Security Excellence: Fusing Security Metrics into a Business Excellence Model

Clemens Martin, University of Ontario Institute of Technology, Canada; E-mail: Clemens.Martin@uoit.ca
Anasuya Bulkan, University of Ontario Institute of Technology, Canada; E-mail: Anasuya.Bulkan@mycampus.uoit.ca

ABSTRACT

The European Foundation for Quality Management's Excellence Model is a highly recognized business framework that has been implemented in many European countries to achieve Business Excellence. It is a documented approach to determine the overall Total Quality Management (TQM) practices of an organization by assessing nine different criteria. Conversely, the US National Institute of Standards and Technology (NIST) has outlined a set of security metrics that are categorized into managerial, operational and technical controls that can be used to express the security posture of an organization. In this paper, we propose to integrate these two domains to produce a comprehensive security framework based on underlying TQM practices and principles. Hence, we have created security metrics that are more accurate in reflecting the holistic state of a business and all its important aspects including IT security aspects that were not formally considered before.

Keywords: TQM, EFQM, NIST controls, security metrics, business excellence

1. INTRODUCTION

According to the 2006 Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) survey, a total estimated loss of US $52,494,290 was recorded for common types of security attacks. This is indicative of the vital role of security in an IT infrastructure when it comes to thwarting threats and attacks that can result in significant damage. IT security must also be addressed in order to comply with legal stipulations. For example, in the US, there must be compliance with HIPAA, FISMA and Sarbanes-Oxley while on the Canadian side, laws like PIPEDA must be abided by or stiff legal penalties could arise. There are also social and ethical obligations that have to be taken into consideration, surrounding privacy and confidentiality issues. If these considerations are overlooked then loss of reputation can result and a loyal customer base can also be destroyed (Calder, 2005).

A critical review on whether business productivity is facilitated by Information Technology (IT) investments in general has been performed by (Dedrick, Gurbaxani, & Kraemer, 2003), which established that there are indeed higher increases in productivity for both manufacturing and service sectors. Empirical results that were gathered in a production environment also support the claim that there is a payoff for investing in Information Technology (Gurbaxani, Melville, & Kraemer, 1998). In addition, (Martinez-Lorente, Sanchez-Rodriguez, & Dewhurst, 2004) performed an analysis of whether IT has an effect on TQM based on key elements from the European Quality Award- instituted by the European Foundation for Quality Management- and the Malcolm Baldrige Award, which reflect quality management and assurance principles. The analysis revealed that large industrial firms that actively support TQM do recognize that IT plays an important role in achieving the desired results of the TQM implementation.

It is therefore imperative that IT security be addressed as a paramount concern since it contributes to business productivity by ensuring that the IT investments and infrastructures are secure at a level that is acceptable to the business environment. By taking the security domain into account, we are a step closer to our synergistic model of Total Quality Management, which can be viewed as an integral approach for improving an existing framework of processes, where goods and services are delivered to customers based on their expectations and the societal impacts are also considered (Nasierowski, 1997).

IT security mitigates business risks by allowing the smooth functioning of daily activities, resulting in an increased possibility of productivity goals being achieved. It is however, primarily up to top-level management to decide the appropriate security levels for their environments (Michaelsen, Michie, & Boulanger, 1985). If this claim that management should determine the amount of emphasis to be placed on security is correct, then it is worthwhile to determine how much cost should be associated with these security investments.

There have been several proposals for measuring the associated costs which include a Cost Benefit Analysis or Return on Investments (ROI) approach which weighs the risks in relation to the value of assets to produce a quantitative measure (Mercuri, 2003) (Erkan, 2005). It is also a more suitable and relevant approach when it comes to clearly projecting business risks (Jorma & Reijo, 2005). Similarly, a scorecard can be used to model the Return on Investments in order to highlight the benefits of security investments when compared to potential business risks (Banker, Chang, Janakiraman, & Konstans, 2004). It has also been suggested that a Cost Benefit Analysis is an improvement over value-neutral models since it is more persuasive in convincing management that business productivity is facilitated by security investments (Michaelsen et al., 1985) . We agree with this claim and have, therefore, incorporated security metrics into an underlying business framework that already evaluates the return on business investments to determine if a business is successful or not.

