s.19(1)

The state and scientific basis of cyber security metrics

Including Canadian perspectives

George Yee
Procom Consultants Group Ltd.

Prepared By:
George Yee

Procom Consultants Group Ltd.
Contractor's Document Number: 310312
Contract Project Manager: Patrick Nadeau, 613-270-9339 ext.238
PWGSC Contract Number: W7714-4500883510
CSA: Matthew Kellett, Defence Scientist, 613-991-4362

Defence R&D Canada – Ottawa

Contract Report
DRDC Ottawa CR 2012-109
October 2012

Approved by

Original signed by Julie Lefebvre

Julie Lefebvre

Head, Cyber Operations Section

Approved for release by

Original signed by Chris McMillan

Chris McMillan

Chief Scientist, Defence R&D Canada - Ottawa

Abstract

This report describes a study on the state of enterprise cyber security metrics in terms of contributions from international research, Canadian university research, and Canadian industry. The study finds that very little published research exists on cyber security metrics compared to related fields such as information security, and existing research lacks scientific rigour. Furthermore, use of cyber security metrics by industry appears to be mostly limited to security information and event management (SIEM) software. This report proposes a scientific framework to provide a firm basis for the analysis of current and future cyber security measures and metrics. The report evaluates the state of the art (SoA) and state of practice (SoP) of published cyber security metrics using the proposed scientific framework, and identifies gaps between the SoA/SoP and what is theoretically possible. The report concludes with a summary of the study results and gives recommendations for future work. In addition, an annex is included that describes the viability of basing a security dashboard on current SIEM technology.

Résumé

Ce rapport décrit une étude portant sur l'état des mesures de la cybersécurité d'entreprise en fonction des travaux de recherche exécutés à l'étranger, dans les universités canadiennes, et des applications dans l'industrie canadienne. L'étude a permis de démontrer que très peu de travaux de recherche ont été publiés sur les mesures de la cybersécurité par rapport à d'autres domaines connexes comme, par exemple, la sécurité de l'information. On a constaté également que les travaux de recherche existants manquaient de rigueur scientifique. En outre, l'industrie semble avoir recours aux mesures de la cybersécurité presque uniquement à l'égard des logiciels de gestion des événements et des renseignements sur la sécurité (SIEM). Le présent rapport propose un cadre scientifique qui servira de base solide pour l'analyse des mesures et des paramètres actuels et futurs en matière de cybersécurité. Le rapport évalue l'état des connaissances et l'état de la pratique relativement aux travaux sur les mesures de la cybersécurité publiés au moyen du cadre scientifique proposé. Il recense aussi les écarts entre l'état des connaissances/état de la pratique et ce qui est théoriquement possible. En conclusion du rapport, on présente un résumé des résultats de l'étude et des recommandations de travaux de recherche à entreprendre dans l'avenir. De plus, il comporte une annexe abordant la viabilité d'un tableau de bord de la sécurité basé sur la technologie SIEM actuelle.

This page intentionally left blank.

Executive summary

The state and scientific basis of cyber security metrics: Including Canadian perspectives

George Yee; DRDC Ottawa CR 2012-109; Defence R&D Canada – Ottawa; October 2012.

Introduction: This study is interested in metrics that quantify the security of a cyber system. A useful metric is one that reflects the true security state of the system that can be determined consistently over time or between systems to allow for a meaningful comparison. Such cyber security metrics can answer important questions on security readiness and investments; however, most security metrics in use today are indicators at best and cannot be validated by others, i.e., they do not have a firm scientific basis. This report determines the current state of cyber security metrics in terms of Canadian and world-wide research, and Canadian industrial application.

Results: There is very little university research into cyber security metrics compared to related fields, such as information security. Much of the readily accessible work that is being done is based in North America. The use of cyber security metrics by Canadian industry appears to be limited to the use of dashboard-like security information and event management (SIEM) systems. This study proposes a scientific framework for cyber security metrics and we use it to evaluate published security metrics. None of these metrics are found to be capable of being independently validated, which is a necessary condition for a scientifically sound metric. The study notes SIEM technology is a viable base upon which to build a security dashboard that displays security alerts and recommends or takes corrective action.

Significance: This report sheds light on the current state of cyber security metrics as well as the makeup of the Canadian cyber security landscape. It is also proposes a potential scientific basis on which to construct future cyber security metrics.

Future plans: Recommendations for future work include further development of the proposed scientific framework for cyber security metrics and the determination of what additional steps are needed to build a security dashboard framework on SIEM technology.

Sommaire

The state and scientific basis of cyber security metrics: Including Canadian perspectives

George Yee ; DRDC Ottawa CR 2012-109 ; R & D pour la défense Canada – Ottawa; octobre 2012.

Introduction : Cette étude porte sur les mesures quantifiant la sécurité d'un système informatique. Une mesure utile permet d'illustrer le niveau réel de sécurité du système, qui peut être déterminé de façon constante au fil du temps ou par l'étude de plusieurs systèmes afin de pouvoir établir une comparaison utile. Ces mesures de la cybersécurité peuvent permettre de répondre à d'importantes questions concernant l'état de préparation et les investissements en matière de sécurité. Toutefois, la plupart des mesures de la sécurité en usage aujourd'hui sont, dans le meilleur des cas, des indicateurs et ne peuvent être validées par d'autres, c'est-à-dire qu'elles ne reposent sur aucune base scientifique solide. Ce rapport détermine l'état actuel des mesures de la cybersécurité en fonction des recherches effectuées au Canada et ailleurs dans le monde, et en fonction de leur application au sein des industries canadiennes.

Résultats : Très peu de travaux de recherche ont été effectués dans les universités sur les mesures de la cybersécurité par rapport à d'autres domaines connexes, par exemple, la sécurité de l'information. La plupart des études auxquelles on a pu avoir accès facilement sont basées sur l'Amérique du Nord. L'industrie canadienne ne semble utiliser les mesures de la cybersécurité qu'au moyen de systèmes de gestion des événements et de renseignements sur la sécurité (SIEM) s'apparentant à des tableaux de bord. Cette étude propose un cadre scientifique en matière de mesures de la cybersécurité que nous utilisons pour évaluer les mesures qui ont été publiées relativement à la sécurité. Nous avons constaté qu'aucune de ces mesures ne peut être validée de façon indépendante, une condition qui s'avère nécessaire pour qu'une mesure soit valide du point de vue scientifique. D'après l'étude, la technologie SIEM constitue une base viable sur laquelle établir un tableau de bord sur la sécurité affichant les alertes de sécurité et recommandant ou prenant des mesures correctives.

Importance : Ce rapport fait la lumière sur l'état actuel des mesures de la cybersécurité et sur le contexte de la cybersécurité au Canada. Il propose en outre une base scientifique sur laquelle on pourrait fonder les mesures de la cyber sécurité dans l'avenir.

Perspectives : Au chapitre des travaux recommandés, il serait bon de peaufiner le cadre scientifique proposé pour les mesures de la cybersécurité et de déterminer quelles seraient les

This page intentionally left blank.

Table of contents

List of figures

List of tables

Acknowledgements

I would like to gratefully acknowledge the insightful guidance of the Measures and Metrics Team consisting of Dan Craigen, Brian Eatock, Matthew Kellett, Julie Lefebvre, and Peter Mason during this study. I also owe thanks to Professor Paul Van Oorschot for his useful advice on where to look for research work on security metrics.

This page intentionally left blank.

1 Introduction

1.1 Motivation

In recent years, attacks against cyber systems have increased many folds. Barely a day goes by without headlines appearing about the latest systems compromise, in terms of web sites being brought down by DDoS (Distributed Denial of Service) attacks, or the loss of privacy due to malware infected computers. In response, systems owners have invested more and more funds into various forms of protection mechanisms (e.g. firewalls, biometrics, data encryption) as well as improve the design of systems and work flows to be more secure. However, the return on these investments or the subsequent increase in the level of security, has been largely unknown, leading to the following quandries:

- How much more do I need to spend to be "safe" from attack?
- Will the changes made to my software to improve security be effective?
- Are my company's work flows or processes sufficiently secure?
- How will adding the third party software component impact security?
- How can legislation requiring certain levels of security be enforced if the level of security is unknown?

These questions can go away if there was some way to measure the level of security of a cyber system. Properly defined, effective, security metrics appear to be the solution. A parallel situation occurs in performance engineering, where there is a need to know if the performance of a cyber system is sufficient to satisfy users when under a certain processing load. There, a performance analysis to obtain performance metrics such as throughput and service time is an effective approach to knowing if the performance is enough, and if not, where are the bottlenecks. Moving back to the security domain, it should be possible to perform a security analysis of a cyber system to obtain security metrics that would indicate if the system is secure from various forms of attack, and if not, where and what are the vulnerabilities.

Security metrics do exist and are being used. However, most of them are far from giving the results described above. They can be ineffective and not meaningful. For example, a traditional metric is the number of viruses detected and eliminated, say at a firewall. This metric is not meaningful since it says nothing about a) the number of viruses that were not detected and got through, and b) why are there so many viruses trying to get through in the first place [1]. Rather, a security metric should [1]:

- Measure organizationally meaningful quantities,
- Be reproducible,
- Be objective and unbiased,
- Be able to measure a progression toward a goal over time.

The above qualities of a good security metric also describe certain metrics that have a basis in science, such as the throughput metric in performance engineering. Throughput measures the number of jobs completed per second by a computing system. It is a quantitative measure of a computing system based on the laws of physics. It is also meaningful, reproducible, objective and unbiased, and can measure the improving performance of a system over time toward a throughput

goal. This leads to the question of what sort of scientific framework could give rise to such science-based metrics. Answering this question is a central theme of this report.

An interesting practical application of security metrics is in determining the security posture of a cyber system in real time. One envisages a security dashboard that displays security metrics associated with vulnerability points. The dashboard would display security alerts corresponding to strategic subsets and groupings of the metrics that exceed critical thresholds. Security officers monitoring the dashboard would then be able to take remedial action, upon which the security alerts would be replaced by "system back to normal" messages. One can further envisage the dashboard as having intelligence sufficient to recommend courses of remedial action appropriate to particular security alerts. This report assesses the viability of such a security dashboard.

1.2 Objectives and Scope

Given the above motivation, the objectives of this study are as follows (quoted from the contract statement of work (SoW) [2]):

1. Describe the broad scientific framework that currently defines measures and metrics for enterprise-wide cyber security.
2. Describe the state of the art (SoA) and state of practice (SoP) within the scientific framework.
3. Identify scientific gaps between the SoA/SoP and theoretically-achievable, evidence-based, enterprise-wide cyber security, including which measures and metrics can be validated reliably in repeatable experiments on what infrastructure and which cannot.
4. Investigate and summarize the Canadian landscape (investment, capabilities, ...), including efforts by government, academia, and industry.

The term "measures" can also mean protection methods as in "security measures for preventing password theft". Therefore, to avoid confusion, the phrase "measures and metrics" is replaced by "metrics", and there will be no further use of "measures and metrics" in the rest of this report.

Subsequent to the SoW, from which the above objectives are taken, it was agreed between all concerned, i.e. the stakeholders of this study and the contractor, that the following changes be made to the above objectives:

- Due to the interest of the stakeholders of this work in security metrics for cyber protection, the scope of objectives 1, 2, and 3 is limited to metrics that measure the security of the "cyber environment" in terms of software and hardware technologies that are in place within the "cyber environment", where "cyber environment" is defined to be "the independent network of information technology structures, including the Internet, telecommunications networks, computer systems and embedded processors and controllers including the software and information that reside within them"[a]. In particular, this scope includes security risk metrics for decision making if these metrics pertain to technologies as mentioned. On the other hand, this scope excludes security metrics for management and development

[a] from "Proposed Cyber Operating Concept Version 1", Cyber Task Force Briefing, 26 Nov. 2010, as related by email from Brian Eatock on Nov. 23, 2011.

processes because these processes are not software or hardware technologies that are in place. For example, a risk metric that gives 74% risk that port 180 will be attacked would be included. A metric that gives the number of code reviews per software module would be excluded.

- In objective 4, "government" is removed, i.e. objective 4 applies to academia and industry.

1.3 Approach

The above objectives were accomplished in 2 phases. Phase 1 consisted of data gathering, and comprised the following activities: a) search the literature for publications on security metrics, b) search Canadian universities for researchers and work on security metrics, and c) search the web sites of information security vendors doing business in Canada for products that make use of security metrics, e.g. security management making use of security metrics. Phase 2 consisted of the carrying out of the above objectives by analyzing the data gathered in phase 1.

The rest of this report is organized as follows. Chapter 2 describes and discusses the information found in Phase 1. Chapter 3 presents the results of carrying out objective 4. Chapter 4 gives the findings for objectives 1, 2, and 3. Finally, Chapter 5 gives conclusions and recommendations. The viability of the security dashboard mentioned at the end of Section 1.1 is discussed in Annex A.

