A CHANGE STRATEGY FOR ORGANISATIONAL SECURITY
The Role of Critical Success Factors

Sue Foster, Kate Lazarenko
Monash University, Sir John Monash Drive, Melbourne, Australia

Paul Hawking, Andrew Stein
Victoria University, Flinders St, Melbourne CBD, Australia

Keywords: Critical Success Factors, Change Management, Security Strategy, Security Framework, Culture.

Abstract: The focus for any organization should be in securing the critical components that are important to business survival This can be accomplished by adopting technical and non technical approaches. The non technical approaches however tend to be more problematic and include changing the way employees perceive enterprise security. People issues have always posed problems when implementing new systems, and an enterprise security strategy is no exception. The identification and adoption of critical success factors to support a sound security strategy could provide a successful security outcome. In this paper a security framework is developed from the literature and each part of the framework provides the opportunity to identify critical success factors. It is contended that by using this framework organizations are able to build a strong security base for their enterprise.

1 INTRODUCTION

The focus for any organization should be in securing the critical components that are important to business survival. The terrorist events in New York and subsequently those in London, have changed the world's perspectives on security. In the business sector for example, many companies are redefining the mission and contribution to security (Dalton, 2003). Before such events enterprises were often reactive to disasters; but these events have demonstrated that organizations need to adopt a proactive approach by protecting critical systems and assets (Dalton, 2003).

Ultimately, the goal of an enterprise is to ensure adequate protection of critical assets and systems through the goals of security. These standard goals are identified as confidentiality, integrity, and availability. These standard goals have been extended by the author to include accountability (Allen, 2005a; Caralli, 2004a). Adequate protection can be defined as a condition where security strategies for the critical business processes and assets are based upon the risk tolerance the organization is willing to accept (Allen, 2005a). A security strategy can be defined as a range of actions that an organization needs to take to reduce security risk to an adequate or acceptable level depending on the protection needs of the organisation (Allen, 2005b).

As organizations have different environments, culture, goals, objectives and business strategies, a security strategy that can be implemented, measured, and revised as its business climate and environment changes is of major importance (Caralli, 2004b, Dalton, 1995). The underlying principle of good strategic security planning can be summed up as doing the right things, in the right way, to achieve a desired outcome. Strategic security planning requires initiatives that are designed to identify risks, assess their impact, contrast that to the cost of prevention, and then develop an appropriate strategy in the organizational context, complete with a mechanism for ongoing assessment designed to measure the consequences of that strategy (Dalton, 1997). Security strategies should be based upon business drivers such as complying with relevant

Foster S., Lazarenko K., Hawking P. and Stein A. (2007).
A CHANGE STRATEGY FOR ORGANISATIONAL SECURITY - The Role of Critical Success Factors.
In *Proceedings of the Ninth International Conference on Enterprise Information Systems - ISAS*, pages 375-380
DOI: 10.5220/0002380003750380

regulations and should focus on developing a top-down strategy for security that permits the integration of many different types and sources of security practices (Alberts & Dorofee, 2001; Caralli, 2004b).

Although, human factors have been identified as one of the major internal threats to confidentiality, integrity and availability of critical assets, there are numerous mechanisms to remedy against these internal threats; such mechanisms could include policies and procedures to support a defence in depth security strategy.

However, the most problematic and challenging aspect of computer security management is in changing personnel (users') attitudes and behaviour regarding computer security practices (AusCERT, 2006). In fact this has been identified as problematic with any required change process. From a psychological perspective, to develop and influence the emotional capability of organisations as a resource to facilitate change is an important break through in change management strategies (Schein, 1988). Cultural theorists argue that the values, beliefs, assumptions, perceptions, behavioural norms, artefacts and patterns of behaviour that are shared by members of an organisation operate unconsciously, and fashion an organisation's view of itself and its environment (Handy, 1996; Schein,1988). There is a crucial need to understand an organisation's culture in designing and implementing successful change initiatives of any nature (Handy, 1996; Schein, 1988).

It is argued in this paper that in order to bring about change and establish positive attitudes towards the use of new procedures, change programs must identify employees as one of the most important critical success factors associated with the uptake of secure systems and procedures.

Further in order to develop a sound organizational security strategy the emphasis should be in identifying critical success factors at each point in the strategy. By adopting this approach organizations are more likely to focus attention on areas vital to a successful security outcome.