By taking this one step further, the security posture of an IT infrastructure is investigated to determine the necessary adjustments that are made to steer the business on the path to excellence. Subsequently, we must have a convergence on what a metric or a measurement should entail: it is Specific, Measurable, Attainable, Repeatable, and Time-dependent (SMART). It is distinguished from a measurement- a single snapshot in time that reflects a certain state- by performing an analysis of the recorded data over time to an accepted baseline (Shirley, 2002). Metrics will be based on IT security goals and objectives and will be, "tools designed to facilitate decision-making and improve performance and accountability through collection, analysis and reporting of relevant performance-related data." (Swanson & Bartol, Nadya et al, 2003). This indicates that the performance-related data is dependent on the specific system and a different combination of the Confidentiality, Integrity and Availability principle will be a security requirement. For instance, governmental and military operations will be more inclined for a higher ratio of confidentiality measures while a commercial enterprise might be more interested in availability principles.

Developing security metrics that accurately produce quantitative results can be a disconcerting task with the level of subjectivity involved. Service Level Agreements had been investigated in the hopes of providing a more quantitative solution to this problem (Henning, 2000). Here, the authors presented different service levels which have distinct, associated cost metrics. In this context, security was investigated to deduce whether it can be represented as a Service Level Agreement by exploring four criteria for metrics: temporal (to be met within a specific time period), performance (tangible delivery of materials), functional (adjustments to systems for normal operations) and process-related (recurring tasks) metrics. However, while this approach to security metrics is important to note, it does not replace assurance methods but instead, defines a set of security-oriented practices for functional operations.

It was further proposed that security metrics should be based on a framework that is already in place or familiar to the organization in order to foster acceptance and widespread understanding of the new security paradigm (Shirley, 2002). As a result, our research aims to progress in this direction by relying on the foundations set, primarily by the European Framework for Quality Management and the US National Institute of Standards and Technology (NIST) in order to capture an

accurate security representation of the state of a business, relative to its existing strategy and goals. We believe that this approach also extends into a broader Total Quality Management solution since the security aspects of an IT infrastructure are also deemed to be important. The EFQM has been chosen based on its wide acceptance and holistic integration of all important business domains while the security controls have been selected based on the US's NIST documents that aim to deduce the security posture of a business.

2. EXISTING MODELS AND STANDARDS

There are numerous existing models that facilitate security evaluation and assurance. The Common Criteria (CC) comprises the ITSEC (*Information technology security evaluation criteria (ITSEC)*1991), TCSEC (Orange Book) and CTCPEC(*Canadian trusted computer product evaluation criteria*1993) while the SSECCM is another important model that can be used throughout the software product lifecycle (Jelen, 2001).

The Orange Book was developed for the Department of Defense in 1985 by the US to apply metrics that determine confidentiality levels of their security systems. On the contrary, the ITSEC was introduced by the UK where a Target of Evaluation has different evaluation levels where there are set security objectives that fit into these levels; the CTCPEC is the Canadian version which provides a guide to evaluate the assurance levels of objects that have certain rights and privileges (Bacic & Robison, 1993). The concerted culmination of these three models into the Common Criteria, focuses on preventing the insecure event from a technical level. In contrast, the Information Security Management System (ISMS) encompasses the BS7799 1995 as a specification and is deemed to be a management model suited for the real world(Brewer, 2005).The ISMS was modified into the ISO/IEC 17799:2000 and later updated as ISO/IEC 17799:2005 where requirements and prescribed roles and responsibilities are better explained. The framework is suited for risk assessment and building management controls (*ISMS standards overview.*2006). In fact, "A mix of aspects such as policies, standards, guidelines, codes-of-practice, technology, human issues, legal and ethical issues constitute an ISMS" (Eloff & Eloff, 2003).

