A Cultural Adaption Model for Global Cyber Security Warning Systems:

A socio-techinal proposal

Bilal Alsabbagh , Stewart Kowalski
Department of Computer and System Sciences, Stockholm University
Kista, Sweden
steawrt.kowaski@dsv.su.se, bilal@dsv.su.se

***Abstract*—In this paper we explore the problems of developing a cyber security alert warning system both from a theoretical and practical perspective. We review some of the current development in warning systems around the world and we also examine the area of security metrics area. We then expanded on a proposed socio-technical coordinate system [1] for global cyber security alerts and adapted it to an information security culture framework.**

Keywords-cyber security; alert systems; security metrics; socio-technical security systems.

I. INTRODUCTION AND PROBLEM STATEMENT

A. Warning Systems – Problems -Past and Present

Regardless if it is a warning system for bad weather or for cyber attacks there are a number of basic and common design principles and functional requirements that are needed to be considered when proposing any alarm/alert and warning system. Four such principles have been outlined by the Norwegian Petroleum Directorate and state that the system must display information that is relevant to the "stakeholders"[2] roles at the time, indicate what response is required, be presented at a rate that the "stakeholders" can deal with, and be easy to understand by "all stakeholders"[1]. The most difficult challenge, and a major problem for alarm/alert systems is to design a system that is easy for all stakeholders to understand, a problem that Sir Francis Beaufort already faced in the early 19th century.

During the 18th and 19th century officers on board of ships made regular weather observations. But since they used subjective common terms their reports were seldom comparable. Sir Francis Beaufort, a British admiral, introduced around 1800 a standardized way of describing the weather conditions. This is today known as the Beaufort scale. It defines 17 (originally 12) categories of wind strength, based on objective observations of the environment. Examples are the behavior of smoke or damages to trees [2]. This allows any two individuals to compare their weather situation by observing their environment without doing any detailed measurements.

Another well know system is the (Modified) Mercalli intensity scale [3], which was developed around 1900. It classifies the strength of earthquakes into 12 groups. Again, the objective effects on the environment are used as the scale. Effects on houses, the landscape or humans are easily observable and also a good indicator of the earthquake's strength.

As the British navy ships of the 18th century modern organizations today need meaningful and actionable information about the cyber security environments they are to navigate and do business in. A number of different attempts to establish warning systems that have been proposed use different types of security metrics. These proposals can be grouped into one of two general categories, those that use generic security metrics or those that use specialized security metrics:

- Generic cyber threat levels for the public
- Specialized metrics for a specific situation

1) Generic Warning Systems. The first group aims to give a broad overview of the current environment, usually focusing on consumers. Examples are the indices that are published by anti-virus vendors [4][5][6][9]. They summarize their current view of virus and other malware activity. Although the result is a categorization, they often do not publish the details of the metric. Only results from the same vendor can therefore be compared.

Some governments also publish their view of the current cyber threat level [7][8][10]. While some of the investigated metrics do have a sufficient description, none of their data sources is stated. This makes the quality of the information questionable.

Lastly, some well known internet organizations, such as the Internet Storm Center [11], also publish a status based on their data collection. But again, in case of the ISC no sources are documented.

2) Specialized Warning Systems. These metrics in this group aim to provide information about a specific environment. Their aim is therefore to aid specialists in their task. All the investigated systems were described in theory. No practical, ongoing implementation was found to be publicy available.

On a lower technical level, [12] defines a system to predict future attacks through analysis of existing data. Variable length

[1] This paper is an extensions of an earlier paper that was pubished at the MetriSec 2011 conference where the socio technical coordinate systems was proposed by one of the authors [X]

[2] The original term was "operator", the term "stakeholder" was added by the authors.

Markov models are used together with the assumption that an attacker follows a certain sequential logic. The results show that the intended prediction is possible.

Kim et al. [13] suggest a system based on real time data. It consists of three analysis engines to minimize false alerts. The result is a forecast about the immediate future of the observed IT environment.

On a higher level, [14] defines threat alert levels for the North American electricity sector. The threats that have to be present for a specific alert level are described in generic terms, such as "general threat of increased cyber (…) activity" and high level counter measures are given.

The MITRE Corporation suggested the Cyber Prep framework [15]. It defines threat levels for an organization based on the intention and capabilities of the potential attacker. This allows for a targeted and effective response to the suspected threats.