2 Security Metrics in the Literature, Universities, and Industry

2.1 Introduction

This chapter presents and summarizes a) the publications found that describe work on security metrics, b) the Canadian universities found to have done work on security metrics, including the names of the researchers and their publications, c) the non-Canadian universities found to have done work on security metrics, including the names of the researchers and their publications, and d) the information security vendors doing business in Canada whose products involve security metrics.

2.2 Publications on Security Metrics

These publications were identified through searching the following sources: the Internet, the IEEE Xplore and ACM Digital Library databases, and the home pages of Canadian university researchers. The publications fall into the following categories of security metrics:

- Describing the nature of security metrics
- Measuring the security of a cyber system
- IT Security Risk Management
- Measuring the effectiveness of a security process

Table 1 lists the publications found along with summaries of their contents. The second category, "Measuring the security of a cyber system", is different from the other categories in that a) it considers the component make-up of the cyber system, b) it concerns the use of scientific tools (e.g. modeling) to measure the security, and c) it is limited to measuring the security of the cyber system and not other aspects such as operational security or security process. Note that a publication may fall under multiple categories, in which case the publication is repeated in each of those categories.

Table 1 – Security metrics publications and summaries

No.	Publication	Summary
A. Describing the Nature of Security Metrics		
1	"Measuring Cyber Security and Information Assurance", IATAC SOAR, May 8, 2009.	Broad coverage of US, including laws, standards, best practices, government programs, industry initiatives, measurable data, tools and technologies.
2	S. Stolfo, S. Bellovin, D. Evans, "Measuring Security", IEEE Security &	Discusses scientific basis for security and security metrics with examples and ideas for

	Privacy, May/June 2011. SBE2011.	research; focuses on security of a computer system.
3	R. Savoia, "Towards a Taxonomy for Information Security Metrics", QoP'07, 2007. Sav2007.	Proposes a high-level security metrics taxonomy for ICT product companies; gives an example of a security metrics taxonomy.
4	D. Chapin, S. Akridge, "How Can Security Be Measured?", Information Systems Control Journal, Vol. 2, 2005. CA2005.	Discusses what is wrong with traditional security metrics, giving characteristics of good metrics; discusses security maturity models with examples.
5	Wayne Jansen, "Directions in Security Metrics Research", NIST, April 2009.	Overviews security measurement and proposes possible research areas such as formal models of security measurement and artificial intelligence techniques.
6	O. Saydjari, "Is Risk a Good Security Metric?", Panel, Proceedings of QoP'06, 2006. Say2006.	Succinct descriptions of risk as a security metric, alternative security metrics, and what makes a good metric.
7	Andrew Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt, Addison-Wesley, 2007.	Discusses security metrics for enterprise application; security metrics applied broadly, not only to computing systems but also to all sorts of enterprise processes.
8	Lance Hayden, IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data, McGraw-Hill Osborne Media, June 2010.	Similar to the Jaquith book in its focus on the enterprise; covers security metrics in terms of effectiveness, implementation, operations, compliance, costs, people, organizations; includes 4 case studies.
B. Measuring the Security of a Cyber System		
1	S. Stolfo, S. Bellovin, D. Evans, "Measuring Security", IEEE Security & Privacy, May/June 2011. SBE2011.	Discusses scientific basis for security and security metrics with examples and ideas for research; focuses on security of a computer system.
2	Wayne Jansen, "Directions in Security Metrics Research", NIST, April 2009.	Overviews security measurement and proposes possible research areas such as formal models of security measurement and artificial intelligence techniques.
3	M. Howard, J. Pincus, J. Wing, "Measuring Relative Attack Surfaces", in *Computer Security in the 21st Century*, Springer, pp. 109-137, 2005. HPW2005.	Proposes "attack surfaces" as a measure of one system's security relative to another; an attack surface is described along 3 dimensions: targets and enablers, channels and protocols, and access rights.
4	M. Howard, "Attack Surface: Mitigate Security Risks by Minimizing the Code You Expose to Untrusted Users", 2004. How2004.	Practical advice to developers on how to reduce the attack surface of their code; based on actual Microsoft products such as Windows XP and Windows Server 2003.
5	L. Wang, A. Singhal, S. Jajodia, "Toward Measuring Network Security Using Attack Graphs", Proceedings of	Proposes a framework for assessing the security of a network based on attack graphs or access paths for attack, e.g. given two

	QoP'07, 2007. WSJ2007.	networks, if one has more paths of attack than the other, it is the less secure of the two; references WJS2007 for attack resistance.
6	S. Noel, L. Wang, A. Singhal, S. Jajodia, "Measuring security risks of networks using attack graphs," International Journal of Next-Generation Computing, Vol. 1, No. 1, pp 113-123, 2010. NWSJ2010	An expanded version of WSJ2007; provides a method for quantitatively analyzing the security of a network using attack graphs; the attack graphs are first populated with known vulnerabilities and likelihoods of exploitation and then "exercised" to obtain a metric of the overall security and risks of the network.
7	L. Wang, S. Jajodia, A. Singhal, S. Noel, "k-Zero day safety: Measuring the security risk of networks against unknown attacks," Proc. 15th European Symposium on Research in Computer Security (ESORICS 2010), Springer-Verlag Lecture Notes in Computer Science (LNCS), Vol. 6345, 20-22 September, pages 573-587, 2010. WJSN2010.	Proposes "k-zero day safety" as a security metric that counts the number of unknown zero day vulnerabilities that would be required to compromise a network asset, regardless of what those vulnerabilities might be. The metric is defined in terms of an abstract model of networks and attacks. Algorithms for computing the metric are included.
8	L. Wang, A. Singhal, S. Jajodia, "Measuring the overall security of network configurations using attack graphs," Proc.21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec 2007), Springer Lecture Notes in Computer Science, Vol. 4602, Steve Barker and Gail-Joon Ahn, eds., Redondo Beach, CA, pages 98-112, 2007. WJS2007.	Proposes an attack graph-based attack resistance metric for measuring the relative security of network configurations; incorporates two composition operators for computing the cumulative attack resistance from given individual resistances and accounts for the dependency between individual attack resistances; referenced by WSJ2007 for attack resistance.
9	L. Wang, T. Islam, T. Long, A. Singhal, S. Jajodia, "An Attack Graph-Based Probabilistic Security Metric", Proc. 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSEC 2008) , Springer-Verlag Lecture Notes in Computer Science (LNCS), Vol. 5094, pages 283-296, 2008. WILS2008.	Proposes an attack graph-based metric for the security of a network that incorporates the likelihood of potential multi-step attacks combining multiple vulnerabilities in order to reach the attack goal; the definition of the metric is claimed to have an intuitive and meaningful interpretation that is useful in real world decision making.
10	A. Singhal, X. Ou, "Techniques for Enterprise Network Security Metrics", Fifth Cyber Security and Information Intelligence Research Workshop (CSIIRW '09), Knoxville, TN, USA, 2009. SO2009.	Presents an attack graph-based method for evaluating the security of a network based on likelihood of attack (similar to WILS2008); stresses the derivation of the metric based on composition of component vulnerabilities whose security levels are already known. This is a short paper with accompanying slides.

11	M. Frigault, L. Wang, A. Singhal, S. Jajodia, "Measuring Network Security Using Dynamic Bayesian Network", Proceedings of QoP'08, 2008. FWSJ2008.	A Dynamic Bayesian Network (DBN) model is used to capture the dynamic nature of vulnerabilities that change over time. An attack graph is converted to a DBN by applying conditional probabilities to the nodes, calculated from the Common Vulnerabilities Scoring System (CVSS). The security of the network is calculated from the probabilities of the attacks being successful.
12	M. Frigault, L. Wang, "Measuring Network Security Using Bayesian Network-Based Attack Graphs", Annual IEEE International Computer Software and Applications Conference, 2008. FW2008	Proposes measuring network security using Bayesian network-based attack graphs so that relationships such as exploiting one vulnera-bility makes another vulnerability easier to exploit may be captured; differs from FWSJ2008 in that FWSJ2008 uses dynamic Bayesian networks whereas FW2008 uses just Bayesian networks; FWSJ2008 refers to FW2008 but not the other way around.
13	L. Krautsevich, F. Martinelli, A. Yautsiukhin, "Formal approach to security metrics. What does 'more secure' mean for you?", Proceedings of ECSA 2010, 2010. KMY2010.	Initial proposal and analysis of a number of mathematically-based definitions of security metrics such as "number of attacks", "minimal cost of attack", "maximal probability of attack", and even "attack surface" of HPW2005.
14	C. Wang, W. Wulf, "Towards a Framework for Security Measurement", Proceedings of 20th National Information Systems Security Conference, 1997. WW1997.	Proposes an initial framework for estimating the security strength of a system by decomposing the system into its security sensitive components and assigning security scores to each component; aggregate the component scores to get an estimate for the security strength of the system.
15	P. Halonen, K. Hätönen, "Towards holistic security management through coherent measuring", Proceedings of ECSA 2010, 2010. HH2010.	Discusses the problems of applying security metrics to telecommunication systems; compares security metric taxonomies, and discusses the need for security impact metrics; presents a broad view of security metrics.
16	D. Mellado, E. Fernández-Medina, M. Piattini, "A Comparison of Software Design Security Metrics", Proceedings of ECSA 2010, 2010. MFP2010.	A survey of various security metrics and standards that may be applicable to software design; compares the relevance of the various approaches to security properties such as authenticity and confidentiality.
17	J. Wang, H. Wang, M. Guo, M. Xia, "Security Metrics for Software Systems", Proceedings of ACMSE '09, 2009. WWGX2009.	Presents a security metrics formulation in terms of weaknesses and vulnerabilities, rated by CVSS scores for CVE vulnerability names; does not show how one would determine such scores for a brand new piece of software; not clear how the final security

		metric can be used to improve security.
18	R. Scandariato, B. De Win, W. Joosen, "Towards a Measuring Framework for Security Properties of Software", Proceedings of QoP '06, 2006. SDJ2006.	Claims that software has security properties that can be measured, much like it has maintainability properties such as complexity; proposes a number of software security properties along with corresponding metrics.
19	O. Saydjari, "Is Risk a Good Security Metric?", Panel, Proceedings of QoP'06, 2006. Say2006.	Succinct descriptions of risk as a security metric, alternative security metrics, and what makes a good metric.
20	Z. Dwaikat, F. Parisi-Presicce, "Risky Trust: Risk-Based Analysis of Software Systems", Proceedings of SESS'05, 2005. DP2005.	Proposes an approach to evaluate the security of a software system in development; security requirements are derived and a method is given for evaluating the likelihood of requirements violation based on the individual risks of system components.
21	Y. Liu, I. Traore, A.M. Hoole, "A Service-oriented Framework for Quantitative Security Analysis of Software Architectures", Proceedings of 2008 IEEE Asia-Pacific Services Computing Conference, 2008. LTH2008.	Proposes a User System Interaction Effect (USIE) model for systematically deriving and analyzing security concerns in service oriented architectures. The model is claimed to provide a foundation for software services security metrics and one such metric is defined and illustrated.
22	Y. Liu, I. Traore, "Properties for Security Measures of Software Products", Applied Mathematics & Information Sciences, I(2), pp. 129-156, 2007. LT2007.	Describes and formalizes properties that characterize security-related internal software attributes; these properties form a framework that can be used to rigorously identify and evaluate new security metrics; this framework is claimed to be sound but not complete; the properties are claimed to be necessary but not sufficient conditions for good security metrics.
23	Y. Liu, I. Traore, "UML-based Security Measures of Software Products", Proceedings of International Workshop on Methodologies for Pervasive and Embedded Software (MOMPES'04), 2004. LT2004.	Proposes the USIE model mentioned above for LTH2008 (probably first publication of the model) and derives it from UML sequence diagrams; this model can be used as a basis for architectural level security metrics and as an example, confidentiality metrics are defined based on the model.
24	E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, W. Robinson, "Performance Measurement Guide for Information Security", NIST SP 800-55, Revision 1, 2008.	Provides guidelines for developing, selecting, and implementing information system level and security program level measures for assessing the implementation, performance, and impact of security controls and other security related activities.
25	"Recommended Security Controls for Federal Information Systems and Organizations", NIST SP 800-53, 2009.	Describes recommended security controls; includes risk assessment as a control; this publication is used by the "Performance