The US National Institute of Standards and Technology is another authority that focuses on the development of security metrics. There are three control areas that are proposed- management, operational and technical controls that contain metrics that can be aggregated into other metric sets as deemed appropriate (Figure 1). This will further be discussed in the following sections. Questionnaires are provided for these critical elements which result in a quantitative measurement being assigned such as a percentage or an average number(Swanson, 2003) .Furthermore, the European Framework for Quality Management is a model that places emphasis on all aspects of a business framework by addressing the non-financial factors- for instance, recognizing the societal impact of its operations(Westlund, 2001) as well as ethical implications (Martín-Castilla, 2002) in the quest for business excellence.

By integrating security metrics into a TQM business model, a solution is created to address business strategy (corporate governance and policy), technology management (utilizing the accepted standards) as well as the management of legal and human-related issues (Eloff & Eloff, 2003). Similarly, Jorma & Reijo (2005) acknowledged the use of business models such as the Malcolm Baldrige model and the EFQM evaluation criteria to measure performance in these areas and noted that IT modeling should be present as well.

3. BUSINESS EXCELLENCE AND THE EFQM

In order for an organization to be a good corporate citizen, it must consider non-financial factors to deliver the required results to customers, the environment and society. In fact, this is increasingly achieved by using a TQM approach (Sciarelli, 2002). Business Excellence (BE) is a holistic concept, also representative of a TQM approach by considering all aspects that have non-financial and/or financial repercussions. Metrics for the non-financial aspects cater for domains that revolve around customers, society and employees. In contrast, financial metrics strive to measure the dollar earnings for the business relative to production goals (Westlund, 2001). On this note, we propose that security excellence is an extension of business excellence by blending the existing requirements of a business- whether being financial, legal or ethical domains- with the necessary security mechanisms to protect critical business information, resources and operations. It is not an add-on feature and should not be isolated from a business framework. Thus, with respect to its integration into the EFQM, there are proposed levels of fusion that can occur at the nine different domains of the EFQM model and these can be assessed or measured at periodic intervals. The **Enablers** in turn produce **Results** which are measured according to a set evaluation process (European Framework for Quality Management, 2003) (Figure 2). It should be noted that these assessments do not replace Risk assessments but instead include them as subset of the metric control sets that will be used in the evaluation process. Refer to the NIST controls which include Risk Assessments as a control set in Figure 1.

The EFQM is a highly recognized model that was formed in 1988 and has grown over the years with applications across a wide variety of sectors including health care (Perides, 2002) and educational settings (Saraiva, Rosa, & Orey, 2003). As a case in point, it was adopted by a University Medical Centre in the Netherlands after an initial implementation of an ISO 9000 system failed to meet their needs. Over time, the system was unable to cope with the integration of all aspects of the University setting in a holistic manner. As a result, the move was made to adopt the EFQM, one of the reasons being the inclusion of a continuous improvement process in its TQM principles (Geraedts, Montenarie, & van Rijk, 2001). As a result, the EFQM model has been chosen as a foundation for our Business Excellence extension because of its inherent feedback process that allows continuous innovation and improvements, which contribute to the business being sustainable and competitive over time. In addition, it encompasses a systemic integration of all business aspects that we also consider to be significant. It however, lacks a security component and this may be due to the period of time in which it was formed since security concerns were not a top priority in the business operations as compared to the shift in focus that they are currently experiencing. We firmly believe that security is an integral component that needs to be included and a security excellence paradigm is obtainable by transcending one step further to include this domain.