1.1 CSF Theory

Critical success factor theory was developed by John Rockart in the 70s-80s. Rockart argued that the identification of 'critical success factors' (CSFs) supports attainment of organizational goals (Millard, 2004). While critical success factors themselves are identified as key areas in which a failure to perform may form a major barrier to achieve organizational goals (Rockart & Bullen, 1981). CSFs represent those managerial or enterprise areas that must be given special and continual attention to bring about high performance. CSFs include issues vital to an organization's current operating activities to achieve its future success. (Boynton, 1984).

The most popular existing security standard ISO 17799 identifies a full range of critical success factors. It is argued that these are required for establishing adequate security (Allen, 2004). The CSFs include but are not limited to establishing information security policies and clear objectives; a good understanding of the information security requirements, risk assessment, and risk management; providing appropriate awareness, training, and education for staff; provision to adequately fund information security management activities; and implementation of a measurement system that can be used to evaluate performance in information security management and feedback suggestions for improvement. The researchers have identified a major failing with the use of these CSFs in that they are not identified in any particular order and more importantly no one factor is identified as being more critical than another. However it should be noted that one factor does stand out from the rest; that is obtaining management support. This CSF is one of the most important and leading critical success factors and has been continuously identified in the CSF information system implementation literature. It is not unrealistic to expect that this factor would be a primary success factor in a security strategy change approach.

Managing change has always been problematic, but it appears that without major factors to support this change the success of the change process will be jeopardized. The one common denominator is that they are all people related and by definition are directly implicated in managing change.

The Security Standard (ISO17799) considers that these factors should be taken into consideration by any enterprise whose aim is to establish an adequate organizational security. In this context an organization should have a framework upon which to establish their enterprise security management. A security framework can be defined as a comprehensive description of the people, processes and technology components that comprise a complete security capability (ISO 2005). This framework should firstly, highlight key areas with which to contribute to the success of adopting enterprise security. Secondly, the framework should demonstrate the relationships between the various key areas and their influence upon one another and thirdly, how they can further be used as a roadmap or standard approach to enterprise security management.

2 CSF FRAMEWORK

The Software Engineering Institute (SEI) from Carnegie-Mellon University has developed a practical framework for enterprise security management. The framework uses the concept of capability areas (CA). These are areas of functionality and responsibility within an organization that integrate with one another allowing an organization to achieve a desired state of enterprise security. The capability areas and the structure of the framework are based upon the generally accepted information security principles (GAISP) described in the Information Systems Security Association (ISSA) (ISSA, 2004). The Information Security Forum's (ISF) standard of good practices (ISF, 2005). The Information Technology Governance Institute's (ITGI) guide on information security governance (ITGI,2006) and the COBIT 4.0 standard framework (ITGI, 2005).

The framework shown in figure 1 (see opposite page) consists of eight integrated capability areas (CA) which should exist in an organization. By applying the concept of critical success factors in each CA, an organization is able to develop a holistic approach to enterprise security (Allen, 2004).

2.1 CA 1: CSFs Determine Priorities

These critical success factors (CSFs) are the business drivers that the organization must achieve in order to reach its goals and objectives Rockart, 1979). From a security standpoint, organizational CSFs contribute to the foundation for creating enterprise-wide collaboration, planning, and execution Caralli, 2004b). By understanding the success factors which influence the organization in achieving its goals and objectives, such as maintaining operational efficiency or strategic planning, the organization is able to identify the business processes and data critical for the livelihood and survival of the business. CSFs have been identified as aligning the organizational business drivers with the information security strategy (Caralli & Wilson, 2004; Herold, 2004a).

