Security Architecture in a Collaborative De-Perimeterised Environment: Factors of Success

Yulia Cherdantseva[1] · Omer Rana[1] · Jeremy Hilton[2]

[1]Cardiff University
{y.v.cherdantseva | o.f.rana}@cs.cardiff.ac.uk

[2]Cranfield University
j.c.hilton@cranfield.ac.uk

Abstract

Security Architecture (SA) is concerned with such tasks as design, development and management of secure business information systems. These tasks are inherently complex and become several orders of magnitude more sophisticated in a Collaborative De-Perimeterised Environment (CDePE). Although significant research exists about the technical solutions that may be used in a CDePE, we believe there is an important gap in current literature in addressing the specifics of collaboration and de-perimeterisation at the stages of design and management of a SA. This paper discusses how a CDePE is addressed in the ISO/IEC 27000 series of standards and identifies ten factors, besides technical ones, that are important for the success of a SA. This paper emerged as a result of an analysis of the current state of the information security discipline and of the modern trends in the discipline.

1 Introduction

Many disciplines have adopted the term *Architecture* from the science of designing and erecting buildings. The term is widely used in computer and information sciences; the field of information security is not an exception. As town building architecture defines rules for the construction of buildings, Security Architecture (SA) is concerned with the design and development of secure business information systems, i.e. systems that are free from danger and damage, reliable and resistant to failures and attacks [ShCL05: p.2].

The main aim of a SA is overall business security. A SA generally provides a framework for enabling security controls of different layers to operate coherently together and depends on three aspects [ShCL05: pp.19-24]:

- The business goals of an organisation implementing it;
- The environment in which an organisation operates;
- The technical capabilities available at the current phase of Information and Communications Technologies (ICT) evolution.

A SA is often investigated purely from a technical viewpoint, whereas the impact of the business goals and the environment on a SA is ignored. We believe that the environment in which an organisation operates is very important and should be taken into account while developing

Cherdantseva Y., Rana O., Hilton J., "Security Architecture in a Collaborative De-Perimeterised Environment: Factors of Success", ISSE Securing Electronic Business Processes, Prague 22-23 November 2011. Highlights of the ISSE 2011 Conference, pp. 201-213

and maintaining a SA. The tasks of SA as a science are inherently complex and become several orders of magnitude more sophisticated in the present environment, which we refer to as a Collaborative De-Perimeterised Environment (CDePE) and describe below.

The term *De-Perimeterisation* was coined by the Jericho Forum (JF), an international association of organisations that concentrates on the issues of secure business in a networked environment. The term refers to the erosion of an organisation's hard perimeter in response to the evolution of ICT and consequent change of business needs. Formally, the JF describes De-Perimeterisation as "the concept of architecting security for the extended business boundary and not an arbitrary IT boundary" [OGJF07].

Thus, a CDePE is an environment where third parties gain access to data and services hosted by the organisation internally and, similarly, the organisation accesses data and services hosted by other organisations. Previously, the distinction was clear: there were people inside the perimeter (staff) who were fully trusted and people outside the perimeter (non-staff) who were not trusted. At present, organisations need to allow access to data not only to its staff - remote and mobile, but also to service providers, collaborators, authorities and customers. Any organisation, to a greater or lesser degree, participates in collaboration and information sharing, works in a distributed environment and has started to exploit Cloud computing capability (mostly for remote data storage, but also, in some instances, for outsourcing high throughput computation) in order to reduce costs and to increase efficiency and commercial profit. As a result, in a CDePE perimeters of organisations erode and "closed" systems no longer exist.

We do not consider a de-perimeterised environment as an equivalent of a distributed environment. A distributed environment may also have a hard perimeter, whereas de-perimeterisation accentuates a need even for a distributed environment to soften its boundaries. Nor do we consider Cloud computing to be the only idiosyncratic feature of the stated environment. Cloud computing is only one many aspects of a CDePE and we discuss it in Section 3.8. A CDePE reflects the complexity that emanates from a plethora of activities, including collaborative information sharing, Cloud computing, remote and mobile working and from the cascading impact of the intensive linkages between them.