4. SECURITY EXCELLENCE

We will use the US National Institute of Standards and Technology's metric sets, which are used to evaluate the security of a business to perform an integrative assessment of the Business excellence aspects. As a result of the different EFQM domains that are present, the NIST metrics have been categorized under **Policy**, **Leadership** and **Process** metric sets to demonstrate their appropriate assessments and integration into the EFQM framework. The NIST metrics have been grouped into the appropriate categories based on their inherent characteristics and dominant factors. For instance, the **Risk management control** forms part

Figure 1. Puzzle of NIST controls hat can be aggregated into different metric sets

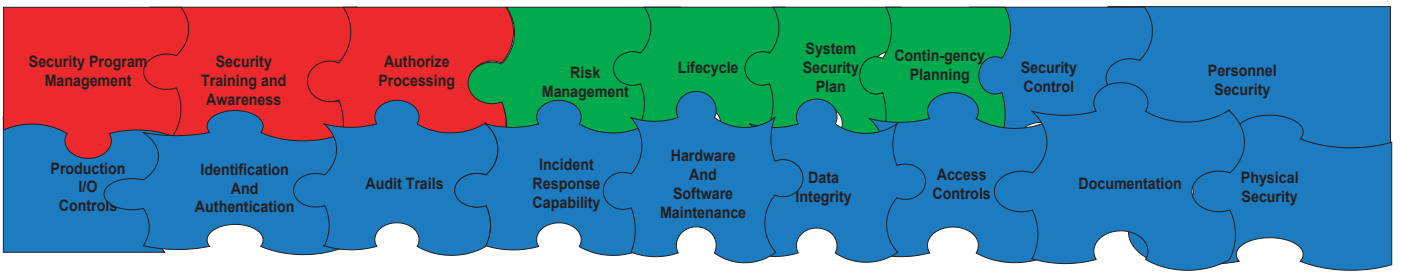
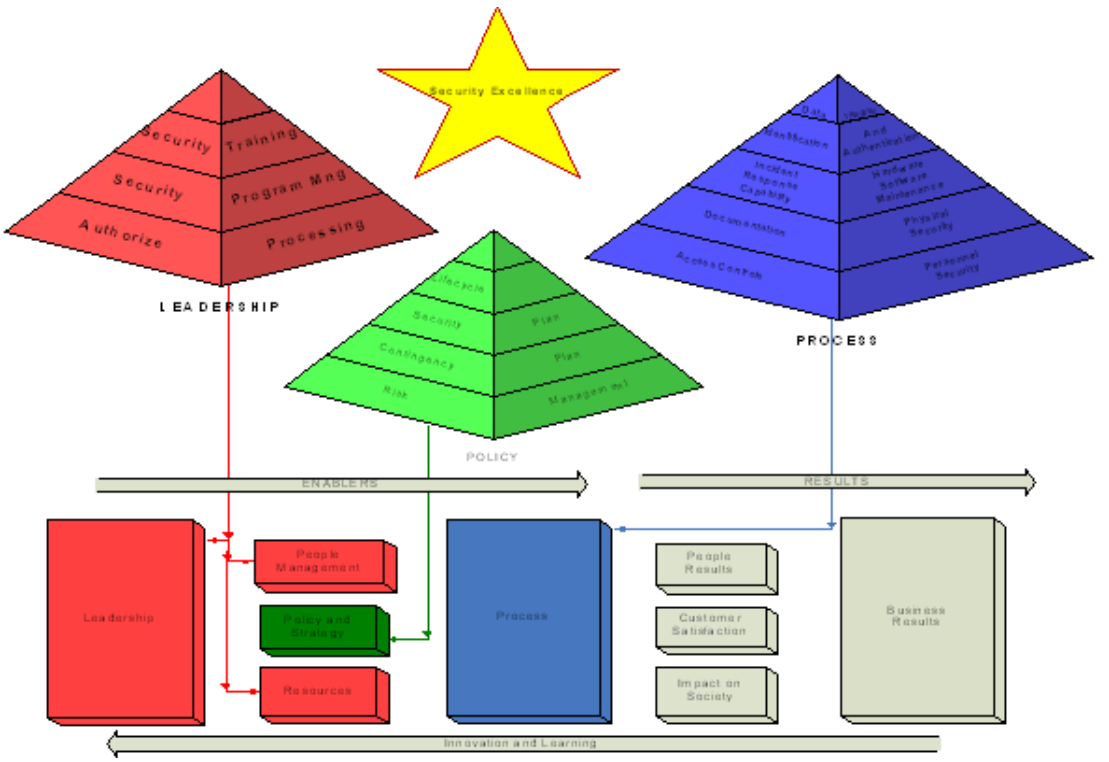