		Measurement Guide for Information Security" as a basis for developing security measures.
26	T.E. Hart, M. Chechik, D. Lie, "Security Benchmarking Using Partial Verification", Proceedings of HotSec 08, 2008. HCL2008.	Proposes quantifying insecurity using the partial results of verification attempts - instrumented code (assertions) is property checked until a failure is found. The aggregate of such failures determine the level of insecurity of the software.
27	T. Maibaum, "Challenges in Software Certification", SQRL Report 59, McMaster University, May 2010. Mai2010.	Considers the requirements of software certification, proposing that certification should be product based, not development process based; considers the Common Criteria (CC) as a possible product based model for certification; although this paper is on software certification, it is relevant to security metrics in that it describes the elements of the CC that are pertinent to evaluating the security of a software product.
C. IT Security Risk Management		
1	Andrew Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt, Addison-Wesley, 2007.	Discusses security metrics for enterprise application; security metrics applied broadly, not only to computing systems but also to all sorts of enterprise processes.
2	Lance Hayden, IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data, McGraw-Hill Osborne Media, June 2010.	Similar to the Jaquith book in its focus on the enterprise; covers security metrics in terms of effectiveness, implementation, operations, compliance, costs, people, organizations; includes 4 case studies.
3	J. Talbot, M. Jakeman, Security Risk Management Body of Knowledge, book, Wiley, 2009.	Describes the security risk management process; discusses the pros and cons of various risk measures, including risks of threats and attacks.
4	G. Stoneburner, A. Goguen, A. Feringa, "Risk Management Guide for Information Technology Systems", NIST SP 800-30, 2002.	Provides a foundation for developing a risk management program; contains definitions and guidelines for assessing and mitigating risks within IT systems.
D. Measuring the Effectiveness of a Security Process		
1	Andrew Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt, Addison-Wesley, 2007.	Discusses security metrics for enterprise application; security metrics applied broadly, not only to computing systems but also to all sorts of enterprise processes.
2	Lance Hayden, IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data, McGraw-	Similar to the Jaquith book in its focus on the enterprise; covers security metrics in terms of effectiveness, implementation, operations,

	Hill Osborne Media, June 2010.	compliance, costs, people, organizations; includes 4 case studies.
3	D. Chapin, S. Akridge, "How Can Security Be Measured?", Information Systems Control Journal, Vol. 2, 2005. CA2005.	Discusses what is wrong with traditional security metrics, giving characteristics of good metrics; discusses security maturity models with examples.
4	S.S. Alaboodi, "Towards Evaluating Security implementations Using the Information Security Maturity Model (ISMM)", MASc thesis, University of Waterloo, 2007. Ala2007.	Extensions and abstractions of the ISMM security maturity model are proposed with the goals of using the extended model to identify the security level of implementations as well as promote the optimization of IT and security expenditures.
5	Carnegie-Mellon University, "The Systems Security Engineering Capability Maturity Model (SSE-CMM) – Model Description Document", Version 3, June 15, 2003. Accessed Mar. 16, 2012, at: http://www.sse-cmm.org/model/model.asp	Describes essential characteristics of a sound security engineering process; addresses security engineering activities that span the entire security engineering lifecycle, including process metrics; applies to all types and sizes of security engineering organizations, including commercial, government, and academic organizations.
6	R.F. Lentz, "Advanced Persistent Threats & Zero Day Attacks", slide presentation, 2010. Len2010.	Describes the stages of the Cyber Security Maturity Model, which can be measures of where an organization stands in terms of its security posture.
7	R.F. Lentz, "Cyber Security Maturity Model", slide presentation, 2011. Len2011.	Describes advanced persistent threats and the stages of the Cyber Security Maturity Model; appears to be an updated version of Len2010.

2.2.1 Discussion

The publications listed above do not all fit neatly into the categories in which they have been placed. This is natural since security metrics can mean different things to different people, and different authors approach the subject from their own varied backgrounds and environments. The chosen categories do, however, help to identify the papers that are most relevant to the objectives of this study. Of course, the research coverage represented by these publications is limited by the data sources searched, since not all research is published or published in these data sources. Nevertheless, one can say that given the dominance of IEEE and ACM publication repositories over other sources, this coverage is reasonably high.

Discussions of the papers in each category vis-à-vis the objectives of this study follow. The papers are referenced as "category-letter(paper number)", e.g. A(1) refers to paper 1 in Category A.

2.2.1.1 Category A: Describing the Nature of Security Metrics

This category treats questions such as "what is a security metric?" (e.g. A(3), A(4), A(7), A(8)), "what makes a good security metric?" (e.g. A(4), A(6), A(7), A(8)), "what does a security metrics taxonomy look like?" (e.g. A(3)), "do security metrics have a scientific basis?" (e.g. A(2), A(5)), "what are good research areas in security metrics?" (e.g. A(5)), and "who are the U.S. industrial and government players in security metrics, and what security metrics initiatives have they undertaken? (A(1))". For the objectives of this study, information is needed on the scientific basis of security metrics and on what makes a good security metric. Thus, A(2), A(4), A(5), and A(6) are the more relevant papers for this study from Category A.

2.2.1.2 Category B: Measuring the Security of a Cyber System

The papers in this category propose a range of techniques that make use of metrics to evaluate the security of a cyber system within an enterprise. The techniques involve the components of the cyber system and generally do not treat supporting areas such as software development practice, security operations, or security process. The papers mostly apply to the software of a cyber system.

Since the objectives of this study call for understanding the scientific framework supporting security metrics for enterprise cyber systems, and the papers in this category develop security metrics for such systems based on various frameworks, it follows that these papers are the most relevant ones for this study. An analysis of the types of paper in this Category is deferred to Chapter 3.

2.2.1.3 Category C: IT Security Risk Management

This category treats risk management for IT vulnerabilities, considering the probability and impact of occurrence. Risk management is a process, consisting of a) identifying risks, b) assessing risks, and c) following procedures to reduce the risks to acceptable levels. In addition, some of the papers (e.g. C(4)) provide guidance on selecting security controls with which to mitigate the identified risks.

Metrics associated with security risk management include quantifications of the risks themselves, employing various formulas to calculate these risks, and metrics that quantify the effectiveness of the risk management process. However, the quantifications of risks and the risk management process cover all of IT, including, e.g. operations and software development, and does not focus on evaluating the security of a cyber system with sufficient detail. Therefore, the papers in this category are not very relevant for achieving the objectives of this study. Papers that use risks in conjunction with system components and metrics to evaluate security, which are more in line with the objectives of this study, have been placed in Category B.

2.2.1.4 Category D: Measuring the Effectiveness of a Security Process

The papers in this category concern metrics that assess the effectiveness of security processes or indicate where an organization is at in terms of a security maturity model. Security processes

usually apply to enterprises but maturity models can apply to regions, and even countries, in addition to enterprises.

This Category is largely not relevant for achieving the study objectives since the metrics do not apply to evaluating the security of a cyber system.

2.3 Security Metrics Research in Canadian Universities

To discover what security metrics research is being done in Canadian universities, a search was conducted on the web sites of 58 universities in Canada. The universities were selected based partly on Maclean's 2011 university rankings [3] and partly on authors' Canadian university affiliations from the publications search. The list of universities included all of the institutions classified by Maclean's as: a) "medical doctoral" universities that "offer a broad range of Ph.D. programs and have medical schools" (e.g. McGill), b) "comprehensive" universities that "have a significant degree of research activity and a wide range of programs at the undergraduate and graduate levels, including professional degrees" (e.g. Waterloo) , and c) "primarily undergraduate" universities that "are largely focused on undergraduate education with relatively fewer graduate programs and graduate students" (e.g. St. Francis Xavier). A listing of universities by province was obtained from [4]. The universities were then selected by comparing this list with Maclean's lists as described above and including universities having researchers with publications found in the publications search in Section 2.2. This ensured a wide coverage of Canadian post secondary institutions.

The results of the search are presented in alphabetical order of province, in Table 2 and Table 3. Table 2 identifies the universities for which no evidence of security metrics research was found. Table 3 shows universities that do have such research and summarizes the research.

Table 2 – Canadian universities without security metrics research

Province	Universities Without Security Metrics Research
Alberta	Athabasca U, U of Alberta, U of Calgary, U of Lethbridge
British Columbia	Simon Fraser U, U of British Columbia, U of Northern British Columbia
Manitoba	Brandon U, U of Manitoba, U of Winnipeg
New Brunswick	Mount Allison U, St. Thomas U, U of Moncton, U of Fredericton, U of New Brunswick
Newfoundland / Labrador	Memorial U of Nfld
Nova Scotia	Acadia U, Cape Breton U, Dalhousie U, Mount St. Vincent U, Saint Mary's U, St. Francis Xavier U

Ontario	Brock U, Carleton U, Lakehead U, Laurentian U, Nipissing U, Queen's U, Royal Military College of Canada, Ryerson U, Trent U, U of Guelph, U of Ontario Institute of Technology, U of Ottawa, U of Western Ontario, U of Windsor, York U, Wilfrid Laurier U
Prince Edward Island	U of Prince Edward Island
Quebec	Bishop's U, McGill U, U de Montréal, École de Technologie Superieure (U du Québec), U du Québec à Montréal, École Polytechnique, U du Québec à Trois-Rivières, U du Québec en Outaouais, U de Sherbrooke, U Laval
Saskatchewan	U of Regina, U of Saskatchewan

Table 3 – Canadian universities with security metrics research

Provinces, Universities and Researchers	**Description of Research and Associated Publications**
British Columbia	
U of Victoria Issa Traore itraore@ece.uvic.ca	Research: Identify, develop and validate mathematically and empirically a family of metrics that can be used to guide efficiently the software security engineering process; they are also developing concurrently a toolkit that will assist developers in generating and interpreting the metrics from UML models; the tool (beta available) is named STEM for Security Testing and Engineering using Metrics; see STEM at: http://www.isot.ece.uvic.ca/projects.html Publications: Y. Liu, I. Traore, "UML-based Security Measures of Software Products", Proceedings of 1st International Workshop on Model-based Methodologies for Pervasive and Embedded Systems (MOMPES'04), May 2004. Also see publications under "software security" at: http://www.isot.ece.uvic.ca/publications.html
Ontario	
McMaster U Alan Wassyng, Tom Maibaum, and Mark Lawford	Research: Software certification; considers and describes the use of the Common Criteria for evaluating software security Publications:

	T. Maibaum, "Challenges in Software Certification", SQRL Report 59, McMaster University, May 2010.
U of Toronto Thomas E. Hart, Marsha Chechik, David Lie	Research: Proposes using the partial results of verification attempts (property checking) to quantify insecurity. Publications: T.E. Hart, M. Chechik, D. Lie, "Security Benchmarking Using Partial Verification", Proceedings of HotSec 08, 2008. HCL2008.
U of Waterloo Gordon Agnew (thesis supervisor)	Research: Evaluation of security implementations using a security maturity model. Publications: S.S.Alaboodi, "Towards evaluating security implementations using the Information Security Maturity Model (ISMM)", masters thesis, 2007.
Quebec	
Concordia U Lingyu Wang	Research: Measuring security using attack graphs, Bayesian networks, security risk analysis Publications: S. Noel, L. Wang, A. Singhal, S. Jajodia, "Measuring security risks of networks using attack graphs," International Journal of Next-Generation Computing, Vol. 1, No. 1, pp 113-123, 2010. NWSJ2010 L. Wang, S. Jajodia, A. Singhal, S. Noel, "k-Zero day safety: Measuring the security risk of networks against unknown attacks," Proc. 15th European Symposium on Research in Computer Security (ESORICS 2010), Springer-Verlag Lecture Notes in Computer Science (LNCS), Vol. 6345, 20-22 September, pages 573-587, 2010. M. Frigault, L. Wang, "Measuring Network Security Using Bayesian Network-Based Attack Graphs", Annual IEEE International Computer Software and Applications Conference, 2008. FW2008 M. Frigault, L. Wang, A. Singhal, S. Jajodia, "Measuring Network Security Using Dynamic Bayesian Network", Proceedings of QoP'08, 2008. FWSJ2008. L. Wang, T. Islam, T. Long, A. Singhal, S. Jajodia, "An Attack Graph-Based Probabilistic Security Metric", Proc. 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSEC 2008) , Springer-Verlag Lecture Notes in Computer Science (LNCS), Vol. 5094, pages 283-296, 2008. WILS2008. L. Wang, A. Singhal, S. Jajodia, "Measuring the overall security of

	network configurations using attack graphs," Proc.21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec 2007), Springer Lecture Notes in Computer Science, Vol. 4602, Steve Barker and Gail-Joon Ahn, eds., Redondo Beach, CA, pages 98-112, 2007. WJS2007-1. L. Wang, A. Singhal, S. Jajodia, "Toward Measuring Network Security Using Attack Graphs", Proceedings of QoP'07, 2007. WSJ2007.