An open architecture of an organisation with a softened perimeter provides business opportunities, but, at the same time, makes information security a greater challenge. With the unprecedented level of interconnectivity available today, previously used strategies of perimeter security are unsustainable. An approach to information security is required that allows an organisation to operate within a soft perimeter and to protect information outside of the organisation's perimeter as well as inside it. This new approach is based on multi-layered security and accumulates protection capabilities of technologies, organisational measures, human factors and legislation.

Currently, within de-perimeterisation research a strong emphasis is placed on technologies [OGJF07]. However, de-perimeterisation is a socio-technical phenomenon worthy of detailed research not only from the standpoint of technical network specialists, but also from the standpoint of managers, system and security architects. Although significant research exists about technical solutions that may be used in the CDePE, there is an important gap in the current literature in addressing peculiarities of this environment at the stages of design, development and management of a SA. Therefore, to cover this gap, we attempt to summarise and debate information security issues relevant to managers, system and security architects. Our aim is not a development of a new framework for a SA, but rather an identification of factors that are essential for the success of a SA in addition to any existing framework.

Cherdantseva Y., Rana O., Hilton J., "Security Architecture in a Collaborative De-Perimeterised Environment: Factors of Success", ISSE Securing Electronic Business Processes, Prague 22-23 November 2011. Highlights of the ISSE 2011 Conference, pp. 201-213

The remainder of this paper is structured as follows: Section 2 discusses how a CDePE is addressed in the ISO/IEC 27000 family of standards that provides a widely used framework for a SA. Section 3 outlines the factors that deserve to be taken into account while designing, implementing and managing a SA. Section 4 draws conclusions from the preceding discussion.

2 How the ISO/IEC 27000 series of standards addresses a CDePE

The ISO/IEC 27000 series of standards is published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), and reserved for information security matters. ISO/IEC 27001:2005 emulates the success of its predecessor BS7799 and sets the trend for this growing family of standards. It specifies the requirements towards an Information Security Management System (ISMS) and covers a wide range of issues, such as risk assessment; management responsibilities and commitment; resource management and provision; training, awareness and competence. Another constituent of the series is ISO/IEC 27002:2005 that contains a code of practice for information security management.

Both ISO/IEC 27001 and ISO/IEC 27002 were developed at the time when the business world was not so considerably affected by de-perimeterisation. Although the ISO/IEC 27000 family provides some basic recommendations that are applicable in a CDePE, these recommendations should be significantly extended and updated by an organisation wishing to make use of them in the present environment. Below we consider how a CDePE is addressed in ISO/IEC 27001 and ISO/IEC 27002, as well as we discuss any omissions in the standards. We start our analysis with ISO/IEC 27001:2005, where Section 4.2.1 a) suggests that an organisation shall

> *"Define the scope and boundaries of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology, and including details of and justification for any exclusions from the scope."*

In the case of a "closed" system, it is easy to assume that the boundaries of the ISMS are equal to the boundaries of an organisation, whereas the task of defining the boundaries and the scope of the ISMS in the de-perimeterised environment is more complicated. According to the definition, the ISMS is a "part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security" and as such it "includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources" [BSIS05]. In the CDePE practices, procedures and policies may spread over multiple organisations that work together in order to achieve a common goal. Therefore, to define the boundaries of the ISMS an organisation should decide whether it should include service providers, collaborators and customers in the scope and to what extent they should be included. Neither ISO/IEC 27001, nor ISO/IEC 27002 provides any further details about establishing the scope and boundaries of the ISMS.

Section 4.2.3 f) of ISO/IEC 27001:2005 states the need to "undertake a management review of the ISMS on a regular basis to ensure that the scope remains adequate". Section 7.3 of the same document further explains that the modification of the ISMS may be done in response to internal and external events, including changes to contractual obligations and legal requirements. The above, should be translated into the requirement to conduct a revision of the ISMS

boundaries with every change in collaboration or information exchange agreements, as well as with any change within an external party that affects common business processes or policies.