3) Review of the Current Situation. The preceding review of some of the research in the area of cyber weather forecasting show very well the issues at hand. Currently, there exists no functional framework to assess the cyber threat level in an objective/quantitative manner.

Those in the first group are too generic, and the algorithm and data basis behind them are not documented sufficiently. Those in the second group aim to provide protection for organizations, but the predictions are made for a very short term for technical countermeasures or they are very generic and independent of the dynamic environment.

Before going on to outline our suggestion for a cyber security warning coordinate system, we shall first review the current state of security metrics and some of the issues that a cyber security warning system needs to address.

B. Security Metrics

To paraphrase the frequently quoted (and misquoted) expression by Lord Kelvin, unless something can be measured, our knowledge of it is insufficient. The readily understood implication of this in the reality of management is that our ability to manage something is directly dependent on our knowledge of it, and that managing something that cannot be (or is not being) measured is generally difficult to near impossible.

This realization has become increasingly apparent in the field of information security over the past ten or so years [16]. For instance, measurement is an explicit requirement in the ISO/IEC 27001 standard [17]; and surveys such as [18] and [19] show that there is a rising interest (and need) for dependable information security metrics among numerous companies and that their importance in the success of information security programs is recognized by many executives and security professionals.

Possibly the greatest driver for this development for most organizations is the recently amplified regulatory environment, demanding greater transparency and accountability. However, organizations are also driven by internal factors, such as the needs to better prioritize and justify the security investments, ensure proper alignment between the security and the overall organizational mission, goals, and objectives, and fine-tune effectiveness and efficiency of their security programs.

Information security metrics, when properly designed and implemented, can aid in the above by facilitating decision making with a level of objectivity, consistency, transparency, and efficiency that may not otherwise be feasible.

C. State of Security Metrics

A number of research initiatives have been emerging and culminating in methodologies, frameworks, best practice and regulatory standards, compilations, tools, technologies, and so on, being developed or adapted to cover/support information security metrics. A recent state-of-the-art report on the subject [16] shows that, while numerous advances have been made in the last decade, in several respects the security measurement field is still in its infancy, and knowledge, methodology, and technology gaps remain.

The dependability and actual value of metrics is generally attributed to the qualities, such as objectivity, consistency, and efficiency, which they *ideally* possess. It can be acknowledged that in practice security metrics often fall short of achieving these qualities [20][21][22]. Guidance on how the challenges of development, implementation, and operation of information security metrics may be overcome is available, however, e.g. [21] and [23].

The ISO/IEC 27004 [24] and the NIST SP 800-55 [25] standards constitute significant efforts towards standardizing various aspects of security measurement. The two standards define requirements and provide best-practice guidelines for establishment and operation of a successful security metrics program, but they are not entirely exhaustive.

D. Security Metrics and the Environment

It can be readily acknowledged that an assessment that an information system or an asset is secure only holds when the potential threats against it are identified and accounted for.

Both ISO/IEC 27004 and NIST SP 800-55 underline the need for organizations to have a sound understanding of their operational environment and the security risks they face, and both of the security measurement standards explicitly require that proper risk assessment be performed by an organization prior to commencing security measurement [24][25].

However, the two standards mostly describe the strategic (i.e. longer-term) connection between security measurement and risk management, and do not cover the more operational aspects of their interrelationship explicitly.

The state of an organization's operational environment is not entirely persistent. It may be subject to rapid changes and fluctuations (that can be expected and planned for) that may affect measurement procedures (e.g. a temporary increase in the probability of particular operational threats may call for a proportionate temporary increase in the frequency of certain measurements).

Another issue that is not directly addressed in the current standards on information security measurement is that (given that the actual security is a function of how well-protected an information system or asset is and the threats present in the operational environment) dependability of security metrics is strongly related to the dependability of estimations regarding the operational risks. That is, if a system can be shown to be adequately secure in quantitative terms given the threats it is exposed to but the threat assessment is qualitative, the actual security metric is not fully quantitative, for instance.

Another consideration is that if levels (and categories) of operational threats are standardized, it allows for deployment

of inter- and supra-organizational warning systems and inter-organizational and national comparison of security postures [26].