2.3.1 Discussion

As Table 3 shows, 9 professors across 5 Canadian universities were found to engage in security metrics research. The majority of the publications came from Concordia University. As well, except for the work based on a security maturity model from the University of Waterloo, all of the research work falls into Category B, Measuring the Security of a Cyber System. As such, it is very relevant to the objectives of this study.

The search for security metrics research work drilled down to professors' university web pages where a professor would indicate his/her research areas and associated publications. The amount of relevant research found in this manner depends, of course, on the degrees to which these web pages have been kept up to date. As mentioned above, universities with security metrics research were also identified through the literature search in Section 2.2. Hence, if the web page search missed any Canadian researcher, he or she should still be identified through the literature search. To further confirm that this identification process has in large measure succeeded, the author contacted acquaintances in academia, who stated that they were not aware of any other such work.

2.4 Security Metrics Research in Non-Canadian Universities

Table 4 presents the non-Canadian universities found to have research in security metrics. This information was compiled from the publications in Section 2.2 that have authors from non-Canadian universities. In Table 4, publications that fall under multiple Section 2.2 categories, have an appended "R" for "Repeated".

Table 4 – Non-Canadian universities with security metrics research

Universities and Researchers	Section 1 Publications
United States	
Columbia University: Sal Stolfo, Steven M. Bellovin	A(2), B(1)R
University of Virginia: David Evans, Chenxi Wang, William Wulf	A(2), B(1)R, B(14)

Carnegie-Mellon University: Jeanette Wing	B(3)
George Mason University: Sushil Jajodia, Steven Noel, Zaid Dwaikat, Francesco Parisi-Presicce	B(5), B(6), B(7), B(8), B(9), B(11), B(20)
Kansas State University: Xinming Ou	B(10)
Southern Polytechnic State University: Ju An Wang, Hao Wang, Minzhe Guo, and Min Xia	B(17)
Italy	
University of Pisa: Leanid Krautsevich	B(13)
Univ. di Roma La Sapienza: Francesco Parisi-Presicce	B(20)
Spain	
University of Castilla-La Mancha: Daniel Mellado, Eduardo Fernández-Medina, Mario Piattini	B(16)
Belgium	
Katholieke Universiteit Leuven: Riccardo Scandariato, Bart De Win, and Wouter Joosen	B(18)

The data in Table 4 shows that even on a world wide basis, excluding Canada, the number of researchers and universities engaged in security metrics research is relatively few. This number is even more remarkable if one additionally excludes the United States, leaving only three countries with this research and essentially only one university in each of these three countries (for Italy, Francesco Parisi-Presicce identifies himself with George Mason University as well).

Comparing Canada to the United States, the latter has 15 researchers across 6 universities that were found to have engaged in security metrics research, whereas Canada has 9 professors across 5 universities. The term "researchers" is used for the United States, since they include students as well as professors. Thus considering the amount of research alone, one can say that Canada is comparable to the United States. However, the latter has roughly ten times the population of Canada and the number of universities in the United States (public and private 4-year institutions) is roughly 2400[b] whereas Canada has about 100[c] universities. Hence on a per capita basis and on a per university basis, Canada has far more research in security metrics than the United States. Canada also has more research in this area than the rest of the world excluding the United States.

[b] Retrieved March 16, 2012 from http://www.infoplease.com/ipa/A0908742.html
[c] Retrieved March 16, 2012 from http://www.canada-city.ca/canada-universities.php

2.5 Information Security Vendors Operating in Canada Whose Products Involve Security Metrics

Step 1 for this part of the study was to identify which information security vendors to consider. "Operating in Canada" meant that both Canadian companies, i.e. companies with headquarters in Canada, and international companies could be candidates, as long as they sell their products to clients residing in Canada. It was hypothesized that products involving security metrics are likely to be at the leading edge of innovation and so would probably be offered by innovative companies, or companies that have a history of innovative products. Hence "innovative history" was one factor for vendor selection. Another factor was "vendor size or amount of sales" since research and development requires ample funds. A third factor was to ensure that companies satisfying the other two factors and that have headquarters in Canada were included, since the focus of this part of the study is the Canadian perspective. Toward these ends, the list of information security vendors was obtained as follows: a) start with the 10 companies that make up the 2010 Branham top 10 ICT security companies in terms of revenue [5], b) add security companies from Industry Canada's pamphlets "ICT Security and Canada: The Future is Here" [6] and "IT Security and Canada: The Future is Here" [7], and c) add companies that have an established reputation and history of innovation (e.g. Symantec, McAfee). Once this list of vendors was identified, the web sites of these vendors were examined for security products making use of security metrics. Table 5 presents these vendors along with their products, identifying the security metrics, if any. SIEM refers to Security Information and Event Management, which is discussed further in Section 3.2.

Table 5 – Information security vendors operating in Canada that use security metrics in their products

Vendor	Product or Service	Security Metrics (SM) Details
The following first 10 companies in order comprise the 2010 Branham Top 10 Canadian ICT Security Companies in terms of revenue (highest revenue at the top).		
MXI Security www.mxisecurity.com	Portable security solutions	No security metrics found
ESI Information Technologies www.esitechnologies.com	Storage, security, availability and compliance solutions	SIEM offering called "Octopus": dashboard, table of services currently affected by incidents, statistics on resolution, statistics on delays, performance indicator report
ParetoLogic www.paretologic.com	PC security and utility software	No security metrics found
Absolute Software	IT asset management, data security and computer theft	Computrace product for asset management employs metrics

www.absolute.com	recovery	such as total number of assets versus subscriptions, products in use/not in use, call-out rate. Also, metrics used in patch management, and application & license management
The Herjavec Group www.herjavecgroup.com	Security solutions, WAN acceleration and emerging technologies	Offers RSA enVision SIEM, reports using SM on log management, as well as compliance and audit. Reports on vulnerabilities,compliance, and patch management; executive dashboard showing security posture.
Graycon Group www.graycon.com	Secure flexible IT support and solutions	SIEM and log management reporting, security assessment
Global Relay Communications www.globalrelay.com	Hosted archiving, compliance and e-discovery of e-mail and IM	No security metrics found
NCI www.nci.ca	IT security, networking and forensic solutions	SIEM reporting; offers SIEM solutions from RSA, Check Point, and Enterasys; UTM (Unified Threat Management) reporting; vulnerability management reporting (including patching); dashboards
Cistel www.cistel.com	IT security and privacy, managed services and IT staffing	SIEM reporting; offers the ArcSight SIEM
TRM Technologies www.trm.ca	E-security, enterprise architecture, ICT infrastructure and risk management	No security metrics found
The following companies were selected based on Industry Canada published information as well as size and history of innovation.		
L-1 Identity Solutions www.l1id.com	Develops advanced biometric technologies, software and stand-alone hardware for identity verification	No security metrics found
S.I.C. Biometrics	Designs, manufactures and internationally commercializes	No security metrics found

www.sic.ca	biometrics security products and solutions; specializes in fingerprints	
Certicom www.certicom.com	Develops robust cryptographic products.	No security metrics found
Entrust www.emtrust.com	Provides authentication, authorization and encryption services	No security metrics found
Okiok www.okiok.com	Offers IT security tools aimed at the specific needs of organizations operating in sectors such as health, financial services and government	risk "report card"
Whitenoise Laboratories www.wnlabs.com	Develops core technologies to secure communications, data, code and applications for businesses and individuals	No security metrics found
Diversinet www.diversinet.com	Offers mobile device security software that allows users to protect their identity and data when communicating or making transactions on wireless networks; focuses on protection of PHI.	No security metrics found
Above Security www.abovesecurity.com	Provides managed security services and consulting to protect vital information from security breaches, leaks, corruptions and system failures; "managed" means monitoring client's systems	Reports for vulnerability assessment, IDS and IPS; possibly SM in ISO 27001 compliance service
Quiettouch www.quiettouch.com	Integrates custom security solutions into its network designs, offering clients managed network virus protection, back-up strategies, and disaster recovery and firewall implementation	Managed security services include reports on the level of protection and the conditions affecting critical operations.
Q1 Labs www.q1labs.com	Provides award-winning network intrusion detection and management software that meets the needs of business and	SIEM offering: QRadar provides reporting functions for logs, security events, vulnerability data, risks, and compliance

	government	requirements - these can be treated as SM
CGI Group www.cgi.com/en/systems-integration-and-consulting/information-security	Enterprise security management, security engineering, business continuity, managed security services (protection from viruses, etc.), cloud security	Offers managed security service which includes monitoring for security incidents and reporting that can involve SM
Domus IT Security Laboratory www.domusitsl.com	IT security test and evaluation; tests cryptographic modules; security evaluations under Common Criteria; company web page not accessible Feb. 21, 2012	No security metrics found
EWA www.ewa-canada.com	Helps clients solve their most complex problems related to Information Management, Identity Management and Information Technology Security	Operates CanCERT which collects, analyzes, and disseminates info related to threats, vulnerabilities, and incidents and offers reports and network attack statistics - these are potentially SM; also offers managed security services and risk management which are additional sources of SM
Bell Business Solutions www.bell.ca/enterprise/EntPrd_Sec_Landing.page	Offers network protection, governance, risk management and compliance, IPv6 professional services, identity and access management, managed DDoS Protection service, privacy solutions	Offers governance, risk management, and compliance (GRC) that includes threat and risk assessment - standardized assessments provide data for auditors and management - this data can be treated as SM
Telus telus.com/en_CA/National/products/Medium_And_Large_Business/Security/natMlbSecurity.html	Application security, data security, governance, risk and compliance, infrastructure security, mobile security, physical security, threat and vulnerability research	Offers governance, risk management, and compliance that are sources of SM (similar to Bell); also offers software security including application testing, code reviews, processes for secure software development that are additional sources of SM
Symantec www.symantec.com/en/ca/solutions/enterprise.jsp	Security management, endpoint security, messaging security, web security	Provides security management that includes "data correlation" to identify risks and vulnerabilities, and a platform to protect against threats and report on incidents -

		this data can be treated as SM
RSA www.rsa.com	Services and products cover the whole gamut of enterprise security needs.	Offers eGRC (RSA Archer eGRC Suite) automation that identifies business risks and evaluates them through online assessments and metrics as well as reporting for incidents and audit management
McAfee www.mcafee.com/ca/	Offers solutions and services that help secure systems, networks, and mobile devices	Compliance reporting,vulnerability assessment reporting, risk-based analytics, decision-support risk metrics (see quantitative metrics brochure)
Sophos www.sophos.com	Offers complete security with full range of endpoint, encryption, email, web, network security and threat management products	Maintains metrics on malware, threats, and spam; operates dashboards for malware, threats, and spam

2.5.1 Discussion

The method of vendor selection described at the beginning of this Section identified 29 information security vendors operating in Canada. Of these, 18 were found to use some form of security metrics in their products. The metrics are used primarily in products that provide information or reporting, for the purposes of compliance management or security situational awareness. Thus, vendors that do not provide a reporting service tended not to use security metrics in their products, e.g. S.I.C. Biometrics, ParetoLogic. Details regarding the nature of these security metrics are deferred to Chapter 3.

Identifying the security metrics was not always straight-forward as in many cases, the vendors did not label relevant data items as "security metrics" per say. Fortunately in these cases, the data items were clearly security metrics, consistent with the industrial use of the term "security metric". For example, "incident counts", "risks", "malware statistics", "spam statistics" are commonly known as security metrics in industry.

The accuracy of Table 5 is directly dependent on the accuracy of vendor web site information. However, the latter should be highly accurate since a vendor that keeps a poorly maintained or inaccurate web site will suffer the consequences in terms of loss of business.

3 The Current Canadian Security Metrics Landscape

The objective of this chapter is to describe the current Canadian security metrics landscape in terms of a) contributions to security metrics research from Canadian universities and b) contributions to the application of security metrics from Canadian industry.

3.1 Contributions to Security Metrics Research from Canadian Universities

To determine the contributions to security metrics research from Canadian universities, the web sites of 58 Canadian universities were searched for evidence of security metrics research. The method for selecting the universities has been described in Section 2.3. A summary of the search results has also been given in Section 2.3.1. More details of these results follow.

The search of the 58 Canadian university web sites found:

- 9 professors across 5 Canadian universities with security metrics research from computer science or computer engineering departments; the universities and distribution of professors and publications are as follows (from west to east):
    - University of Victoria, 1 professor, 1 publication
    - McMaster University, 3 professors, 1 publication
    - University of Waterloo, 1 professor, 1 publication
    - University of Toronto, 3 professors, 1 publication
    - Concordia University, 1 professor, 7 publications

  Note that the number of publications shown here may not accurately reflect the true number of publications as some publications may be missing from the web site.