> *"4.2.4 c) communicate the actions and improvements to all interested parties with a level of detail appropriate to the circumstances and, as relevant, agree how to proceed."*

In a CDePE information security of one organisation may strongly depend on the reliability of the ISMS of other organisations. Thus, a change or an improvement in the ISMS, that affects cross-organisational business policies must be pre-agreed between the involved parties and, where possible, must be developed in co-operation. The collaborating parties should be adequately prepared and relevant security controls should be put in place before such a change goes live.

Section 4.3.2 of ISO/IEC 27001:2005 suggests the need to protect and control documents required by the ISMS and, more specifically, to establish a procedure to define the management actions needed to ensure identification of documents of external origin. In a CDePE, in addition to identification of an external document, it is also needed to recognise the level of its confidentiality and to implement pertinent controls and procedures in order to process, store and transmit a document in accordance with the author's security requirements. The document may have a certain level of access in the original information system, but when transferred to another system the privilege rights may be ignored or wrongly interpreted. The procedures and policies related to the processing, storage and transmission of the external documents should be agreed between the parties involved. ISO/IEC 27002:2005 in Section 7.2.2 declares that one of the possibilities to achieve appropriate security of external documents is through the ability "to interpret the classification labels from other organisations." In fact, consistent cross-system document level security may be reached through the integration of information systems of collaborating parties. More efficient approaches to secure processing of external documents may include agreed-upon document classification schema and integrated authentication system [Simm04].

Delving deeper into this question, Sections A.7.2.1 and A 7.2.2 require classification of information within the organisation, its labelling and appropriate handling. In a CDePE, an organisation should not only recognise and treat external documents in accordance with the author's security guidelines, but also protect its own information assets outside of its perimeter. An organisation should ensure that its information is treated in conformance with the organisation's security requirements outside the organisation's perimeter. One of the modern concepts for user-friendly communication of security needs and controls on inter-organisational level is the icon-based labelling scheme known as Protective Commons [HiTa08]. Protective Commons emulate Creative Commons retaining a focus on document protection.

Information security associated with outsourcing is perfunctorily covered by Section A.6.2 of ISO/IEC 27001:2005 that defines the requirement to identify risks related to the involvement of external parties and by Section A.10.2 that defines the requirements to monitor the conformance of the services provided by third parties to the agreements. Corresponding security controls are outlined in Sections 6.2 and 10.2 of ISO/IEC 27002:2005. The above sections consider neither the risk management perspective of outsourcing [Isec11b], nor the requirements towards outsourcing agreements. In the environment where an organisation significantly depends on the services provided by third parties, financial penalties should be established for information security breaches occurring due to the fault of service providers as well as for failures to provide the service (i.e. meet particular Quality of Service requirements). This

measure identifies the underlying financial intensives that encourage service providers to pay more attention to customers' information security [Ande01].

Section 12.1 of ISO/IEC 27002:2005 defines the need for security requirements to be established at the early stages of the information system development process. Hence, security requirements for multi-organisational business processes and integrated information systems should also be defined at the initial stage of system requirements formulation and extended at the stage of system modelling and design. There is a significant gap in the research and practice in this area, although some attempts to model security aspects in the Business Process Modelling Notation (BPMN) collaboration diagram exist [RFMP07].

Both ISO/IEC 27001 and ISO/IEC 27002 address information security issues within a single organisation. However, with emerging interest in e-commerce, supply chain and joint product development, where complex business processes spread over multiple organisations, the overall control and consistency of procedures across organisations are essential. In 2011, in order to address this evolving area of inter-organisational processes the Object Management Group (OMG) introduced into the BPMN 2.0 the concept of choreography, the essence of which is the coordination of communications between organisations or processes without an overarching process in charge of such coordination [OMG11]. Addressing information security in choreography process is a critical challenge in virtue of the fact that security in these processes could only be achieved if business processes of all parties involved and communications between them are secure.