E. Social Aspect of cyber security

In the International Telecommunication Union (ITU analysis which compare cyber security initiatives in several countries, different culture and social aspect of security systems were observed [27]. This difference can be understood by the different approaches these countries take to understand the cyber security threats, how they define their assets and what security measures they take to protect them. The understanding of these national initiatives will be necessary in order to develop a viable glocal framework in cyber security. The primary source used in this study was the "Handbook of Critical information infrastructure protection" [28].. The 2008/2009 edition presents governmental practices in 25 countries in North and South America, Europe, Asia and the Pacific for protecting their critical information infrastructure The data were gathered using surveys collected from public resources, area experts from governmental, organizational and academic sectors. The focal pointes used in the survey are:

- How critical sectors are defined
- The organizational framework of Critical information infrastructure protection
- Early warning approaches
- Law and legislations
- Initiatives and policies

The global treaty on cyber security and cybercrime, a draft for international framework for cyber security, has also stressed that security practice is strongly related to local culture, ethics, politics and law [29]. According to the treaty, this fact should be considered for systemic and global approach when dealing with cyber security. Systemic by considering the social and technical aspects of cyber security, and global by looking at security a problem requires cooperation, collaboration and knowledge sharing by the different members sharing the cyberspace with no borders against cybercrimes and cyber threats.

II. PROPOSED COORDINATE SYSTEM

Organizations use security control systems to prepare for and to mitigate threats that are both social and technical in nature. Consequently, any cyber security warning system needs to provide meaningful and actionable indicators of the cyber threat environment to control systems intended to deal with either one or both of these categories of threats.

On Figure 1 below, we use a coordinate system in order to visualize the relationship between operational environment threat metrics and organizational security posture. The Y axis in the coordinate system ranges from less to more complex attacks in both the technical (bottom) and the social (top) halves of the coordinate system. On the X axis, degrees of severity of the threat environment ranging from level 1 (low severity) to 3 (high severity) are located in quadrants 1 and 4, and in quadrants 2 and 3 we have mapped the security posture levels that range from weak (level 1) to strong (level 3). The levels used in this case are heuristic and are introduced purely for illustrative purposes.

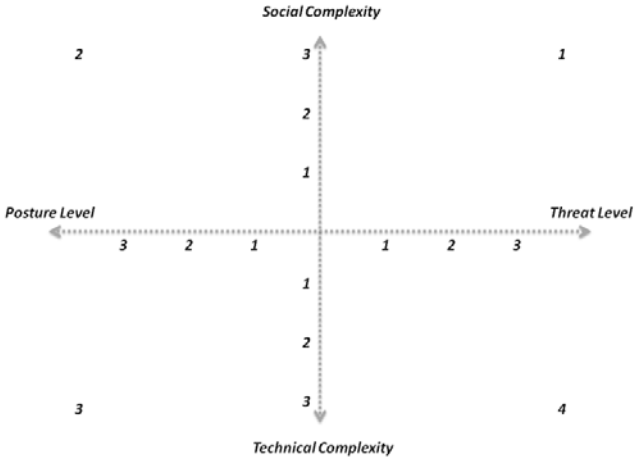


Figure 1. Cyber Security Warning Coordinate System.

The coordinate system attempts to provide a flexible yet semi-formal visual model to capture the relationship between technical and social security controls systems, and organize and capture complex attack vectors, presenting them in a useful way. Useful in that the information system security managers and the IT security experts can discuss both technical and non-technical security issues based on the same graph. That is to say, from a socio-technical modeling perspective, it attempts to make sure that everyone is on "the same page".

To provide a basic example of how the system can be used, let us describe an attack scenario. In the scenario the attackers are environmentalists who want to discredit an environment agency. They are using a two prong attack targeting the intranet of the organization to distribute misguiding information on security instructions to internal staff and at the same time have the organization send out misinformation to the company's customers. A customer will contact employee in the company to request a special rate on electricity. The employees have been informed to help the customer. The scenario is visualized on Figure 2 below.

In the scenario we see how the attackers have a social attack of level 2, since they have to not only obtained both employee email addresses and customer email addresses but also composed and sent email. On the technical side, since they only had to compromise, let's say, a poorly configured mail server, the technical complexity of the attack is only level 1. Since this attack is more a discrediting rather than a financial or operational attack, the severity level is suggested here for the explanation purpose is deemed to be level 1. The figure also shows that the security posture of the organization in question is not able to completely deal with a social attack of that complexity level, indicating a gap in security and potential operational risk that needs to be understood and accepted or mitigated by the relevant stakeholders in the company.