- The following contributions to security metrics research:
    - University of Victoria: security metrics for guiding secure software engineering
    - McMaster University: measuring software security using the Common Criteria
    - University of Waterloo: measuring security using a security maturity model
    - University of Toronto: measuring software security by quantifying insecurity
    - Concordia University: measuring network security using attack graphs, Bayesian networks, and risk analysis

  As noted in Section 2.3.1, all contributions to research, except for security maturity model work, fall within Category B, Measuring the Security of a Cyber System.

The comparison made in Section 2.4 of Canada's contributions in this area to those of other countries placed Canada in good stead despite the seemingly low Canadian numbers. There, it was determined that Canada's contributions are roughly quantitatively the same as the United States, but because the United States has roughly 24 times the number of universities as Canada, Canada's contributions are actually better than those of the United States on a per university basis. Compared to countries other than the United States, Canada's contributions are far better.

Given the above findings, the contributions to security metrics research by Canadian universities may be characterized as shown in Figure 1.

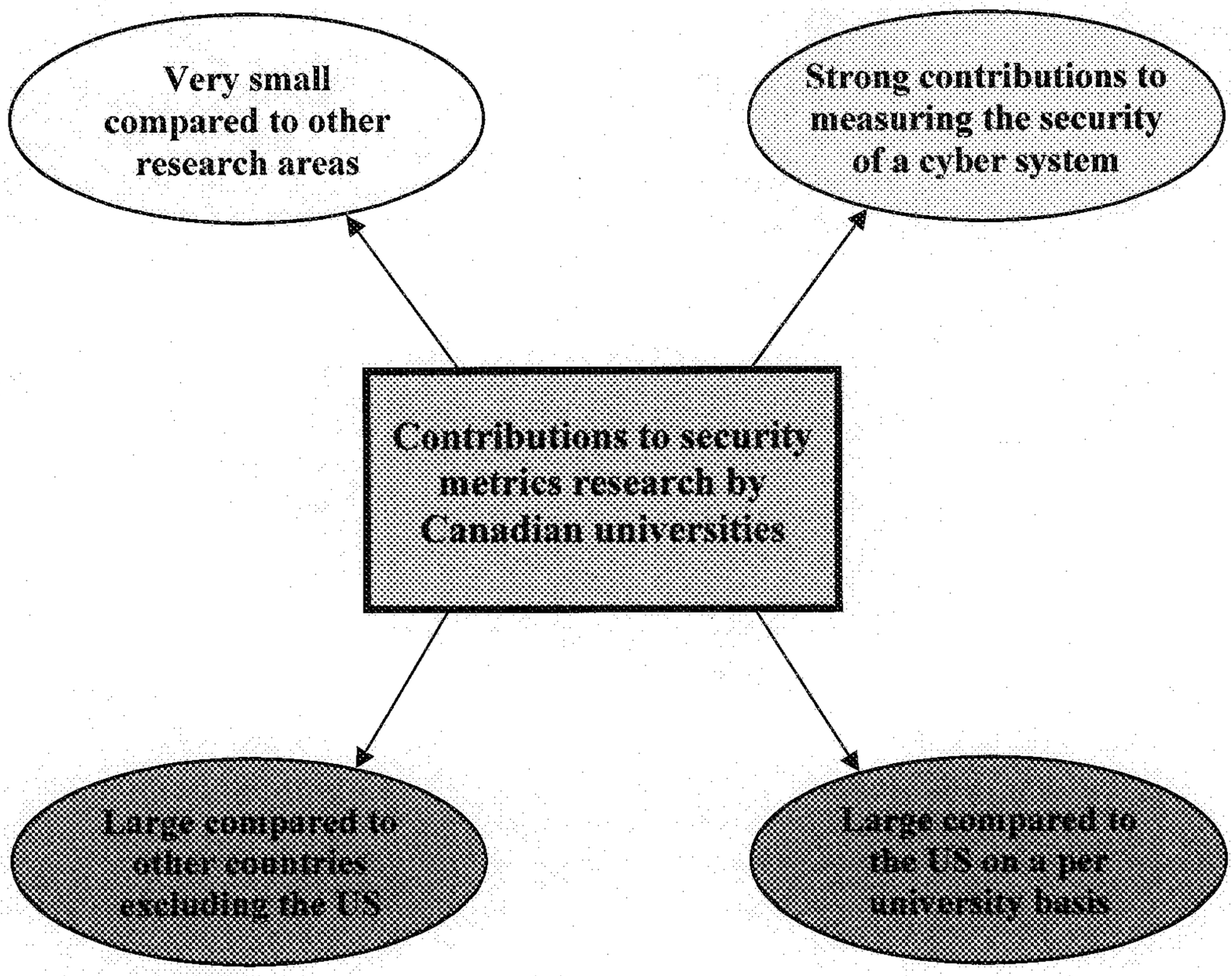

Figure 1 – Characteristics of the contributions to security metrics research by Canadian universities

3.2 Contributions to the Application of Security Metrics from Canadian Industry

As mentioned in Section 2.5.1, 18 out of 29 information security vendors operating in Canada used some form of security metrics in their products. As well, Table 5 shows that the majority of the security metrics arise from SIEM products. SIEM stands for Security Information and Event Management.. According to Wikipedia, "SIEM technology provides real-time analysis of security alerts generated by network hardware and applications. SIEM solutions come as software, appliances or managed services, and are also used to log security data and generate reports for compliance purposes"[d]. More details on SIEM products are given in Chapter 4.

Table 6 examines the nature of the security metrics presented in Table 5. In Table 6, "security process management" includes security processes such as logging, patching, vulnerability identification and reporting, and threat management.

[d] Retrieved Mar. 20, 2012 from http://en.wikipedia.org/wiki/Security_information_and_event_management

Table 6 – Contributions to the application of security metrics by information security vendors operating in Canada

Vendor	Security Metrics (SM) Details (from Table 5)	Nature of Security Metrics
ESI Information Technologies www.esitechnologies.com	SIEM offering called "Octopus": dashboard, table of services currently affected by incidents, statistics on resolution, statistics on delays, performance indicator report	Consists of counts and statistics for security process management, and security situational awareness
Absolute Software www.absolute.com	Computrace product for asset management employs metrics such as total number of assets versus subscriptions, products in use/not in use, call-out rate. Also, metrics used in patch management, and application & license management	Consists of counts for asset management (including loss detection) and security process management
The Herjavec Group www.herjavecgroup.com	Offers RSA enVision SIEM, reports using SM on log management, as well as compliance and audit. Reports on vulnerabilities, compliance, and patch management; executive dashboard showing security posture.	Consists of counts and statistics for security process management, compliance management, audits, and security situational awareness
Graycon Group www.graycon.com	SIEM and log management reporting, security assessment	Consists of counts and statistics for security process management, and security situational awareness
NCI www.nci.ca	SIEM reporting; offers SIEM solutions from RSA, Check Point, and Enterasys; UTM (Unified Threat Management) reporting; vulnerability management reporting (including patching); dashboards	Consists of counts and statistics for security process management, compliance management, audits, security situational awareness, and dashboards
Cistel www.cistel.com	SIEM reporting; offers the ArcSight SIEM	Consists of counts and statistics for security process management, and security situational awareness
Okiok	risk "report card"	Consists of identified risks for

www.okiok.com		security process management, and security situational awareness
Above Security www.abovesecurity.com	Reports for vulnerability assessment, IDS and IPS; possibly SM in ISO 27001 compliance service	Consists of counts and statistics for security process management, compliance management, and security situational awareness
Quiettouch www.quiettouch.com	Managed security services include reports on the level of protection and the conditions affecting critical operations.	Consists of counts and statistics for security situational awareness
Q1 Labs www.q1labs.com	SIEM offering: QRadar provides reporting functions for logs, security events, vulnerability data, risks, and compliance requirements - these can be treated as SM	Consists of counts, statistics, and risks for security process management, compliance management, and security situational awareness
CGI Group www.cgi.com/en/systems-integration-and-consulting/information-security	Offers managed security service which includes monitoring for security incidents and reporting that can involve SM	Consists of counts and statistics for security situational awareness
EWA www.ewa-canada.com	Operates CanCERT which collects, analyzes, and disseminates info related to threats, vulnerabilities, and incidents and offers reports and network attack statistics - these are potentially SM; also offers managed security services and risk management which are additional sources of SM	Consists of counts, statistics, and risks for security process management, and security situational awareness
Bell Business Solutions www.bell.ca/enterprise/EntPrd_Sec_Landing.page	Offers governance, risk management, and compliance (GRC) that includes threat and risk assessment - standardized assessments provide data for auditors and management - this data can be treated as SM	Consists of counts and statistics for security process management, compliance management, audits, and security situational awareness
Telus www.telus.com/en_CA/National/products/Medium_And_Large_Business/Security/natMlbSecurity.html	Offers governance, risk management, and compliance that are sources of SM (similar to Bell); also offers software security including application	Consists of counts, risks, and statistics for security process management, secure software development, compliance management, and security

	testing, code reviews, processes for secure software development that are additional sources of SM	situational awareness
Symantec www.symantec.com/en/ca/solutions/enterprise.jsp	Provides security management that includes "data correlation" to identify risks and vulnerabilities, and a platform to protect against threats and report on incidents - this data can be treated as SM	Consists of counts, risks, and statistics for security process management, and security situational awareness
RSA www.rsa.com	Offers eGRC (RSA Archer eGRC Suite) automation that identifies business risks and evaluates them through online assessments and metrics as well as reporting for incidents and audit management	Consists of counts, risks, and statistics for security process management, audits, and security situational awareness
McAfee www.mcafee.com/ca/	Compliance reporting, vulnerability assessment reporting, risk-based analytics, decision-support risk metrics (see quantitative metrics brochure from website)	Consists of counts, risks, and statistics for security process management, compliance management, security situational awareness, and decision making
Sophos www.sophos.com	Maintains metrics on malware, threats, and spam; operates dashboards for malware, threats, and spam	Consists of counts and statistics for security process management, security situational awareness, and dashboards

Table 6 shows that the nature of the security metrics used by each of the 18 vendors is roughly the same across all the vendors, differing from one another only by one or two uses of the metrics. This is not surprising since most of the metrics arise through SIEM product offerings. As well, the nature of these metrics is consistent with what is accepted within industry as to what and how security metrics should be applied, as described in the current two leading books [8][9] on security metrics.

The 29 information security vendors only represent a small portion of Canadian industry. However, since they are the vendors to Canadian companies, one can conclude that for the most part, Canadian companies will employ the same security metrics that are available from their vendors if they employ any security metrics at all. Data on how many Canadian companies employ security metrics is hard to come by, short of surveying the companies directly, and it was decided by the sponsors of this study that surveying was not feasible (for reasons of non-response since the surveys would be coming from government). However, the author found a reference to a joint study by Telus and the Rotman School of Management at the University of Toronto [10]

which presents the results of a 2011 survey of Canadian organizations on their IT practices. This publication offers the following information on SIEM deployment and the use of "business level" security metrics:

- Type of organization surveyed: Government: 14.79%, Private Company: 65.02%, Publicly Traded Company: 14.02%
- SIEM deployment in the next 12 months (all organizations): Limited Deployment: 16.23%, Full Deployment: 15.56%, Total: 31.79%
- Creating business-level security metrics (all organizations): Deploying: 9.3%, In Place: 22%, Total: 31.3%

The percentage of Canadian companies surveyed is the sum of the percentage of private companies surveyed and the percentage of publicly traded companies surveyed or 79.04%. Therefore, the percentage of Canadian companies surveyed that make use of business-level security metrics is 31.3% x 79.04% or 24.74%. "Business-level security metrics" are not defined in the Telus-Rotman report but they are probably security metrics that have been put in a business context and that are higher-level than metrics such as raw number of incidents, number of patches deployed, and so on (these are low-level metrics). Business-level security metrics would be data reported to management that are of interest to them and may be derived (aggregated) from the lower-level metrics. Examples of security metrics reported to management are: number of security assessments performed, exceptions to compliance policies, and status of active security projects [11]. Here, one security assessment may consist of a number of lower level assessments, and exceptions and statuses are of interest to management.

Unfortunately, there is no information on SIEM deployment in place, but assuming a conservative 10% of all organizations have SIEM in place, then the total SIEM deployment is 31.79% plus 10% or 41.79% of all Canadian organizations have SIEM in place. This yields 41.79% x 79.04% or 33.03% of all Canadian companies have SIEM.

Thus the contributions made by Canadian industry to the application of security metrics can be described as follows:

1. 18 of 29 (62.07%) of information security vendors examined that operate in Canada make use of security metrics in their products.
2. Canadian companies use security metrics consisting of counts, risks, statistics, and business-level data for security process management, compliance management, auditing, security situational awareness, decision making, and dashboards.
3. Since the metrics in item 2 are generated by SIEM technology and it is conservatively estimated that 33% of Canadian companies have SIEM technology, one concludes that 33% (conservative estimate) of Canadian companies use the metrics in item 2.
4. 25% of Canadian companies make use of business-level security metrics.