While collaboration and information sharing leverage new business opportunities, it is important to prevent exposure of strategic organisational knowledge. The ISO/IEC 27000 is focused on data and information assets and does not actually distinguish knowledge as a valuable asset. This, consequently, leads to a failure to address threats to this critical asset caused by collaboration and de-perimeterisation [AlSa10]. The importance of distinguishing knowledge assets as well as assessing its business value is derived from a necessity to retain strategic advantage in a highly competitive world.

The analysis of the ISO 27000 series of standards leads to a conclusion that although the series provides strong basis for information security, it does not comprehensively reflect the complexity of a CDePE. The series is actively growing in response to a rapidly changing environment. Thus, several new standards in this series, that will more coherently address the modern environment, are expected to emerge within the next 2-3 years. The release of ISO/IEC 27036 - *IT Security - Security techniques - Information security for supplier relationships*, a multi-part standard addressing risks to information related to the external parties, is expected in 2012. The standard is anticipated to provide a solid basis for security of outsourcing and, potentially, for Cloud computing as a form of outsourcing [Isec11b]. ISO/IEC 27010 - *Information Technology - Security techniques - Information security management for inter-sector and inter-organizational communications*, another emerging standard of the series, is a supplement to ISO/IEC 27001:2005 and ISO/IEC 27002:2005. It considers in more detail the inter-organisational information security issues and information exchange between organisations that are only briefly addressed by other existing standards [BSIS11]. A committee draft of the standard (that is currently available for review) still does not address all the issues discussed above. The draft expires on 31 August 2011 and hopefully the final version will cover issues relevant to a CDePE more exhaustively.

Thus, the requirements and controls outlined in ISO/IEC 27001 and ISO/IEC 27002 do not comprehensively cover the issues of information security that arise in a CDePE from manage-

rial and system architects' perspectives. In the next section we list and analyse the issues that should be taken into account by managers, system and security architects in addition to the security requirements defined in published standards of the ISO/IEC 27000 series.

3 Factors of Success

3.1 Comprehensive and Systematic Approach

Any organisation that aims to increase commercial profit, gain trust of partners and effectively and efficiently use new technologies in a CDePE should protect information in a comprehensive and systematic manner. Comprehensive protection refers to the exploitation of countermeasures of different layers in order to achieve "complete" security. Countermeasures could include, but are not limited to an organisation's strategy, policies and procedures; business processes; training and educational programs; technical security controls; and legal measures. Reliance on any single layer of defence does not often provide adequate security. Security controls of different layers should support information security concurrently. If any of the controls fail, the others should be sufficient to provide an adequate level of information security until the functionality of the failed control is restored. With regards to the comprehensiveness of information protection, a SA helps to avoid a piecemeal approach to information security: rather than applying security countermeasures in an ad-hoc manner, a SA creates a holistic enterprise-wide picture and allows to structure inter-relationships between the various measures being considered. The additional task of a SA in a CDePE is to provide a comprehensive approach to inter-organisational business processes and accompanying information sharing.

A systematic approach refers to addressing information security at every stage of a system lifecycle, including such stages as requirements analysis, system design, implementation and maintenance. Hence, security requirements in multi-organisational projects should be agreed at the initial stage of system requirements formulation and at the stage of system design. At present, information security at cross-organisational business processes is very rarely addressed at the design level. Information security is often left for the computer specialists to sort out as an a posteriori task.

The above implies that a CDePE, that significantly affects a SA, should also be addressed at every protection layer and at every stage of a system development lifecycle. We believe that a comprehensive and systematic approach to information security and, consequently, to the specifics of the environment in which the system (and therefore the SA) should operate is the most important and unconditionally required factor of a successful implementation of a SA.

3.2 Adjusted Security Framework

It is often mentioned that a good security framework should serve as a road map for information security. An organisation should carefully consider and choose a security framework to follow, since the belated change of a framework may lead to unnecessary additional work and costs. Despite a plethora of existing security frameworks promising high standards of information protection, an organisation should not entirely rely on any of them. There are two underlying reasons for this. First, existing standards and best practices fail to address the effects of changing environment and newly emerging threats in a timely way. As alluded to in Section 2 of this paper, commenting on the ISO/IEC 27000 series of standards, it takes several years to adjust the series to the new environment. Second, neither bodies that develop secu-

rity standards and frameworks, nor certification organisations are financially or in any other way accountable for the security failures in organisations that follow the standards and practices. In fact, information security strongly depends on economic motives, but in this case such motives are absent [Ande01].