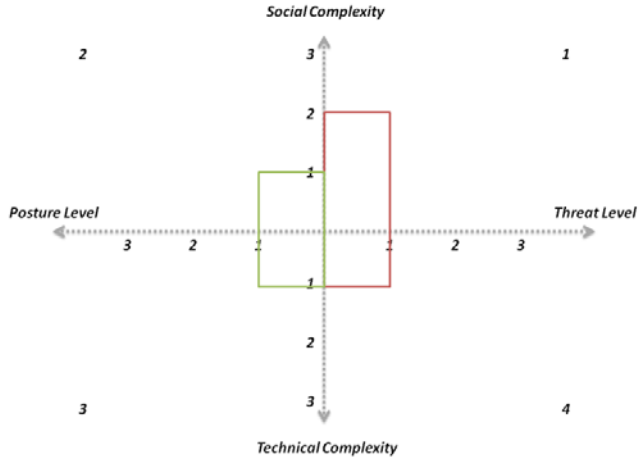


Figure 2. Cyber Security Warning Coordinate System with the environmentalist attack scenario.

III. PROPOSED SOCIALY OPTIMIZED CYBER SECURITY ALERT SYSTEM

. Our proposed socially optimized cyber security alert system is based on the security value chain [30]. The term was originally used to study the security spending mental models of different organizations in terms of the main security access control categories: Deter, Detect, Protect, Correct and Recover. In other words, on which control categories given organization budget would be spent when addressing security issues.

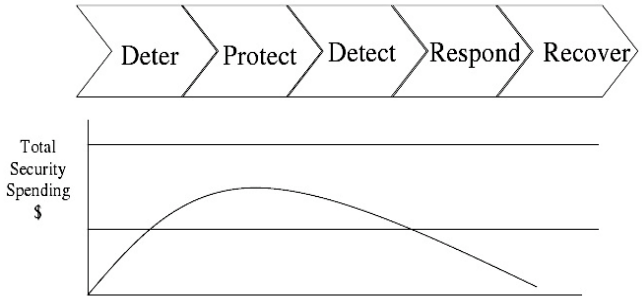
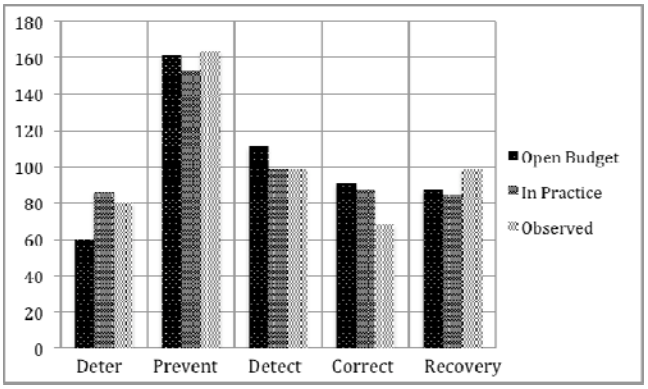


Figure 3. Security Spending Mental Models

The model was then further developed and suggested as social security metric for modeling the security mental models in different cultures. It was actually used in case study for exploring the security mental models of IT workers in Saudi Arabia to understand what security controls they would implement to deal with security issues at personal, organizational and national levels [31].

Figure 4. IT Workers secuirty mentla models in Organizations (case study)



The suggested location for the proposed system is at regional CERT that act as center of coordination between the local and global CERTs and ensure the cyber security alert is better understood and dealt with. When new cyber security alert is announced, the regional CERT will analyze the alert details including descriptions, threat level and what security controls are the most effective to address the associated threat. These controls are then compared to check whether they conform to the local culture security mental models in terms of the security value chain. If the required mitigation measures are found to fall under the same control category the local culture would go with, then no changes are needed to the alert details. If the required mitigation measures are found to be among controls categories not matching with the local culture security mental models then naturally the security risk here should be increased because the threat might then not be addressed enough. In this case the regional CERT has to escalate the security threat criticality level in the alert based on the variance between the required effective controls and the security mental models. The cyber security alert description and details are then updated accordingly and additional instructions are added to fill the gap.

