.

Authors do not assume any exhaustiveness of the worldwide approaches nor the properties chosen for comparison. A philosophy on security is considered in terms of how one interprets security. This has nothing to do with formal definitions of security of which a majority could agree on few of them, but tells how one visualizes, understands, and senses the presence or absence of security in the context of measurement or assessment. This is a primary concern to security measurement. The next property "focus" highlights the items considered for measurement, like process or product assessments. "Degree of quantification" property accounts for the extent to which the measurement results of a particular approach will be quantitative. The final property is "Motivation", and in this context refers to the rationale for approach and target audience or use.

The three approaches revisited on Table 3 enlighten at best four important properties. Firstly, there is an asymmetric visualization on the presence or absence of security on a particular target of evaluation. The second issue is inconsistency in internal implementation of measurement to arrive at security posture. This may affect credibility and hence acceptability of results. The third property shows that all of the examined approaches are comparatively quantitative. The fourth and final issue considered concerns the general motivation for use of that approach. These differences arguably build a case for tailoring a measurement approach to a specific domain in order to have common view. By enabling different entities in the e-Healthcare ecosystem to have a degree of confidence of the other entity security posture, trust could be gained to foster information sharing. In the next section, our novel approach is presented.

6. Proposed approach

Bishop pointed the need to define security based on the requirement of specific organisation [32]. Though for organizations of the same domain like healthcare organizations operating in a slightly similar environment can have same sense of understanding of what is to be or not to be secure and therefore a generic set of requirements and their respective key performance indicators can be formulated.

The current assessments practices are not suitable for providing meaningfully comparable results as they are tightly tailored to specific organizational security programme or not being reproducible. A new approach is considered to address the named shortcomings. This approach has several advantages: It shall be easy to implement the metric programme across different organizations to ensure confident information sharing. The approach shall also influence security measurement improvement.

Security in this context is considered to possess three components: requirements, policy, and mechanisms [32]. Requirements portray security goals. Policy describes steps to reach the goal. Mechanisms put into effect policy, mechanisms also refer to safeguards or countermeasures [12]. Security policy is derived from threat modeling; possible ways in which an organisational IS can be sabotaged. Threat modeling can results into a huge set of possible attack channels some of which may be difficult to mitigate and thus other approaches like business continuity and recovery plan may be assumed.

The approach we are proposing constitutes five elements; technology maturity analysis, threat analysis and modeling, requirements establishment, policies and mechanisms, and system behavior.

Technology maturity analysis: conduct technology maturity analysis to organizations considered for this metric. The analysis will provide minimum and maximum set of technologies applicable to the organizations. This is necessary in order to ensure uniform application of threat modeling and requirements. Different technology comes with different threat scenario. Also to ensure comparable metrics results (past against present), monitoring of technology adoption is necessary.

Threat analysis and modeling: it is confined into technology maturity analysis results. In relation to threat mitigation, some assumptions are considered:

1. Organizations strive to reduce the number of ways it can be attacked (reduce attack surface).
2. For each threat scenario, there may be several ways to contain the situation.
3. Organizations can opt zero, one or more approaches to mitigate the threat.

One aspect of measuring the security of an organisation is to assess the extent to which it minimizes attack surface [33]. It can be done by employing a score board, where coverage points are taken and compared against a baseline.

Requirements establishment: A generic set of requirement is formulated as sourced from threat analysis, laws and best practices.

Table 3: Comparison of approaches based on selected properties			
Properties	**Approaches**		
	NIST [7]	**WEISS et al [29]**	**CHAPIN & AKRIDGE [30]**
Philosophy (View of security)	totality of effectiveness and efficiency of implemented security programme	calculation of asset loss	safeguards implementation
Focus	assessment of various elements of programme	Scenario modeling and calculation of loss (expressed in monetary terms)	process maturity in terms of number of implemented sub processes
Degree of quantification	Numbers	Numbers	ranking; maturity score
Motivation	organisational self-correction tool; fulfilling regulatory requirements	compare results among different organisations	compare results among different organisations
(Source : Author, 2010)			

Policies and mechanisms: in practice, each organisation devises its own policy and chooses a set of mechanisms to implement the policy. If assumptions 2 and 3 hold, then the measurement process has to treat this part as black box to ensure comparable results. Since there are confined technologies, we can opt for a few, general aspects of policy and mechanisms to consider.

System behavior: security assessment should capture more information on top of security components in order to reveal a complete picture of security posture of an organisation. Information on security incidents trends and successful attacks are to be captured and analyzed. Information related to management and use of information systems (operational behavior) has to be monitored. The overall picture shall be revealed by looking at several dimensions of security.