Thus, it is always up to an organisation to fine-tune a framework for the current environment as well as to adjust it to a particular business context. The challenge for a contemporary security framework is to find an optimum balance between information sharing and information protection staying within legal and compliance regulations.

3.3 Senior Management Role

Section 6.1.1 h) of ISO/IEC 27001 states that management should "ensure that the implementation of information security controls is co-ordinated across the organization." In the present landscape, in addition to co-ordinating the implementation of security controls within the organisation, senior management should be involved in agreeing security controls with collaborating parties and other members of the information exchange. Security aspects of inter-organisational information exchange require attention at the level of senior management because only such individuals (and stakeholders) have the required level of understanding of business needs to be able to answer questions such as:

- Who are the prospective strategic partners?
- To what degree does a company want to share or segregate its information?
- How much does the company trust a partner or a third party?
- What is the liability for information misuse by partners and third parties?

Consequently, in a CDePE the following responsibilities should be included into the scope of managers in addition to those declared in ISO/IEC 27001:2005:

- Within the organisation's security strategy define the level of trust for each external party;
- Collaborate with the third parties' management in order to agree cross-organisational security strategy, policies and controls;
- Ensure cross-organisational consistency of security strategies, policies and controls within the collaborating community;
- Ensure adequate protection of the organisation's information and knowledge assets outside of the organisation's perimeter.

3.4 Responsibilities Allocation and Required Qualities of Information security Personnel

A CDePE stems new responsibilities not only for managers as discussed above, but also for information security personnel. Some newly emerging responsibilities may be as follows:

- Communicate with external parties in order to develop consistent cross-organisational security policies and procedures;
- Develop and implement procedures for informing relevant external parties about changes in organisation's security strategies, policies and procedures;
- Address security concerns in relationships with customers.

Furthermore, information security personnel should co-ordinate all activities that aim to protect information in order to prevent omissions that may arise due to a granular approach. In

many cases information sharing needs are defined at the business level, some security controls are realised to protect information at the technical level, liability for information misuse is defined in agreements by legal personnel – all these measures contribute to information security and, therefore, require overarching administration. ISO/IEC 27002:2005 requires clear definition and allocation of information security responsibilities. Thus, the importance of the activities mentioned above should be recognised by an organisation and responsibilities for them appropriately allocated.

In addition to clearly defined responsibilities, information security personnel should have up-to-date technical knowledge, understanding of business and economics, and good communication skills. However, the most important quality of information security personnel in the current rapidly altering environment is open-mindedness. At present, there is no commonly agreed definition of information security and the set of security goals is variable within security standards: some standards limit the realm of information security to confidentiality, integrity and availability [CNSS10, ISACA08]; others include non-repudiation, accountability, reliability and authenticity [ISO09]. The limitation of the scope of information security and, consequently, of personnel responsibilities to the certain goals may lead to the overlooking of new threats and vulnerabilities that are constantly emerging in the ever-changing world of ICT. Therefore, staff responsible for information security should perceive an overall protection of information as their major goal, rather than the achievement of goals predefined in standards. Moreover, personnel should be ready to protect information from both known and unknown threats and quickly adapt to the new environment. We refer to this important quality of information security personnel as open-mindedness.

3.5 Up-to-date Security Policies and Procedures

The organisation's security policies and procedures should be constantly revised and improved in order to be adequate for a rapidly changing environment. They should cover continually emerging technologies in a timely manner. Therefore, the process for the introduction of improvements should be predefined and established. In a CDePE, this process apart from development and implementation of an improvement should include the agreement of an improvement with external parties, raising awareness among internal and external personnel, and analysis of external parties' feedback regarding an improvement introduced.