Figure 2. Integration of the NIST controls in the EFQM model



of the **Policy** metric set since it needs to be established firstly, in the Security Policy for it to flow across the remaining TQM structure (Figure 3). All of the remaining NIST controls will be further grouped into their appropriate categories in the following section.

Risk management, in the security context, is a process that encompasses identification and assessment of risks as well as mitigation, monitoring, reporting and prediction of security risks. After these phases have been completed satisfactorily to the expectations of the risk analysts, the appropriate procedures and guidelines are compiled into a Risk management document. The documented procedures will complement the Security Policy of the business which is integrated with the EFQM's corresponding **Strategy and Policy** domain; it represents a merger between both business and security policies. The top-down TQM structure becomes evident as the **Resources** are then tailored to deal with the results of the Risk management assessment as well as any contingency plans and guidelines in the Security/Business Policy. The **Leadership** criterion then comes into focus by communicating the contents of the Policy to all levels of the organizational structure. In addition, the Leadership skills must support and promote these Risk management assessments. **People** are then trained through aggressive security programs and awareness campaigns to carry out the guidelines of the Policy. Finally, the **Processes** are carried out as expected after having made the necessary changes that resulted from the security risk assessment.

The above is a description of how a specific control flows along the TQM structure and integrates with all the relevant business domains but it is however, performed from a security perspective. The obvious integration cannot be dismissed and as depicted in Figure 2, the synergy of these two domains is explicitly shown as the NIST metric sets are fused with their corresponding counterparts in the EFQM. Each specific control in each of the metric sets follows a similar TQM structure as explained above with the Risk management control (Figure 3). In essence, after the control is placed in the appropriate metric set by determining where it has a stronger impact, it is then related to all the other business domains in the EFQM. This relation or interaction of the metric sets produces a more integrated and accurate result for the individual security metric. This is due to the fact that there is an evident interaction of the security metric to the goals of the different business domains and the metric, thus, needs to be applied to all of the other EFQM criteria as well. This therefore, contributes to a more accurate result of the state of the business' performance level when it comes to that particular area or control, as defined by NIST.

As another example, the **Security Training control** can be considered as more of a driving force as part of the Leadership domain since it is an appropriate metric to determine how supportive management is toward training sessions. If management has the right approach and support for training sessions, then the **People** will be motivated to be security-conscious and will be educated on how to use the **Resources** effectively so that the **Processes** can then function as expected. This same sort of analysis has been performed for each metric to determine the category in which it is assigned to and a TQM approach is then followed to establish its relationships to the other domains, as explained above with the **Security Training** control.

After a control has been placed in either of the **Policy**, **Leadership** or **Process** categories (or pyramids), it is grouped along with other similar controls that collectively, will reflect the overall measurement or state of that category. We have therefore, classified similar controls in their respective categories which are depicted as pyramids in Figure 2. Each metric set has been represented as a pyramid due to the fact that all the stages of a pyramid converge to a common apex. The common apex is representative of precise goals and objectives that are shared by all the elements or controls of that metric set. For instance, all controls of the **Policy** pyramid should converge to the same security requirements that are reflected in the Security policy. If all layers have satisfactorily produced desirable results, then the pinnacle of the pyramid is reached in terms of there being an "excellent" Policy framework in place. The same is applicable to the other Process and Leadership pyramids or metric sets.