Table 4. Elements of security posture assessment		
S_p		**Generic requirements:** -derived from threat modelling
	P & M	**Systems acquisition & configurations:** -machine monitoring -patch management -systems upgrade, ..
		Usage scenarios: -access control levels -policy violations -identification & authorization, ..
		Incident reports: -number of attacks (blocked/unblocked),..
(Source: Author, 2009)		

To illustrate this approach, let T be threat modeling results and R be a generic set of requirements, S_p be set of values depicting security posture of a measured organization. Let P be a set of policy describing requirements R, and let M be a set of mechanisms for enforcing policy P, then it follows that for single set of requirements R, organizations may deduce several policies: $P_i : i=$ 1,2,.., n. For each policy P_i, several different mechanisms can be derived: M_j : $j=$ 1,2,.., m. Where $m \geq n$. It is expected that, at minimum, S_p can reveal relatively comparable results if P and M are treated as black box and R is made to fulfill T. Since security is a process [12], it is important to include general performance indicators for P and M as shown in Table 4. Thus, S_p is not a single value, rather a set of values.

Security is not directly measured, so it needs validation to avoid measurement distortion [34]. Bad metrics use may lead to catastrophic decisions [35]. Metrics have to meet to a number of characteristics. These include:

- **Precision:** the extent that repeatable concise results can be demonstrated for several measurements taken under similar condition [6, 23].
- **Accuracy:** the degree of agreement of individual or average measurements with an accepted reference value or level [6].
- **Validity:** degree to which it measures what was intended to be measured [6].

- **Correctness:** the degree of formality adhered during measurement process [6].
- **Cost effective:** metrics data must be inexpensive to gather in terms of time and cost, preferably gathered automatically [23, 25].

While these characteristics are highly desirable, they are difficult to achieve. Fulfilling them has proven to be difficult [ref]. It is also important to stress that, to-date there are no established baselines through which the developed metrics can be compared, neither in the healthcare domain nor in any other domains.

Our novel approach when compared to those described in table 3 differs in that it considers security measurements in several aspects as shown in table 4. Metrics from this approach are not tailored to any security programme of individual organisations. Security posture is depicted as trends of various measurements results collected and aggregated in several different clusters. However, similar to others in table 3, this approach provides quantitative results. It is also intended to be used as a yardstick to compared security posture of different healthcare organisations.

7. Conclusion and further work

Security assessment is ad hoc due to increased complexity of information systems. While measurement principles require a clear definition of measurement boundary, the complexity of information systems makes it difficult. As dependence of life critical domains like healthcare to information systems increases, objective assessment of security is necessary to ensure adequate effort towards protection of information against all sorts of violations is devoted. In this networked world, ensuring the security of one organisation is not enough, a consideration of security posture of other links in the chain is important.

The current security assessment approaches do not provide comparable results among different organizations and thus cannot help to build confidence among different organizations.

The approach proposed in this paper facilitates the development of domain specific security metrics to assess the security posture of organisations. The metrics guided by this approach, shall only be useful for comparison of security posture of different organizations of the same domain, operating in slightly similar environments, not a replacement of the other metrics for internal security management like information security management (ISM), or network management. This approach will be useful because it will target a specific domain, so a notion or security view can be understandably shared across that specific domain. Also, these metrics are not confined to individual organization policy and procedure, so their results can be meaningfully shared and trusted.

As part of future work, an experiment of the validation of this approach is required in order to refine further its components to abide to the metric characteristics presented.

8. References

[1] J. a. Grimson, G. Stephens, B. Jung, W. Grimson, D. Berry, and S. Pardon, "Sharing health-care records over the Internet," *Internet Computing*, vol. 5, pp. 49-58, 2001.

[2] J. Grimson, G. Stephens, B. Jung, W. Grimson, D. Berry, and S. Pardon, "Sharing health-care records over the Internet," vol. 5, pp. 49-58, 2001.

[3] T. C. Rindfleisch, "Privacy, information technology, and health care," 1997.

[4] S. C. Payne, "A guide to security metrics," *SANS institute*, 2006.

[5] A. Jaquith, "The security of applications: Not all are created equal," *stake research Report*, 2002.

[6] D. S. Herrmann and S. Herrmann, *Complete guide to security and privacy metrics: Measuring regulatory compliance, operational resilience, and ROI*: CRC Press, 2007.

[7] E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson, "Performance Measurement Guide for Information Security (NIST Special Publication 800-55 Revision 1)," National Institute of Standards and Technology 2008.

[8] ISO/IEC-27002, "Information technology - Security techniques - Code of practice for information security management," ISO 2005.