Most recently the policies and procedures that address threats emerging from mobile communications and social networking are the focus of security specialists. If use of mobile devices is a business necessity for an organisation, then mobility should be appropriately addressed by security policies. The policies may be, for instance, as follows:

- Access to a mobile device must be protected by a password of a certain strength;
- In case of the loss of a mobile device an organisation retains the right to destroy all the data on the device;
- The same security policies should be applied to the mobile device independent whether it is within an organisation's network or outside it.

With the rapid growth of the social networking industry the risk of data leakage through social networks becomes more significant. In 2010, 20% of companies encountered data loss via social networking sites [Good10]. To address this threat, security policies should clearly define which information may and may not be exposed at social networking sites, blogs and professional communities.

3.6 Involvement of Interested Parties

ISO/IEC 27001:2005 states that security actions and improvements should be communicated to all interested parties where interested parties are implicitly limited to the employees and stakeholders of an organisation. There are two extensions required to the above statement in the CDePE. First, the scope of the interested parties becomes broader: apart from interests of internal parties, interests of employees and stakeholders of external organisations involved should be taken into account while taking decisions about security actions. This is due to the fact that while the most of the security changes done by the organisation affect the organisation's personnel productivity, some of the changes may affect productivity of the personnel of other organisations that use services or data provided by the organisation. Therefore, it is preferable to reach a consensus not only between security people and internal users, but also between security people and external users in order to prevent security improvements being banned as reducing productivity.

Second, a more in-depth involvement of external parties is required. It should not be limited to the communication of security policies to external parties. Security policies and procedures should be planned, designed and implemented in close rapport with interested parties. The level of involvement of a party in the above processes may vary depending on the status of the party: service provider, collaborator, authority or customer. Section 5.1.1 of ISO/IEC 27002:2005, for example, declares the requirements towards an Information Security Policy Document (ISPD), which is considered in the standards as a purely internal document that only is some cases communicated to the external parties. In the CDePE, the ISPD should equally address protection of information within and outside an organisation's perimeter and, as such, parts of the document that cover security of collaborative information sharing should be developed with the close cooperation of the parties involved.

3.7 Information Security Training and Awareness

Training and awareness programs require regular revisions and updates in order to remain adequate for a rapidly changing environment. The programs should instruct employees in a clear form about how to do business securely using new technologies and make them aware in a timely way about emerging threats. The areas that at present are rarely or poorly addressed by training and awareness programs and require more attention are social networking, mobile communications and social engineering.

Furthermore, the reasoning behind information security countermeasure should be made clear to personnel in order to overstep rote compliance [BoJe02]. Rote compliance is only sufficient until a situation that is not covered by any of the existing policies or procedures occurs. At present, hardly any organisation, in terms of its security policies and procedures, will be able to keep pace with the fast evolution of technologies. Therefore, to solve this problem any security training or awareness program should pursue two major aims. Firstly, to teach system users to exploit common sense when using progressive technologies or working in unforeseen circumstances. Secondly, to educate users to perceive information security as everyone's personal responsibility, rather than something that has nothing to do with their day-to-day activities. As any information security measure - technical or organisational - could be disregarded by simple carelessness, an understanding of the reasoning behind security measures and an appreciation of personal responsibility may help to improve information security with minimal cost.

Cherdantseva Y., Rana O., Hilton J., "Security Architecture in a Collaborative De-Perimeterised Environment: Factors of Success", ISSE Securing Electronic Business Processes, Prague 22-23 November 2011. Highlights of the ISSE 2011 Conference, pp. 201-213

3.8 Approach to Outsourcing

Many organisations outsource IT functions: the reason is obvious - outsourced services may cost several times less than maintaining in-house IT. Cloud computing, a modern form of outsourcing, significantly reduces business costs. The problem that arises with outsourcing is that organisations often ignore such in-house activity as development of information security strategy and inconsiderately rely on outsourcing companies in terms of security, forgetting that security is not a feature that outsourcing companies provide by default. Security measures supplied should meet requirements of the organisation's information security strategy and policies, should be carefully negotiated and stated in contracts as well as financial penalties for the information security breaches occurred by fault of service provider. For Cloud computing the contract should, for example, prevent access of the cloud provider's personnel to confidential data, prevent data sharing with unauthorized third parties, require destruction of data after termination of the contract as well as state the liability for data misuse. The new member of the ISO/IEC 27000 family – ISO/IEC 27036 - *IT Security - Security techniques - Information security for supplier relationships* – promises to address information security issues in outsourcing in detail. The standard is currently in preparation.