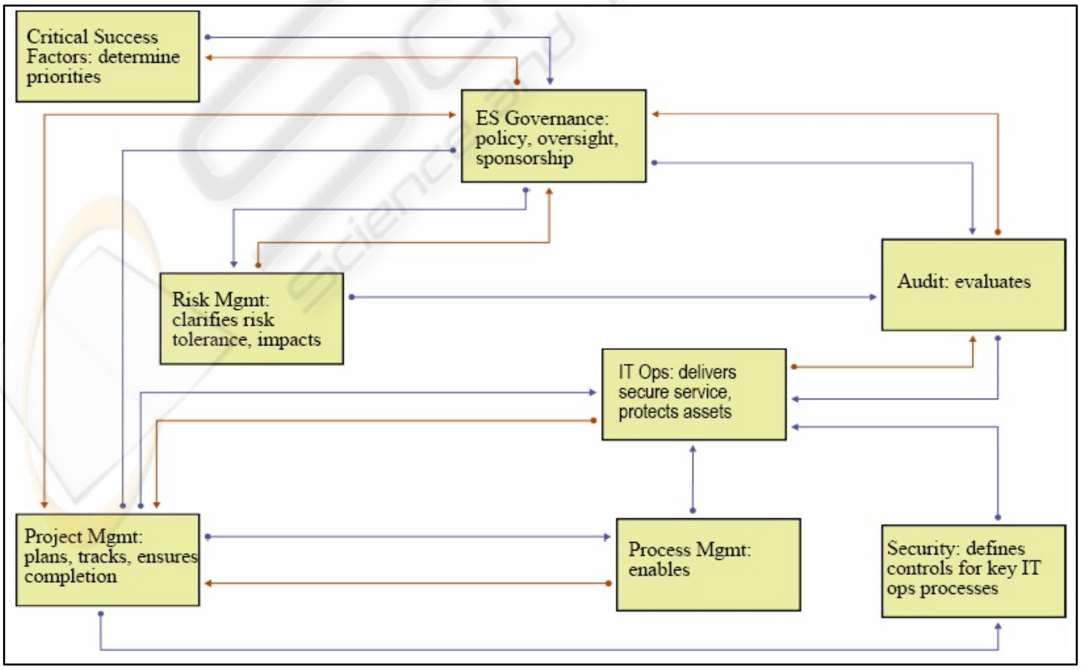
Critical Success Factors: determine priorities
ES Governance: policy, oversight, sponsorship
Audit: evaluates
Risk Mgmt: clarifies risk tolerance, impacts
IT Ops: delivers secure service, protects assets
Project Mgmt: plans, tracks, ensures completion
Process Mgmt: enables
Security: defines controls for key IT ops processes

Figure 1: Practical framework for enterprise security management (Allen J., 2004).

2.2 CA 2: ES Governance

Enterprise security governance directs and controls an organization to establish and maintain a culture of security throughout the enterprise (Allen, 2005a). The goal of enterprise security governance is to define adequate security for the organization in relation to all the organizational components that affect the achievement of the organizational CSFs. In this regard critical success factors guide enterprise security governance by identifying the crucial components of an organization. By using CSFs as a guideline, the executive manager can identify responsibilities and judge the importance of each organizational department in achieving CSFs (Caralli, 2004a). A CSF such as development of human resources is dependant upon the human resource department, while a CSF such as strategic planning is the responsibility of both financial and sales departments.

Management at all levels of the organization must place value on and show the importance of security (McCarthy, 2003). Security governance helps the business with security, providing sponsorship and governance for enterprise security, and creating a focus on the productive elements, processes and information, critical to its survival (Caralli, 2004b). Security governance provides knowledge at all levels of management and provides awareness of the various security controls available, and implementation best practice (Straub & Welke, 1998).

2.3 CA 3: Risk Management

Once all levels of management have been coached on the security requirements, they can begin to sponsor and commit the efforts to risk management. The organizational CSFs can be utilized to determine the scope of the risk assessment and risk analysis activities (Caralli, 2004a). This can be done through using evaluation criteria such as Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE).

OCTAVE is a self-directed evaluation approach focusing on risk to information assets, mitigation procedures and practices, and constant monitoring of the security practices. It involves all departments of the enterprise (Alberts & Dorofee, 2002). Applying CSFs to existing information security evaluation criteria, such as OCTAVE, ensures that risk assessment is focused on the right areas of the organization (Caralli & Stevens, 2004) and ensures the phases of OCTAVE yield meaningful results; building asset-based profiles, identifying vulnerabilities and threats, and developing security strategy and plans (Alberts et al, 2001).

Once the critical assets have been identified, the security requirements for each asset can be determined. These security requirements should place emphasis on the aforementioned security goals. Based on the role of identified assets in achieving organizational goals and mission, and the boundaries of adequate security, certain security requirements might be prioritized over others. For instance, an ERP system might require availability, accountability, and integrity while a financial system would prioritize confidentiality and privacy over availability, while other parameters remain the same (Caralli, 2004a).