Furthermore, when the goals have been achieved in each pyramid, there is an alignment of their summits to the desired concept of **Security Excellence**. However, only if each pyramid has produced the required results then this can

Figure 3. Top-down TQM approach to formulating risk management security control

be achieved. Otherwise, it will not be a total security solution if one pyramid has been positioned correctly while its counterparts are dangling in a precarious or insecure position.Each metric set can now be immersed into their corresponding components in the EFQM framework. For instance, the **Policy** pyramid is fused with the evaluation criteria of the **Policy and Strategy** criterion of the EFQM. The same integration is also performed for the other pyramids as depicted in Figure 2. Tables 1 and 2 depict an integration of the **Policy** and **Leadership** security metrics into the EFQM's **Leadership and Policy** criteria.

4.1 NIST Pyramid for Policy Metric Set

The **Policy** metric set is representative of all the controls that measure the effectiveness of a Security Policy. They may be interlinked with each other at varying degrees and are as follows:

- **Lifecycle**- Deals with the implementation of security to any new process or even existing methodologies that have already been implemented.
- **Security Plan**- A plan should be implemented depending on the system requirements and defined roles to personnel should be allocated. The plan should be periodically assessed and should conform to an ISMS policy, such as ISO/IEC 17799.
- **Contingency Plan**- In the event of a catastrophe, a back up plan must be in place based on potential risks. Responsibilities and prescribed actions should be clearly outlined to avoid confusion and to restrict further damage.
- **Risk Management**- Risks should be eliminated or controlled to an acceptable level. The outcomes are mostly projected on an economic basis and can also be consequences that result from failing to comply with regulations. Even past experiences that have been recorded could be taken into account to provide a more comprehensive risk analysis. Also, linkages to other systems must be documented and those arising risks should be dealt with accordingly (Calder & Watkins, 2005).

Table 1. Integration of leadership metric

Enablers- Leadership				
1.1Leadership-10%(Inspire, Support, Promote)	Checklist Questions	Policy (Docs/records)	Process (actual procedure)	Tested and Improved (continual assessment)
"Visible demonstration of TQM"-Zink [30]	1.1.1 Do managers participate in regular meetings?			
	1.1.2 Do managers take initiative and train new employees?			
	1.1.3 Are they available to answer questions via email or other means?			
	1.1.4 Do they participate in training courses or make new courses available?			
	1.1.5 Do they share their knowledge that they may have learnt from training courses/conferences themselves?			
	1.1.6 Do they regularly remind and keep the security culture alive in meetings?			
	1.1.7 Are they present at all levels of meetings whether personally or by distributing memos?			
	1.1.8 Do they make use of other media such as bulletin boards, posters, letters, videos to communicate concepts?			
	1.1.9 Do they explicitly inform employees and stakeholders about the current state/level achieved in terms of security?			
	1.2.0 Do they effectively communicate the steps that need to be taken to reach the company's ideal security target or state?			
"Support of TQ through provision of appropriate resources and assistance"[30]	1.2.1Is management available when defining security issues in improvement activities?			
	1.2.2 Is there a security budget or emergency security fund?			
	1.2.3 Is there active support for moderating workshops or executing training activities?			
	1.2.4 Are resources made available for training sessions e.g. fully equipped room or releasing staff for training sessions?			
	1.2.5 Is support available for those actively taking improvement activities and suggestions taken into account?			
"Involvement with clients, external customers, external organizations" [30]	1.2.6 Are security links to other branches, divisions, conglomerates protected?			
	1.2.7 Are clients' privacy concerns ranked as a high priority and systems are in place to protect this?			
	1.2.8 Does the company software facilitate the adherence to legal and social implications?			
"Recognition and appreciation of the efforts and achievements of people"	1.2.9 Is there a system in place to provide recognition for departments or divisions that provide innovative security-related solutions?			
	1.3.0 Is there recognition and support for those teams/individuals that have effective security solutions?			
	1.3.1 Are the evaluations constructive in motivating persons to reflect on their strengths and weaknesses?			