Figure 2 illustrates these results.

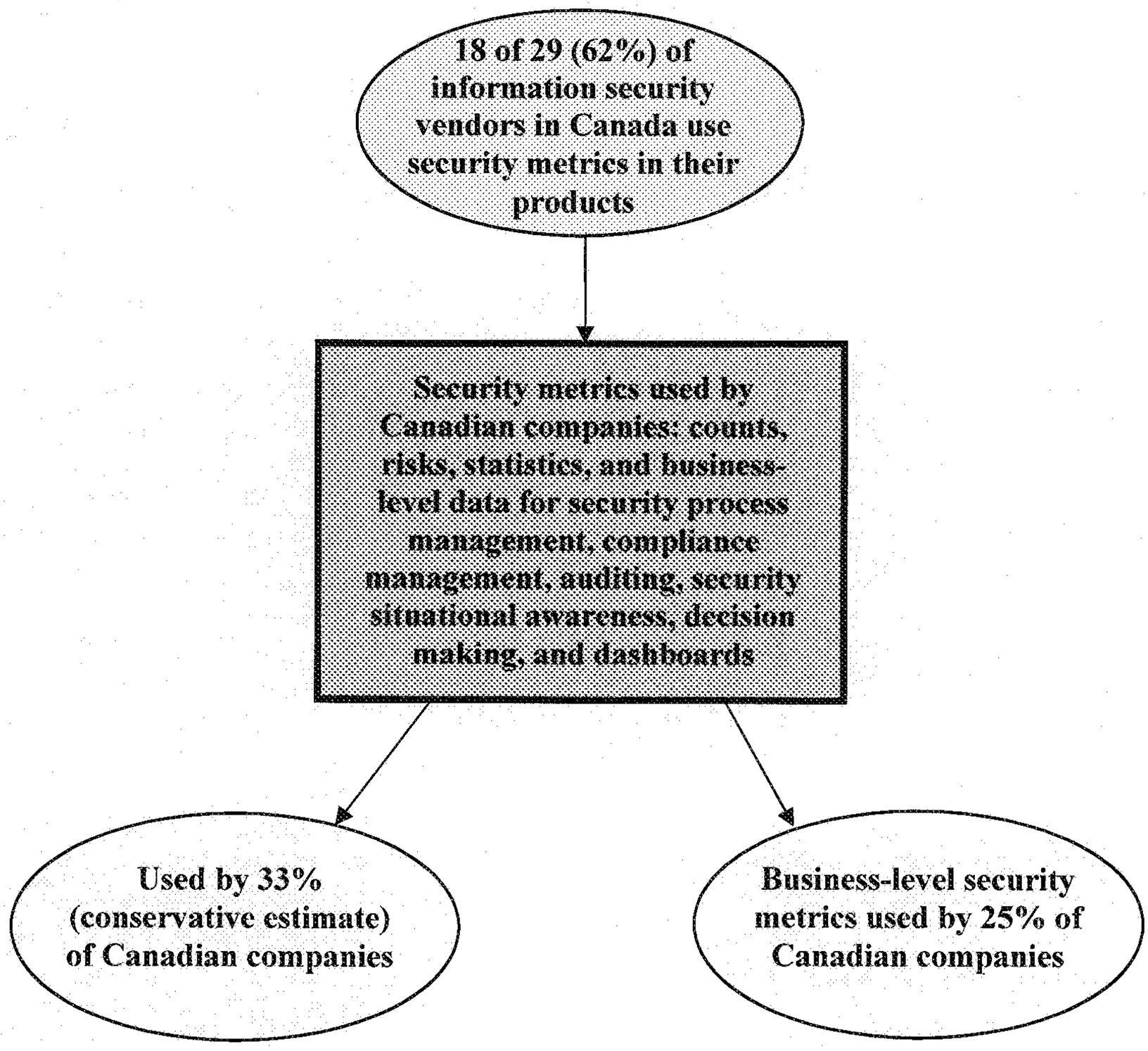

Figure 2- Contributions of Canadian industry to the application of security metrics

4 A Scientific Framework for Enterprise Cyber Security Metrics

The objectives of this chapter are to a) identify the elements of a scientific framework for enterprise cyber security metrics, b) describe the state of the art (SoA) and state of practice (SoP) within this framework, identifying the gaps between the SoA/SoP and what's theoretically possible, and c) identify which security metrics can be validated reliably in repeatable experiments, on what infrastructure, and which cannot. The scope of this chapter is limited to metrics that measure the security of the "cyber environment" as defined in Section 1.2.

4.1 A Scientific Framework for Enterprise Cyber Security Metrics (ECSM)

A scientific framework must be based on science. There are three interpretations of science that can be considered for cyber security metrics [12], as follows:

- Weak sense: science as the generalization and systematization of knowledge – for example, consider the body of knowledge within physics, where laws and descriptions of behaviour have been systematized and interwoven into an integral whole.

- Strong sense: science used to develop laws with which predictions can be made – for example, in physics, laws of motion have been developed and used to predict the future position of planets.

- Methodological sense: science used for research by forming hypotheses and proving or disproving the hypotheses with experiments. The results of the experiments must be confirmable by independent experimenters. Hence the experiments must be repeatable and yield the same results. This is the embodiment of the scientific method and established sciences have in fact been built up in this fashion.

Basing cyber security metrics on the weak sense of science is currently at best unknown as there has not been sufficient research to show that it is even possible outside of perhaps a highly specialized sub-area of security. Basing the metrics on the strong sense is likewise untenable since it is more likely that laws can be developed only after systematization of the knowledge, i.e. the strong sense is more likely after the weak sense has been established. This leaves the methodological sense, which is developed below into a framework for cyber security metrics.

4.1.1 Components of an ECSM Framework Based on the Methodological Sense of Science

It is envisaged that an ECSM framework based on the methodological interpretation of science would have the following components:

1. *A theory (hypothesis) of the enterprise cyber system's vulnerabilities, along with a metric for measuring the vulnerabilities representing the level of security.* For an example of

such a theory, consider a system that receives input from a user through port A, partially processes the input, and then forwards the rest of the input to another system for further processing through port B. Knowing this is how the first system treats user data, one could hypothesize or theorize that the first system has 2 vulnerabilities, one at port A and another at port B. A security metric would then be defined taking account of these 2 vulnerabilities to give a measure of the security of the first system.

2. *Test cases (experiments) to test the theory and the metric in item 1. A test case consists of a series of attacks against the system at a particular value of the metric, corresponding to a specific set of vulnerabilities, and designed to discover and take advantage of as many vulnerabilities as possible. A test case is successful if and only if the value of the metric remains the same after the test case is run (i.e. the vulnerabilities found result in the same value for the metric). An unsuccessful test case means that the theory or metric in item 1 needs to be revised and retested using new test cases corresponding to the revised theory. This is repeated until all test cases are successful, at which point the metric is declared sound.*

3. *A test case generator (model of attacker)*. A good test generator is essential but may be difficult to obtain [12]. The perfect generator would be one that behaves the way the most capable attacker would behave. This may be difficult to achieve but appears possible – think of IBM's Watson beating the best Jeopardy players. As well, it may be the case that the generator does not have to be perfect to be useful since it might be possible to show formally that not all possible test cases need to be run to validate a metric (for example, consider the proof technique known as mathematical induction).

4. *An implementation of the system, on which the tests in item 2 may be run. The implementation may be a model of the system, in which case the model must be as close to the real implementation as possible (low level), to avoid loss of details that may impact the results.*

5. *A formal specification language for specifying the tests, the system implementation under test, and the test environment in such a way that that these components can be identically duplicated by others, so that they can carry out the same testing on identical components to confirm the results (repeatability). Once the test results are confirmed by others, the metric is declared validated.*

For convenience, call this framework MSF (for Methodological Scientific Framework). Figure 3 illustrates the component interrelationships of MSF. A formal specification language is a means to achieve a rigorous, unambiguous, accurate description of the tests, the system implementation, and the test environment.

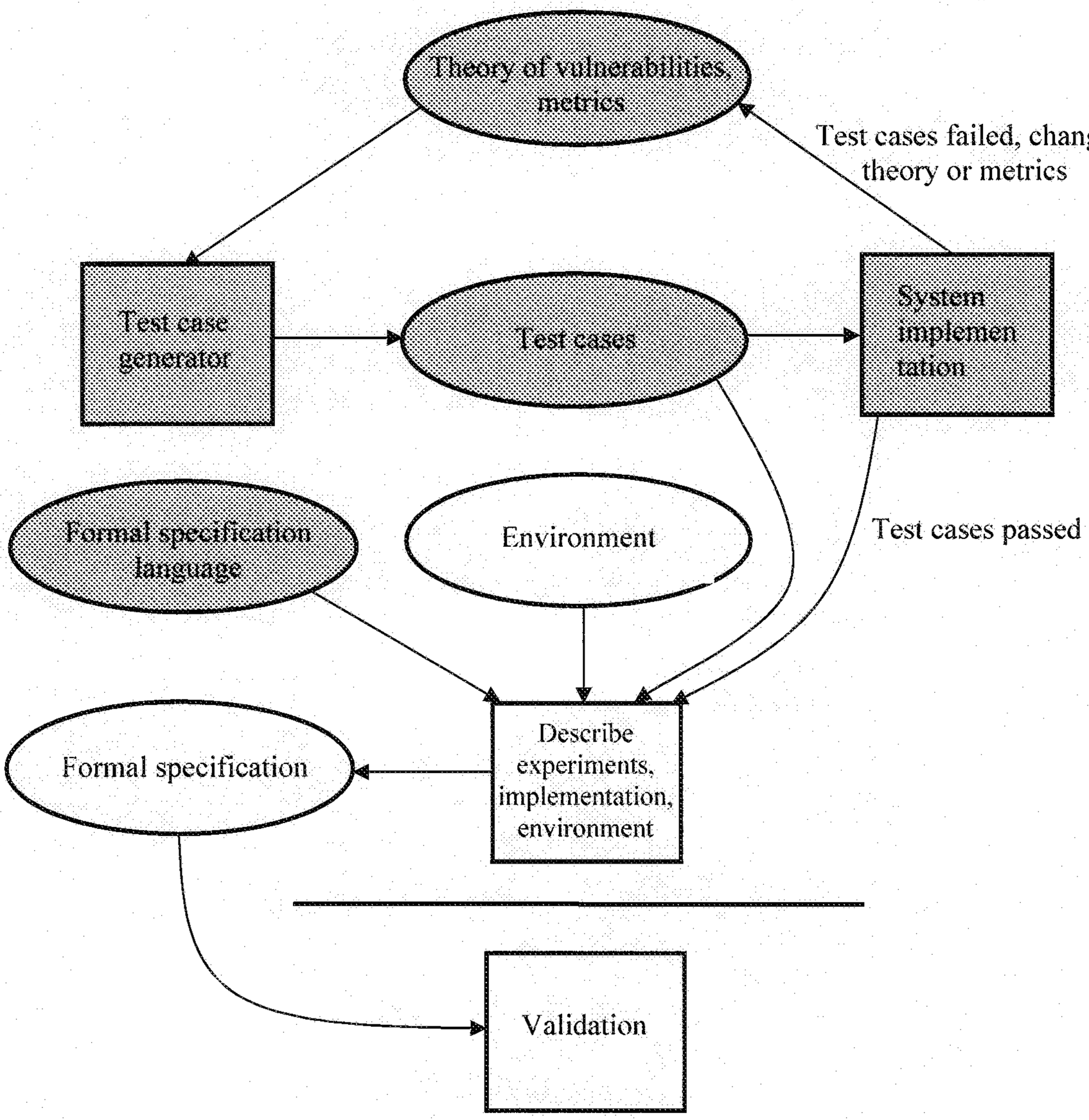

Figure 3- Component inter-relationships of MSF (MSF components in blue)

Table 7 compares the qualities of a cyber security metric governed by MSF to the requirements for a good cyber security metric, as described by Chapin and Akridge [1].

Table 7- Comparing MSF metrics to "good" cyber security metrics

Requirements of a Good Cyber Security Metric [1]	Cyber Security Metric Governed by MSF
Measure organizationally meaningful things	Yes – measures the security of the organization's cyber system
Reproducible	Yes – can be validated by others
Objective and Unbiased	Yes – the metric relates to a theory of vulnerabilities which is thoroughly tested – this testing should remove any possibility of bias or lack of objectivity
Measure progression toward a goal	Yes – can measure progressive improvements in security toward a security goal

As demonstrated by Table 7, a cyber security metric governed by MSF satisfies the requirements of a good metric as defined by [1].