A risk mitigation framework, such as OCTAVE, may focus security on operational areas that employ a tactical and strategic approach (Alberts et al, 2001).. Best practices, such as that offered in ISO 17799, focus on standards that the enterprise is required to fulfill, and provides a checklist the organization should accomplish; what they must do but not how to do it (Saint-Germain, 2005). CSFs become the evaluation criteria upon which to measure the risk mitigation strategies identified by OCTAVE and whether best practices have been followed that fulfill the security needs. It is argued the CSFs tie the risk mitigation strategies and best practices together, for each asset and for each department, into a unified enterprise perspective making CSFs crucial in achieving objective and goals (Caralli, 2004a).

2.4 CA 4: IT Ops

After performing risk mitigation, the organization proceeds to create procedures, standards, controls, and policies which allow them to mitigate the risk to the critical assets they have identified. The procedures, standards, controls, and policies that the enterprise creates must reflect the business objectives, be consistent with the organizational culture, and have the support and commitment by all levels of management (Alberts & Dorofee, 2001; Caralli, 2004b). CSFs assist the process of creating the strategic security measures by becoming the foundation on which those measures are based (Allen, 2005a; Caralli, 2004b). CSFs focus and align the different security measures with the organizational CSFs, therefore ensuring each measure supports the CSF and adequate security defined by management.

Once security standards, controls, procedures, and policies have been created, they must be communicated throughout the entire enterprise. Training and support ensure that awareness and understanding of enterprise security is communicated throughout the enterprise (GAISP, 2004; (Alberts et al, 2001; Caralli, 2004b). Training and awareness helps the enterprise create a culture of security at every level (Allen, 2004).

CSFs help define the role and function of different employees in different departments in helping to achieve security goals and objectives (Allen, J. 2004 and Caralli, R. 2004a) Using CSFs as an evaluation criteria, enterprises are able to measure whether the security measure they have implemented were successful or not. On-going evaluation at every level will create the culture of security within the enterprise as employees realize the importance of security in the enterprise (Allen, 2005b; Allen, 2005b; Alberts, et al, 2001; Caralli, 2004b).

2.5 CA 5: Audit

After the enterprise has created and carried out their security procedures, they must constantly measure and review their security strategy. A security audit enables the enterprise to evaluate the state of enterprise security against established criteria (Allen, 2005a). By periodically evaluating and measuring the effectiveness of security measures against an audit program based upon CSFs, the organization is able to continuously improve upon their strategic security plan to adapt to changing environments and situations (Caralli et al, 2005; Alberts et al, 2001; Caralli, 2004b).

2.6 CA 6: Process Management

Process management is the continuous improvement of the security definitions and security measures that encompass the strategic security plan (Allen, 2005a; Starr, Newfrock & Delurey, 2003). Process management ensures that the enterprise becomes a resilient enterprise. Enterprise resilience is the ability of the enterprise to adapt to changing risk environments (Starr et al, 2003). Enterprise resilience requires a proactive and adaptive approach and in this way can treat security as an on-going iterative process that has various lifecycles. The security strategy for the enterprise is an on-going process that changes and matures over time (Alberts et al, 2001; Caralli et al, 2005).

2.7 CA 7: Change Approach

In this approach an organization requires effective change management to enable and coordinate the analysis, creation, audit, and ongoing improvement to the strategic security plan (Allen, 2005a). Change management can be defined as

> *the process of assisting the organisation in the smooth transition from one defined state to another, by managing and coordinating changes to business processes and systems.*
>
> *Change management involves the effective communication with stakeholders regarding the scope and impact of the expected change; formal processes for assessing and monitoring the impact of the change on the stakeholders and their work processes, and identifying and developing effective and appropriate techniques to assist stakeholders to cope and adapt to the new technology* (Foster, Hawking & Stein, 2004).

This definition is inclusive and clearly identifies some of the main critical success factors involved in change management.

Therefore, the task and scope of security requires that the enterprise manage strategic security as a critical planning project. The use of organizational CSFs coupled with an enterprise security strategy provides the impetus to identify and create security measures for the critical assets of the organization. It is argued then that enterprise security itself should become part of the organization's CSF.

3 CONCLUSIONS

The critical success factors framework developed by the Carnegie-Mellon University views the organization as a unique institution with its own culture, environment, goals, objectives, and mission. This approach identifies security as one of the critical success factors for the organization. Subsequent strategic security planning is aligned with organizational business goals, drivers, and objectives.