A case study of using this system is when a new security threat of local bank phishing website is discovered in Saudi Arabia. The CERT before announcing the cyber security alert needs to review the threat details and what are the most effective controls needed for dealing with the problem. From security best practices perspective, the CERT recognizes the need to implement preventive and detective measures to mitigate the risk and reduce the chance and use of stealing bank customers credentials. Detective measures where banks increase their customers security awareness about recognizing phishing threats and that the bank will never request customers credentials through emails or chat channels. Preventive measures are also implemented in place using strong means of authentication by multi-factor techniques based on what customers know (usernames, answer to certain questions) and something they have (hardware based one time authentication tokens). Of course there could be also deterrent measures recommended by legislating laws to but in cyber security threats might be originating from different countries and as yet there is no global law to deal with cyber security, this option is left out.

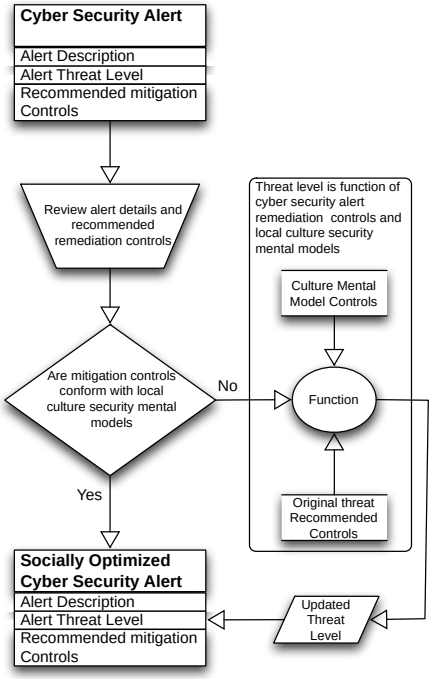


Figure 5. Socially Optimized Cyber Security Warning System.

Because the IT workers security mental models of the local culture where this CERT operates seem to be compatible with the required controls categories for addressing the phishing threats, then the CERT find that there is no need to adjust the threat level thus the security alert is announced.

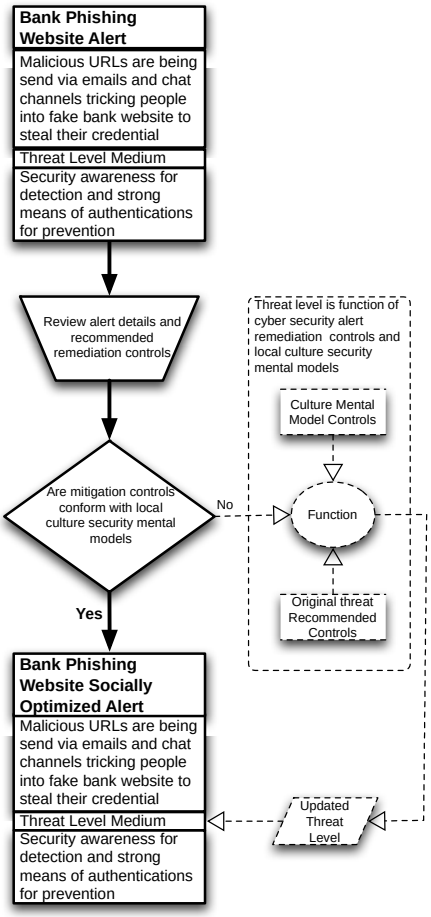


Figure 6. Socially Optimized Cyber Security Alert Scenario.

IV. SUMMARY AND DISCUSSION

In this short paper we have adapted the proposed socio-technical security warning coordinate system and intergrated a culture filter.

Furthermore, the proposed coordinate system can possibly be supplemented by a Z axis, representing the time factors for the threat levels in the environment and security posture levels in the organization to deal with strategic vs. operational action.

REFERENCES

[0] Kowalski, S., Barabanov, R., Hoffmann,R., Cyber Security Alert Warning System:A socio-techical coordinate systems proposal, International Workshop on Security Measurements and Metrics, ESEM 11 2011 ACM-IEEE International Symposium on Empirical Software Engineering and Measuremen Banff Alberta Canada September 21 - 22, 2011.

[1] Norweign Petroleum Directorate, Principles for alarm system design, February 2001, Availabe at http://www.ptil.no/getfile.php/Regelverket/Alarm_system_design_e.pdf.

[2] Met Office, Beaufort scale, 2011, Available at http://www.metoffice.gov.uk/weather/marine/guide/beaufortscale.html.

[3] U.S. Geological Survey, Magnitude / Intensity Comparison, 2010, Available at http://earthquake.usgs.gov/learn/topics/mag_vs_int.php.