4.1.2 The SoA/SoP Within the MSF

To determine the SoA/SoP within the MSF, the security metrics proposed in the papers of Table 1, Section B (Measuring the Security of a Cyber System) have been evaluated for adherence to the MSF and the results presented in Table 8. In Table 8, "Adherence to MSF" column, "implementation" can have values of "no", "low level", or "high level". Note that 3 publications from Table 1, Section B, namely B(1), B(2), and B(27) were excluded from this evaluation. The first two are the books that don't address the topic of scientifically based security metrics, and the last one is about software certification.

Table 8- Adherence of Table 1, Section B papers to MSF

Publication	Summary	Adherence to MSF
M. Howard, J. Pincus, J. Wing, "Measuring Relative Attack Surfaces", in *Computer Security in the 21st Century*, Springer, pp. 109-	Proposes "attack surfaces" as a measure of one system's security relative to another; an attack surface is described along 3 dimensions: targets and enablers,	Vulnerabilities theory: yes Metric defined: yes Test cases: yes Test cases generator: yes Formal spec. language: no

137, 2005. HPW2005.	channels and protocols, and access rights.	Implementation: low level Repeatable: yes Repeatable by others: no
M. Howard, "Attack Surface: Mitigate Security Risks by Minimizing the Code You Expose to Untrusted Users", 2004. How2004.	Practical advice to developers on how to reduce the attack surface of their code; based on actual Microsoft products such as Windows XP and Windows Server 2003.	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: no
L. Wang, A. Singhal, S. Jajodia, "Toward Measuring Network Security Using Attack Graphs", Proceedings of QoP'07, 2007. WSJ2007.	Proposes a framework for assessing the security of a network based on attack graphs or access paths for attack, e.g. given two networks, if one has more paths of attack than the other, it is the less secure of the two; references WJS2007 for attack resistance.	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: high level
S. Noel, L. Wang, A. Singhal, S. Jajodia, "Measuring security risks of networks using attack graphs," International Journal of Next-Generation Computing, Vol. 1, No. 1, pp 113-123, 2010. NWSJ2010	An expanded version of WSJ2007; provides a method for quantitatively analyzing the security of a network using attack graphs; the attack graphs are first populated with known vulnerabilities and likelihoods of exploitation and then "exercised" to obtain a metric of the overall security and risks of the network.	Vulnerabilities theory: yes Metric defined: yes Test cases: yes Test cases generator: yes Formal spec. language: no Implementation: high level Repeatable: yes Repeatable by others: no
L. Wang, S. Jajodia, A. Singhal, S. Noel, "k-Zero day safety: Measuring the security risk of networks against unknown attacks," Proc. 15th European Symposium on Research in Computer Security (ESORICS 2010), Springer-Verlag Lecture Notes in Computer Science (LNCS), Vol. 6345, 20-22 September, pages 573-587, 2010. WJSN2010.	Proposes "k-zero day safety" as a security metric that counts the number of unknown zero day vulnerabilities that would be required to compromise a network asset, regardless of what those vulnerabilities might be. The metric is defined in terms of an abstract model of networks and attacks. Algorithms for computing the metric are included.	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: high level
L. Wang, A. Singhal, S. Jajodia, "Measuring the overall security of network configurations using attack graphs," Proc.21st Annual IFIP WG 11.3 Working	Proposes an attack graph-based attack resistance metric for measuring the relative security of network configurations; incorporates two composition operators for computing the	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: high level

Conference on Data and Applications Security (DBSec 2007), Springer Lecture Notes in Computer Science, Vol. 4602, Steve Barker and Gail-Joon Ahn, eds., Redondo Beach, CA, pages 98-112, 2007. WJS2007.	cumulative attack resistance from given individual resistances and accounts for the dependency between individual attack resistances; referenced by WSJ2007 for attack resistance.	
L. Wang, T. Islam, T. Long, A. Singhal, S. Jajodia, "An Attack Graph-Based Probabilistic Security Metric", Proc. 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSEC 2008) , Springer-Verlag Lecture Notes in Computer Science (LNCS), Vol. 5094, pages 283-296, 2008. WILS2008.	Proposes an attack graph-based metric for the security of a network that incorporates the likelihood of potential multi-step attacks combining multiple vulnerabilities in order to reach the attack goal; the definition of the metric is claimed to have an intuitive and meaningful interpretation that is useful in real world decision making.	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: high level
A. Singhal, X. Ou, "Techniques for Enterprise Network Security Metrics", Fifth Cyber Security and Information Intelligence Research Workshop (CSIIRW '09), Knoxville, TN, USA, 2009. SO2009.	Presents an attack graph-based method for evaluating the security of a network based on likelihood of attack (similar to WILS2008); stresses the derivation of the metric based on composition of component vulnerabilities whose security levels are already known. This is a short paper with accompanying slides.	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: high level
M. Frigault, L. Wang, A. Singhal, S. Jajodia, "Measuring Network Security Using Dynamic Bayesian Network", Proceedings of QoP'08, 2008. FWSJ2008.	A Dynamic Bayesian Network (DBN) model is used to capture the dynamic nature of vulnerabilities that change over time. An attack graph is converted to a DBN by applying conditional probabilities to the nodes, calculated from the Common Vulnerabilities Scoring System (CVSS). The security of the network is calculated from the probabilities of the attacks being successful.	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: high level
M. Frigault, L. Wang, "Measuring Network Security Using Bayesian Network-Based Attack Graphs",	Proposes measuring network security using Bayesian network-based attack graphs so that relationships such as exploiting	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no

Annual IEEE International Computer Software and Applications Conference, 2008. FW2008	one vulnera-bility makes another vulnerability easier to exploit may be captured; differs from FWSJ2008 in that FWSJ2008 uses dynamic Bayesian networks whereas FW2008 uses just Bayesian networks; FWSJ2008 refers to FW2008 but not the other way around.	Formal spec. language: no Implementation: high level
L. Krautsevich, F. Martinelli, A. Yautsiukhin, "Formal approach to security metrics. What does 'more secure' mean for you?", Proceedings of ECSA 2010, 2010. KMY2010.	Initial proposal and analysis of a number of mathematically-based definitions of security metrics such as "number of attacks", "minimal cost of attack", "maximal probability of attack", and even "attack surface" of HPW2005.	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: no
C. Wang, W. Wulf, "Towards a Framework for Security Measurement", Proceedings of 20th National Information Systems Security Conference, 1997. WW1997.	Proposes an initial framework for estimating the security strength of a system by decomposing the system into its security sensitive components and assigning security scores to each component; aggregate the component scores to get an estimate for the security strength of the system.	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: high level
P. Halonen, K. Hätönen, "Towards holistic security management through coherent measuring", Proceedings of ECSA 2010, 2010. HH2010.	Discusses the problems of applying security metrics to telecommunication systems; compares security metric taxonomies, and discusses the need for security impact metrics; presents a broad view of security metrics.	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: no
D. Mellado, E. Fernández-Medina, M. Piattini, "A Comparison of Software Design Security Metrics", Proceedings of ECSA 2010, 2010. MFP2010.	A survey of various security metrics and standards that may be applicable to software design; compares the relevance of the various approaches to security properties such as authenticity and confidentiality.	Vulnerabilities theory: no Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: no
J. Wang, H. Wang, M. Guo, M. Xia, "Security Metrics for Software Systems", Proceedings of ACMSE '09, 2009. WWGX2009.	Presents a security metrics formulation in terms of weaknesses and vulnerabilities, rated by CVSS scores for CVE vulnerability names; does not show how one would determine such scores for a brand new piece of software; not clear how the final	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: low level

	security metric can be used to improve security.	
R. Scandariato, B. De Win, W. Joosen, "Towards a Measuring Framework for Security Properties of Software", Proceedings of QoP '06, 2006. SDJ2006.	Claims that software has security properties that can be measured, much like it has maintainability properties such as complexity; proposes a number of software security properties along with corresponding metrics.	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: no
O. Saydjari, "Is Risk a Good Security Metric?", Panel, Proceedings of QoP'06, 2006. Say2006.	Succinct descriptions of risk as a security metric, alternative security metrics, and what makes a good metric.	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: no
Z. Dwaikat, F. Parisi-Presicce, "Risky Trust: Risk-Based Analysis of Software Systems", Proceedings of SESS'05, 2005. DP2005.	Proposes an approach to evaluate the security of a software system in development; security requirements are derived and a method is given for evaluating the likelihood of requirements violation based on the individual risks of system components.	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: high level
Y. Liu, I. Traore, A.M. Hoole, "A Service-oriented Framework for Quantitative Security Analysis of Software Architectures", Proceedings of 2008 IEEE Asia-Pacific Services Computing Conference, 2008. LTH2008.	Proposes a User System Interaction Effect (USIE) model for systematically deriving and analyzing security concerns in service oriented architectures. The model is claimed to provide a foundation for software services security metrics and one such metric is defined and illustrated.	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: high level
Y. Liu, I. Traore, "Properties for Security Measures of Software Products", Applied Mathematics & Information Sciences, I(2), pp. 129-156, 2007. LT2007.	Describes and formalizes properties that characterize security-related internal software attributes; these properties form a framework that can be used to rigorously identify and evaluate new security metrics; this framework is claimed to be sound but not complete; the properties are claimed to be necessary but not sufficient conditions for good security metrics.	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: no
Y. Liu, I. Traore, "UML-based Security Measures of Software Products", Proceedings of International	Proposes the USIE model mentioned above for LTH2008 (probably first publication of the model) and derives it from UML	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no

Workshop on Methodologies for Pervasive and Embedded Software (MOMPES'04), 2004. LT2004.	sequence diagrams; this model can be used as a basis for architectural level security metrics and as an example, confidentiality metrics are defined based on the model.	Formal spec. language: no Implementation: high level
E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, W. Robinson, "Performance Measurement Guide for Information Security", NIST SP 800-55, Revision 1, 2008.	Provides guidelines for developing, selecting, and implementing information system level and security program level measures for assessing the implementation, performance, and impact of security controls and other security related activities.	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: low level
"Recommended Security Controls for Federal Information Systems and Organizations", NIST SP 800-53, 2009.	Describes recommended security controls; includes risk assessment as a control; this publication is used by the "Performance Measurement Guide for Information Security" as a basis for developing security measures.	Vulnerabilities theory: yes Metric defined: no Test cases: no Test cases generator: no Formal spec. language: no Implementation: no
T.E. Hart, M. Chechik, D. Lie, "Security Benchmarking Using Partial Verification", Proceedings of HotSec 08, 2008. HCL2008.	Proposes quantifying insecurity using the partial results of verification attempts - instrumented code (assertions) is property checked until a failure is found. The aggregate of such failures determine the level of insecurity of the software.	Vulnerabilities theory: yes Metric defined: yes Test cases: no Test cases generator: no Formal spec. language: no Implementation: low level

Table 8 offers the following insights:

1. No proposed cyber security metric fully adheres to the MSF. Therefore no proposed metric can be said to be scientifically based in the methodological interpretation of science.

2. There are 2 metrics that come the closest to being methodological science based, namely "attack surface" (paper B(3)) and "attack graphs" (paper B(6)). They both have all the MSF components except for the "formal specification language" and the "repeatable by others" (a consequence of not having the language). However, attack surface has a low level implementation and is therefore preferred over attack graph, which has a high level implementation. In addition, it is clear that a suitable language could be added, which would make these metrics fully compliant with MSF and hence qualify them to be termed "scientifically based".

3. Many of the metrics in Table 8 have only the components "Vulnerabilities theory", "Metric defined", and "Implementation". This is typical of security metrics papers that do not concern themselves with basing metrics on science. These papers proceed through the steps of describing vulnerabilities (Vulnerabilities theory), proposing metrics to measure

the vulnerabilities (Metric defined), and showing how their metrics can be evaluated (Implementation).

4. Excluding the two metrics in item 2 above, none of the remaining metrics have the components "Test cases", "Test cases generator", and "Formal spec. language". The lack of these components, which are key for being scientifically based, is primarily responsible for failing to conform to MSF.

Table 8 represents the SoA/SoP among cyber security metrics proposed for measuring the security of enterprise cyber systems. Based on Table 8 and the MSF, the gaps between the SoA/SoP and what's theoretically possible (MSF) are:

- Lack of a formal specification language for describing the experiments, the system, and the environment,
- Lack of a sufficiently powerful test case generator (attacker model) that could generate all the test cases needed to reflect the behaviour of the perfect attacker,
- Lack of an implementation that is generally applicable and sufficiently low level to avoid the loss of system detail that could lead to loss of security through side channel leakage. Low level implementations exist for specific cases as seen in Table 8. However, there is no low level implementation that can be used in all cases and that is guaranteed to be sufficiently low level to avoid the side channel leakage.