Table 2. Integration of risk management metric

2. Enabler-Policy and Strategy	2.1.1 Is there a documented risk policy included in the security policy?
2.1 Risk Mgmt-NIST control	2.1.2 Is there current documentation available about the state of each system/entity?
	2.1.3 Are risks outlined regarding CIA principle?
	2.1.4 Are natural/manmade disasters taken into account as well as expected guidelines?
	2.1.5 Are other links to systems documented?
	2.1.6 Is there an acceptable level of risk defined and communicated throughout the organization?
2.2 "Policy based on info that is relevant and comprehensive" –{{391 Calder, Alan 2005; }}	2.2.1 Are social, political and legal scenarios covered?
	2.2.2 Do employees agree based on feedback that it is comprehensive?
	2.2.3 Compared to other best in class companies, are the security measures comparable or inferior to theirs?
	2.2.4 Is there an annual evaluation to address and update the security policy?
2.3 "How policy and strategy are developed" and " How the policy and strategy are regularly updated and improved"	2.3.1 Are the corporate goals fused with the security policy in the employee handbook?
	2.3.2 Are customer and other concerns updated in the policy as they occur?
	2.3.3 Are there regular internal and/or external assessments of the policy?
	2.3.4 Are the results incorporated into an annual strategy review and then adapted?
	2.3.5 Are less time-consuming, regular assessments done at least fortnightly?

4.2 Process Pyramid Metric Set

The **Process** metric set forms the core of the IT infrastructure and appropriate metrics that facilitate the smooth functioning of the Security

Policy is categorized here under the process-oriented view. The corresponding controls are:

- Data Integrity
- Identification and Authentication
- Incident Response Capability
- Documentation
- Access Controls
- Hardware and Software Maintenance
- Physical Security
- Personnel Security

4.3 The Leadership Pyramid Metric Set

The **Leadership** pyramid represents leadership skills that are applied in a more cutting-edge, integrative management style that is integrates best security practices. The metric set is dependent on the Policy being carefully crafted and being used in a way that is understood and engrained in those who are involved in the process. To achieve this aggressive security training and a security management program should be enforced. The metric set also evaluates how enthusiastic and supportive management is toward training sessions and if they themselves serve as reminders and enforcers of the Policy. In addition, management should make provisions to assign key roles and responsibilities to the right personnel.

The Leadership metrics measure:

- Security Training
- Security Program Management
- Authorize Processing

5. FUTURE WORK

The next stage of the project involves producing the actual quantitative security metrics that will represent the EFQM structure since the TQM relationships have been determined for the NIST metrics. The metrics will be applied to an environment that already utilizes a TQM approach in the form of a case study. We envision that a software prototype can then be built which encompasses a fusion of Security and Management principles and supports an evaluation process that encompasses both Business and Security Excellence.

6. CONCLUSION

TQM has been widely adopted because its value has been understood in supporting the corporation in its on-going efforts to satisfy its business objectives while at the same time paying attention to other non-financial aspects as well. IT Security, therefore, needs to be considered as a part of any Business Excellence effort. We presented an approach on how such an integration can be achieved by complementing an existing business excellence framework in order to maintain the competitive advantage and to be sustainable over time. In addition, the accompanying metrics to measure the effective merger of these two domains are not done in isolation since the security goals also support the business goals and therefore, can be measured in an integrated fashion.

ACKNOWLEDGMENTS

The authors received funding from Bell University Labs, Canada and would like to express their gratitude.

REFERENCES

Bacic, E. M., & Robison, A. (1993). The rationale behind the canadian criteria. 170-179.

Banker, R. D. (., Chang, H. (., Janakiraman, S. N. (., & Konstans, C. (. (2004). A balanced scorecard analysis of performance metrics. *European Journal of Operational Research, 154*(2), 423-436.

Brewer, D. (2005). Is the CC the only way? *International Common Criteria Conference,* Tokyo.

Calder, A. (2005). *A business guide to information security: How to protect your company's IT assets, reduce risks and understand the law*Kogan Page.