One of the major advantages of the framework is that it provides the basis for the enterprise to identify

CSFs. With the emphasis on governance, protection of informational and physical assets, and ensures that best practices are able to adapt to changes within the organization through a change management strategy.

The CSFs framework is aimed at overcoming existing security flaws. Future research will test the strength of the framework within an enterprise.

REFERENCES

Alberts, C. and Dorofee, A. (2001). *OCTAVE criteria, version 2.0. Technical report.* December 2001.

Alberts, C. and Dorofee, A. (2002). *Managing Information Security Risks: the OCTAVE approach.* NY City: Addison-Wesley.

Allen, J. (2005a). *Governing for enterprise security.* (CMU/SEI-2005-TN-023).

Allen, J. (2005b). How Do I Know If I Have a Culture of Security? *Enterprise Risk Management and Governance E-Mail Advisor*, Cutter Consortium, April 2005.

Allen, J. (2004). Building a practical framework for enterprise-wide security management. *Carnegie Mellon University*.

AusCERT Survey (2006). Australian Computer Emergency Response team. Retrieved on October 8, 2006, located at www.AusCERT.org.au/

Boynton, A. (1984). *An assessment of Critical Success Factors*. Sloan Management Review.

Caralli, R. (2004a). *The critical success factor method: establishing a foundation enterprise security management*. *Technical Report,* (CMU/SEI-2004-TR-010).

Caralli, R. (2004b). *Managing for Enterprise Security*. *Technical Note, (*CMU/SEI-2004-TN-046).

Caralli R. and Stevens, J. (2005). Focus on Resiliency: a process-oriented approach to security. *32nd Annual CSI Conference and Exhibition, November 14 - 16, 2005 Washington, DC*

Caralli, R. and Wilson, W. (2004). Applying CSFs to Information security planning. *Carnegie Mellon University*

Dalton, D. (1995). *Security management: business strategies for success.* Butterworth-Heinemann: USA.

Dalton, D. (1997). *The art of successful security management.* Butterworth-Heinemann: USA.

Dalton, D. (2003). *Rethinking corporate security in the post 9/11 era.* Butterworth-Heinemann: USA.

Foster, S. V, Hawking, P., Stein, A., (2004). The Forgotten Critical Success Factor in Enterprise Wide System Implementations, Proceedings of the 15th Australasian Conference on Information Systems 2004, pp. 1-10.

Handy, C. (1996). The gods of management. *Executive Book Summaries*, 18(2), 1-8.Herold, R. (2004a). *The practical guide to securing assets*. Realtimepublishers.com.

Herold, R. (2004b). *The practical guide to managing risk*. Realtimepublishers.com

Information Security Forum (ISF) (2005). *The standard of good practice for information security*. Retrieved May 18, 2006, from www.isfsecuritystandard.com/pdf/standard.pdf.

Information Systems Security Alliance (ISSA) (2004). *Generally Accepted Information Security Principles (GAISP) V3.0*. Retrieved May 17, 2006, from www.issa.org/gaisp/_pdfs/v30.pdf .

International Standards Organization (ISO) (2005). *ISO/IEC 17799* (2nd Ed.). Geneva, Switzerland: ISO.

IT Governance Institute (ITGI) (2005). *COBIT 4.0*. Rolling Meadows, Illinois: IT Governance Institute.

IT Governance Institute (ITGI) (2006). *Information security governance: guidance for boards of directors and executive management* (2nd Ed.). Rolling Meadows, Illinois: IT Governance Institute.

McCarthy, L. (2003). *IT security: risking the corporation*. Upper Saddle River, New Jersey: Prentice-Hall.

Millard, E. (2004). *The Proactive vs. Reactive Security Approach*. Processor, Vol.26 Issue 8

Rockart, J. F. (1979). *Chief executives define their own data needs*. Harvard Business Review

Rockart, J. F. and Bullen, C. V. (1981) *A primer on critical success factors*. CISR Working Paper, 69.

Schein, E. (1988). Defining Organisational Culture. Jossey-Bass: London.

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *The Information Management Journal*, July/August 2005, 60-66.

Starr, R., Newfrock, J., and Delurey, M. (2003). *Enterprise resilience: managing risk in the networked economy*. Retrieved May 17, 2006, from www.boozallen.com/media/file/139766.pdf.

Straub, D. W. and Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, *22(4)*, 441-46