The lack of a formal specification language can be overcome in a relatively straight forward fashion, through establishing a committee to call for and review proposals for one. There are several precedents for formal description languages that can be used as starting points, e.g. VDM[e]. The remaining two gaps are much harder to overcome. Currently there is no consensus that a perfect attacker model is even possible. As for the low level implementation, how does one show that an implementation is generally applicable and sufficiently low level to avoid potential side channel attacks, especially given that it would depend on knowing about unforeseen vulnerabilities? We may have to forego the generality, treating implementations on a case by case basis, and strive for as low level as possible. As for the perfect attacker model, probably the only recourse we have is to embed into the attacker model as much information about attacker behaviour as we know, perhaps through reviews of past attacker behaviour. In addition, the size of the problem may be reduced by the fact that certain attack patterns may be ruled out given the constraints imposed by the system under attack. For example, if the system does not accept email, then all attacks that use email to deliver a malware payload can be ruled out.

4.1.3 Validation of Security Metrics By Repeatable Experiments

The following conditions determine whether or not experiments for evaluating cyber security metrics are "repeatable" and "repeatable by others":

Repeatability Condition *(Necessary and Sufficient): Experiments for evaluating a security metric are repeatable if and only if the experiments, the system implementation on which the experiments*

[e] "Specification language", accessed Mar. 25, 2012 at: http://en.wikipedia.org/wiki/Specification_language

are carried out, and the environment in which the experiments are carried out are all identical to those of the original experiments. Experiments for which this condition holds are termed "repeatable".

Repeatable by Others Condition *(Necessary and Sufficient): Experiments for evaluating a cyber security metric are repeatable by others if and only if i) there exists a formal specification language or some form of unambiguous accurate description capability that is used to describe the original experiments, the original system implementation, and the original environment so that they may be identically duplicated by others for use in repeating the experiments, and ii) the Repeatability Condition holds.*

Definition of Validation*: A cyber security metric is validated if experiments for evaluating it are repeatable by others, who after repeating the experiments obtain the same results as obtained by the original experimenters.*

The infrastructure required for the Repeatability Condition consists of the identical experiments, the identical system implementation, and the identical environment. Identical environment means an environment that is identical to the original hardware and software environment of the system, including any other programs that were executing at the time of the original experiments along with their input and output. The infrastructure required for the Repeatable by Others Condition is the same as for the Repeatability Condition plus the accurate description capability.

In the absence of the accurate description capability, the Repeatability Condition degenerates into the trivial case, in which the experiments are repeated on the original infrastructure by the original experimenters. Note that "repeatable by others" means repeatable by others on identical infrastructure, not on the same infrastructure as used for the original experiments.

The Repeatable by Others Condition can be related to MSF using the following theorem:

Theorem (Validation Using MSF)*: A cyber security metric adhering to MSF can be validated.*

Proof*: MSF satisfies the Repeatable by Others Condition.*

For this theorem, "adhering to MSF" means "identifiable to the same components as MSF" as demonstrated in Table 8.

The above conditions and theorem can be used to evaluate whether or not a proposed security metric is repeatable by others. Security process metrics such as number of alerts, number of employees with security training, or number of patches successfully applied are non-repeatable according to the Repeatability Condition, since the system (security process) and the environment are non-reproducible. Hence they also cannot be validated. Cyber security metrics that adhere to MSF are repeatable by others. In general, cyber security metrics are repeatable by others if the Repeatable by Others Condition holds for them. None of the metrics in Table 8 are repeatable by others since they all lack the accurate description capability.

5 Conclusions and Recommendations

This study has looked at the topic of cyber security metrics in terms of contributions to the topic from world research, Canadian university research, and Canadian industry. Based on the results of the study, the following conclusions can be drawn:

- There is little research on cyber security metrics from Canadian universities, but the research that is conducted concerns measuring the security of a cyber system.

- Canada's university research on cyber security metrics is comparable to that of the United States. However, on a per university basis, Canada does more research on cyber security metrics than the United States due to the much higher number of American universities.

- Excluding the United States, Canada does more research on cyber security metrics than the rest of the world.

- Canadian companies use cyber security metrics generated by SIEM technology, including counts (e.g. count of security alerts), risks, statistics, and business-level metrics.

- About a third of Canadian companies use SIEM technology and therefore use the metrics in the previous point.

- MSF can be the scientific basis of enterprise cyber security metrics.

- Due to the lack of a formal specification language for specifying experiments, system implementations, and environments, none of the cyber security metrics studied can be independently validated by others.

- At least 3 scientific gaps exist between the SoA/SoP and what is theoretically possible (MSF / Repeatability). The lack of a formal specification language gap is more easily remedied than the gap of a sufficiently powerful test case generator and the gap of a sufficiently low level implementation.

- Cyber security metrics are repeatable by others if they satisfy the Repeatable by Others Condition. Metrics that are not repeatable by others include Security process metrics such as number of alerts, number of employees with security training, or number of patches successfully applied, since the system (security process) and the environment are non-reproducible. It follows that these metrics also cannot be validated.

- Cyber security metrics that adhere to MSF are repeatable by others.

- SIEM technology is a promising base from which to build a security dashboard that monitors the security state of a cyber system in real time and aid or automate responses to security alerts. Annex A discusses the viability of SIEM technology for this purpose.

Recommendations for future work are as follows:

- Promote research in scientifically based cyber security metrics in order to tackle the scientific gaps identified above.

- Further develop MSF, including the test case generator, the formal specification language, and the low level implementation, e.g. use MSF to develop a cyber security metric.

- Write a paper on the results of the previous point and submit it for peer review.

- Draw up requirements for a security dashboard. Map these requirements to existing SIEM technology, and determine what additional steps are needed to build the dashboard.

References

[1] D. Chapin, S. Akridge, "How Can Security Be Measured?", Information Systems Control Journal, Vol. 2, 2005.

[2] DRDC-CSEC, Statement of Work, file "SoW – DRDC-CSEC Metrics Final.pdf" on the sharepoint.

[3] Macleans.ca, "Maclean's 2011 University Rankings", accessed Jan. 28, 2012 at: http://oncampus.macleans.ca/education/2011/10/26/macleans-2011-university-rankings-2/

[4] University of Waterloo, "Canadian Universities", accessed Jan. 28, 2012 at: http://uwaterloo.ca/canu/

[5] Branham Group Inc., "Top 10 Canadian ICT Security Companies", accessed Feb. 18, 2012 at: http://www.branham300.com/index.php?year=2011&listing=8

[6] Industry Canada, "ICT Security and Canada: The Future is Here", PDF document "Iu64-34-3-2006E.pdf" downloaded Feb. 18, 2012 from: http://publications.gc.ca/site/eng/301343/publication.html

[7] Industry Canada, "IT Security and Canada: The Future is Here", PDF document "Iu64-34-3-2008E.pdf" downloaded Feb. 18, 2012 from: http://publications.gc.ca/site/eng/330760/publication.html

[8] Andrew Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt, Addison-Wesley, 2007.

[9] Lance Hayden, IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data, McGraw-Hill Osborne Media, June 2010.

[10] "2011 Executive Briefing: Telus-Rotman Joint Study on Canadian IT Security Practices", retrieved Mar. 20, 2012 from: http://promo.telus.com/manage_risk/2011/survey/

[11] Ramon Krikken, "Field research: Security Metrics Programs", Burton Group, 2009. Retrieved Mar. 21, 2012 from the Internet (link too long to include here). Included on the sharepoint as file Kri2009.

[12] S. Stolfo, S. Bellovin, D. Evans, "Measuring Security", IEEE Security & Privacy, May/June 2011. On the sharepoint as file SBE2011.

Annex A Security Information and Event Management (SIEM) Technology

According to Wikipedia, SIEM technology "provides real-time analysis of security alerts generated by network hardware and applications. SIEM solutions come as software, appliances or managed services, and are also used to log security data and generate reports for compliance purposes"[f]. The same Wikipedia page also gives the following list of SIEM capabilities:

- "**Data Aggregation:** SIEM/LM (log management) solutions aggregate data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.
- **Correlation:** looks for common attributes, and links events together into meaningful bundles. This technology provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information.
- **Alerting:** the automated analysis of correlated events and production of alerts, to notify recipients of immediate issues.
- **Dashboards:** SIEM/LM tools take event data and turn it into informational charts to assist in seeing patterns, or identifying activity that is not forming a standard pattern.
- **Compliance:** SIEM applications can be employed to automate the gathering of compliance data, producing reports that adapt to existing security, governance and auditing processes.
- **Retention:** SIEM/SIM solutions employ long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance requirements."

This study is interested in the possibility of using SIEM technology as a base upon which to build a security dashboard that displays security alerts and responds to the alerts by either suggesting corrective action, automatically taking corrective action (depending on the action) or both. It appears from the above list of SIEM capabilities, that the "alerting" and "dashboard" capabilities map directly to the security dashboard's display of security alerts, and that the "data aggregation" and "correlation" capabilities map directly to the security dashboard's suggesting or taking of corrective action. Thus it does seem viable to use SIEM technology as the base to build the security dashboard. Additional research is required to determine what cyber security metrics should be used to trigger the security alerts. As well, research is needed to know how to construct the security dashboard's corrective action engine, which may be built using artificial intelligence techniques. The construction of the security dashboard based on SIEM technology appears feasible.

[f] "Security information and event management", accessed Mar. 27, 2012 at: http://en.wikipedia.org/wiki/Security_information_and_event_management

This page intentionally left blank.

Distribution list

Document No.: DRDC Ottawa CR 2012-109

LIST PART 1: Internal Distribution by Centre

1 Scientific authority
2 Cyber Operations Section
2 Library

5 TOTAL LIST PART 1

LIST PART 2: External Distribution by DRDKIM

3 Library and Archives Canada
1 DRDKIM
1 Guy Turcotte, DRDC Valcartier
1 Melanie Bernier, CORA
5 George Yee, Office of the Privacy Commissioner of Canada
112 Kent Street, Ottawa, ON K1A 1H3
4 Dan Craigen, Communications Security Establishment Canada

15 TOTAL LIST PART 2

20 TOTAL COPIES REQUIRED

This page intentionally left blank.

s.19(1)

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

George Yee

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

The state and scientific basis of cyber security metrics: Including Canadian perspectives

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

George Yee

5. DATE OF PUBLICATION (Month and year of publication of document.)

October 2012

6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)

62

6b. NO. OF REFS (Total cited in document.)

12

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contract Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Defence R&D Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)

43ga01

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

W7714-4500883510

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

310312

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

DRDC Ottawa CR 2012-109

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

This report describes a study on the state of enterprise cyber security metrics in terms of contributions from international research, Canadian university research, and Canadian industry. The study finds that very little published research exists on cyber security metrics compared to related fields such as information security, and existing research lacks scientific rigour. Furthermore, use of cyber security metrics by industry appears to be mostly limited to security information and event management (SIEM) software. This report proposes a scientific framework to provide a firm basis for the analysis of current and future cyber security measures and metrics. The report evaluates the state of the art (SoA) and state of practice (SoP) of published cyber security metrics using the proposed scientific framework, and identifies gaps between the SoA/SoP and what is theoretically possible. The report concludes with a summary of the study results and gives recommendations for future work. In addition, an annex is included that describes the viability of basing a security dashboard on current SIEM technology.

Ce rapport décrit une étude portant sur l'état des mesures de la cybersécurité d'entreprise en fonction des travaux de recherche exécutés à l'étranger, dans les universités canadiennes, et des applications dans l'industrie canadienne. L'étude a permis de démontrer que très peu de travaux de recherche ont été publiés sur les mesures de la cybersécurité par rapport à d'autres domaines connexes comme, par exemple, la sécurité de l'information. On a constaté également que les travaux de recherche existants manquaient de rigueur scientifique. En outre, l'industrie semble avoir recours aux mesures de la cybersécurité presque uniquement à l'égard des logiciels de gestion des événements et des renseignements sur la sécurité (SIEM). Le présent rapport propose un cadre scientifique qui servira de base solide pour l'analyse des mesures et des paramètres actuels et futurs en matière de cybersécurité. Le rapport évalue l'état des connaissances et l'état de la pratique relativement aux travaux sur les mesures de la cybersécurité publiés au moyen du cadre scientifique proposé. Il recense aussi les écarts entre l'état des connaissances/état de la pratique et ce qui est théoriquement possible. En conclusion du rapport, on présente un résumé des résultats de l'étude et des recommandations de travaux de recherche à entreprendre dans l'avenir. De plus, il comporte une annexe abordant la viabilité d'un tableau de bord de la sécurité basé sur la technologie SIEM actuelle.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

cyber security; measures; metrics; survey; Canadian industry; Canadian academia