[4] Symantec Corporation, ThreatCon, 2011, Available at http://www.symantec.com/business/security_response/index.jsp#.

[5] Trend Micro Incorporated, Current Threat Activity, 2011, Available at http://us.trendmicro.com/us/trendwatch/current-threat-activity/index.html.

[6] Sunbelt Software, Current VIPRE® Threat Level, 2011, Available at http://www.sunbeltsecurity.com/ThreatLevel.aspx.

[7] New York State, New York State Cyber Alert Level, 2011, Available at http://www.dhses.ny.gov/ocs/.

[8] North Dakota Information technology Department, Cyber Threat Level Indicator, 2011, Available at http://www.nd.gov/itd/services/it-security.

[9] ESET spol. s r. o., Threat Center, 2011, Available at http://www.eset.eu/threat-center.

[10] Blue Glacier Management Group, Threat Levels, 2011, Available at https://www.it-isac.org/alertcon_n.php.

[11] SANS-ISC, Infocon, 2011, Available at http://isc.sans.edu/infocon.html.

[12] D. Schnetzer Fava, Characterization of Cyber Attacks Through Variable Length Markov Models, Rochester Institute of Technology, Rochester, New York, 2007.

[13] S. Kim, S. Shin, H. Kim, K. H. Kwon, and Y. Han, Hybrid Intrusion Forecasting Framework for Early Warning System, IEICE, vol. E91-D, 2008.

[14] North American Electric Reliability Council, Threat Alert System and Cyber Response Guidelines for the Electricity Sector, USA, 2002.

[15] D. Bodeau, J. Fabius-Greene, and R. Graubart, How Do You Assess Your Organization's Cyber Threat Level?, The MITRE Corporation, USA, 2010.

[16] IATAC, Measuring Cyber Security And Information Assurance: State-of-the-Art Report. Herndon, VA: Information Assurance Technology Analysis Center, 2009.

[17] ISO, ISO/IEC 27001:2005, Information Technology -- Security Techniques -- Information Security Management Systems -- Requirements. Geneva: ISO, 2005.

[18] R. Ayoub, Analysis of Business Driven Metrics: Measuring for Security Value (White Paper). Frost & Sullivan, 2006. Available at http://www.intellitactics.com/pdfs/Frost_SecurityMetricsWhitePaper.pdf

[19] S. K. O'Bryan, "Critical elements of information security program success," Information Systems Control Journal, vol. 3, 2006. Available at http://www.isaca.org/Journal/Past-Issues/2006/Volume-3/Pages/default.aspx

[20] D. A. Chapin and S. Akridge, "How can security be measured?" Information Systems Control Journal, vol. 2, 2005. Available at http://www.isaca.org/Journal/Past-Issues/2005/Volume2/Pages/default.aspx

[21] A. Jaquith, Security Metrics: Replacing Fear, Uncertainty, And Doubt. Upper Saddle River, NJ: Addison-Wesley, 2007.

[22] W. Jansen, Directions in Security Metrics Research. Gaithersburg, MD: National Institute of Standards and Technology, 2009.

[23] D. S. Herrmann, Complete Guide To Security And Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, And ROI. Boca Raton, FL: Auerbach Publications, 2007.

[24] ISO, ISO/IEC 27004:2009, Information Technology -- Security Techniques -- Information Security Management -- Measurement. Geneva: ISO, 2009.

[25] E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson, Performance Measurement Guide For Information Security. Gaithersburg, MD: National Institute of Standards and Technology, 2008.

[26] S. Kowalski,Cybernetics Analysis of National Computer Security, Computers & Security, Vol. 10, No 3, 1991.

[27] Dunn Myriam, "A Comparative Analysis of Cyber security Initiatives Worldwide", WSIS Thematic Meeting on Cybersecurity, Geneva, 28 June-1 July 2005.

[28] Elgin M. Brunner and Manuel Suter (2008) INTERNATIONAL CIIP HANDBOOK 2008 / 2009, 2008

[29] Schjølberg S. and Ghernaouti-Hélie S. A Global Treaty on Cybersecurity and Cybercrime, Second Edition, 2011

[30] Kowalski, S., & Edwards, N. , "A security and trust framework for a Wireless World: A Cross Issue Approach", Wireless World Research Forum no. 12, Toronto, Canada, 2004

[31] AlSabbagh, B. and Kowalski S. , Developing Social Metrics for Security: Modeling the Security Culture of Saudi Arabia (Case Study)