[9] P. Joseph, A. Paul, J. Sushil, and R. Ronald, "A framework for establishing, assessing, and managing trust in inter-organizational relationships," in *Proceedings of the 3rd ACM workshop on Secure web services*. Alexandria, Virginia, USA: ACM, 2006.

[10] S. Noel, D. Wijesekera, and C. Youman, "Modern Intrusion Detection, Data Mining, and Degrees of Attack Guilt," in *Applications of Data Mining in Computer Security*, vol. 6, *Advances in Information Security*, D. Barbarà and S. Jajodia, Eds.: Kluwer Academic Publisher, 2002.

[11] P. K. Manadhata, "An attack surface metric," in *School of Computer Science*, vol. PhD. Pittsburgh: Carnegie Mellon University, 2008, pp. 165.

[12] B. Schneier, *Secrets and lies: digital security in a networked world*: Wiley New York, 2004.

[13] NIST-CSRC, "FIPS PUB 199: Standards for security categorization of federal information and information systems," National Institute of Standards and Technology 2004.

[14] NIST-CSRC, "FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems", 2006.

[15] S. Kremer and J. F. Raskin, "A game-based verification of non-repudiation and fair exchange protocols," *Journal of Computer Security*, vol. 11, pp. 399-429, 2003.

[16] J. Hallberg, A. Hunstad, and M. Peterson, "A framework for system security assessment," *Proc. from the Sixth Annual IEEE SMC Information Assurance Workshop IAW '05*, pp. 224-231, 2005.

[17] M. Swanson, N. Bartol, J. Sabato, J. Hash, and L. Graffo, *Security metrics guide for information technology systems*: NIST Special Publication 800-55, 2003.

[18] E. Vaast, "Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare," *Journal of Strategic Information Systems*, vol. 16, pp. 130-152, 2007.

[19] M. Meingast, T. Roosta, and S. Sastry, "Security and Privacy Issues with Health Care Information Technology," *In Proc. 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 5453 - 5458, 2006.

[20] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "SAGE: A Strong Privacy-Preserving Scheme Against Global Eavesdropping for eHealth Systems," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, vol. 27, pp. 365, 2009.

[21] BS-EN/ISO, "Health informatics - Information security management in health using ISO/IEC 27002 (BS EN ISO 27799:2008)," ISO 2008.

[22] S. L. Pfleeger, R. L. Trope, and C. C. Palmer, "Managing Organizational Security," *Security & Privacy*, vol. 1540, pp. 13-15, 2007.

[23] D. Rathbun and L. Homsher, "Gathering Security Metrics and Reaping the Rewards," SANs Intitute 2009.

[24] Y. Beres, M. C. Mont, J. Griffin, and S. Shiu, "Using Security Metrics Coupled with Predictive Modeling and Simulation to Assess Security Process," Hewlett-Packard Development Company 2009.

[25] A. Jaquith, *Security metrics: replacing fear, uncertainty, and doubt*: Addison-Wesley Professional, 2007.

[26] M. N. Wybourne, M. F. Austin, and C. C. Palmer, "National cybersecurity research and development challenges related to economics, physical infrastructure and human behavior," Institute for Information Infrastructure Protection (I3P) 2009.

[27] A. Atzeni and A. Lioy, "Why to adopt a security metric? A brief survey," in *Proceedings of the First Workshop on Quality of Protection*, 2005.

[28] S. Weiss, O. Weissmann, and F. Dressler, "A comprehensive and comparative metric for information security," in *Proceedings of IFIP International Conference on Telecommunication Systems, Modeling and Analysis (ICTSM2005)*, 2005, pp. 0-10.

[29] D. A. Chapin and S. Akridge, "How can security be measured," *information systems control journal*, vol. 2, pp. 43-47, 2005.

[30] M. Siponen, "Information security standards focus on the existence of process, not its content," *Communications of the ACM*, vol. 49, pp. 97-100, 2006.

[31] A. J. A. Wang, "Information security models and metrics," presented at 43rd ACM Southeast Conference, 2005.

[32] M. Bishop, "What is Computer Security?" *IEEE Security & Privacy*, vol. 1, pp. 67-69, 2003.

[33] P. K. Manadhata, "An attack surface metric," University of North Carolina, 2008.

[34] C. Kaner and W. P. Bond, "Software Engineering Metrics: What Do They Measure and How Do We Know," *10th International Software Metrics Symposium (Metrics 2004)*, pp. 1-12, 2004.

[35] W. Boyer and M. McQueen, "Ideal Based Cyber Security Technical Metrics for Control Systems," *CRITIS*, vol. 7, pp. 3-5, 2007.