Calder, A., & Watkins, S. (2005). *IT governance: A manager's guide to data security and BS 7799/ISO 17799, 3rd edition* (3rd ed.) Kogan Page.

Canadian trusted computer product evaluation criteria(1993). No. Version 3)Canadian Systems Security Centre, Communications Security Establishment, Government of Canada.

Dedrick, J., Gurbaxani, V., & Kraemer, K. L. (2003). Information technology and economic performance: A critical review of the empirical evidence. *ACM Comput.Surv., 35*(1), 1-28.

Eloff, J. H. P., & Eloff, M. (2003). Information security management: A new paradigm. *SAICSIT '03: Proceedings of the 2003 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement through Technology,* 130-136.

Erkan, K. (2005). *Evaluating IT security performance with quantifiable metrics.* Retrieved May 25, 2006, from

European Framework for Quality Management. (2003). *Introducing excellence.* Retrieved 8/26, 2006, from

Geraedts, H. P. A., Montenarie, R., & van Rijk, P. P. (2001). The benefits of total quality management. *Computerized Medical Imaging and Graphics, 25*(2), 217-220.

Gurbaxani, V., Melville, N., & Kraemer, K. (1998). Disaggregating the return on investment to IT capital. *ICIS '98: Proceedings of the International Conference on Information Systems,* Helsinki, Finland. 376-380.

Henning, R. R. (2000). Security service level agreements: Quantifiable security for the enterprise? *NSPW '99: Proceedings of the 1999 Workshop on New Security Paradigms,* Caledon Hills, Ontario, Canada. 54-60. from http://doi.acm.org.uproxy.library.dc-uoit.ca/10.1145/335169.335194

Information technology security evaluation criteria (ITSEC)(1991). No. Version 1.2)Office for Official Publications for the European Communities.

ISMS standards overview. (2006). Retrieved 06/14, 2006, from http://www.gammassl.co.uk/topics/hot1.html

Jelen, G. (2001). *SSE-CMM security metrics.*

Jorma, K., & Reijo, S. (2005). *Towards better information security management by understanding security metrics and measuring process.* Retrieved May 27, 2006, from

Martín-Castilla, J. I. (2002). Possible ethical implications in the deployment of the EFQM excellence model. *Journal of Business Ethics, 39*(1/2), 125-134.

Martinez-Lorente, A. R., Sanchez-Rodriguez, C., & Dewhurst, F. W. (2004). The effect of information technologies on TQM: An initial analysis. *International Journal of Production Economics, 89*(1), 77-93.

Mercuri, R. T. (2003). Analyzing security costs. *Communications of the ACM, 46*(6), 15-18.

Michaelsen, R. H., Michie, D., & Boulanger, A. (1985). He technology of expert sy- stems. *BYTE 10, No. 4,* , 303.

Nasierowski, W. (1997). Rethinking corporate restructuring: A comparison of the four central approaches. *Technology Analysis and Strategic Management, 9*(1), 75-84.

Perides, M. (2002). Aiming at excellence in healthcare- the european foundation for quality management excellence model. *Business Briefing: Global Healthcare,* (3), 56-59.

Saraiva, P., Rosa, M., & Orey, J. (2003). Applying an excellence model to schools. *Quality Progress,* , 46-51.

Sciarelli, S. (2002). Business quality and business ethics. *Total Quality Management, 13*(8), 1141.

Shirley, C. P. (2002). A guide to security metrics. Retrieved May 18, 2006, from

Swanson, M. (2003). *Security self-assessment guide for information technology systems* No. 800-26). USA: National Institute of Standards and Technology, US Department of Commerce.

Swanson, M., & Bartol, Nadya et al. (2003). *Security metrics guide for information technology systems* No. 800-55). USA: National Institute of Standards and Technology , US Department of Commerce.

Westlund, A. H. (2001). Measuring environmental impact on society in the EFQM system. *Total Quality Management, 12*(1), 125-135.