Whereas development security strategy by an organisation itself is preferred, outsourcing strategy development is also possible, but should be done with the active involvement of an organisation's management, which is accountable and is the only party that has an in-depth understanding of the business needs.

Finally, it is not a question of what is more secure - in-house or outsourced IT. It is a question of a SA to be adjusted to a preferred way of operation [ShCL05: p.146].

3.9 Security Return on Investment

Security Return on Investment (ROI) is a very popular topic. There are different approaches to economics of security. Some authors argue that security should be evaluated in a similar way to other business projects in terms of ROI. Others, on the contrary, claim that information security does not have an ROI. Third argue that security is more similar to insurance as it reduces risks to business and prevents possible losses.

In fact, cost and benefits calculations based on risk analysis are needed as they serve as a bridge between managers and security specialists. They help to translate security concerns through probability arithmetic into monetary terms that are familiar to management and allow estimation of security projects [KoDK00]. Security projects *per se* are different from most business projects, although they have some similarity with PR and advertising projects in a sense that it is very hard to measure benefits, whereas costs are obvious. As a result, the standard way of ROI calculations is not always sufficient for security projects. It is possible to quantify the financial benefits and measure the effectiveness of information security, but adequate calculations and analysis are quite complex and time-consuming. Sherwood et al., for example, propose a method for security ROI calculations based on a set of 85 attributes, each with suggested metrics and measurements [ShCL05: pp.79-110].

Despite the difficulty of adequate calculations, a demonstration of ROI significantly increases popularity and, more importantly, the budget of a security project. Management quite often actively supports a security project at the initial stage, but loses interest in the project at further stages if they cannot see a positive ROI. Thus, to maintain management's support, finan-

cial benefits of information security measures should be quantified and clearly articulated to stakeholders and other interested parties at every stage of a security project.

The importance of the economic side of information security is lately recognised by ISO/IEC, which is currently in preparation of ISO/IEC TR 27016 - *IT Security - Security techniques - Information security management - Organisational economics*. The standard, which is expected to be released in 2013, will cover financial perspectives of information security [Isec11a].

3.10 Business Continuity

Any system may fail to some extent at a certain point. Therefore, the aim of a SA is not only to prevent security failures, but also to allow a system to fail in a "good" way, i.e. with minimum destruction and negative consequences to the business. In a CDePE, managers and security experts should be concerned with two questions with regards to business continuity. Firstly, how failure on the side of collaborators, service providers or other external parties involved may injure an organisation and what an organisation should do in a case of such a failure. Secondly, how a security failure on the organisation's side will affect external parties and what should be done to reduce or prevent a negative effect.

Section 14 of ISO/IEC 27002:2005, that describes information security aspects of business continuity management, does not comprehensively address issues relevant to involvement of external parties. In terms of the impact of external parties on an organisation the ISO/IEC 27000 series and, in particular ISO/IEC 27031:2011 - *Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity*, concentrates on ICT-related risks and does not consider risks of system failures that may crop up from business interdependencies [SKHA08].

A SA should be built to avoid the complete dependence of a system on external parties. If, for instance, important business data resides in the Cloud, additional remote backups could guarantee data availability, in case of the failure of a cloud service provider. Thus, the responsibility to develop a SA that will support business continuity in the interdependent environment resides with system and security architects, and should take appropriate place among their other duties.

4 Conclusion

The evolution of ICT recently resulted in a noticeable phenomenon referred to as *de-perimeterisation*. The significance of this complex socio-technical phenomenon is still underestimated. This implies that the specifics of the present environment, affected by collaboration and de-perimeterisation, are often overlooked or ignored at the level of business strategy, system design and in a SA in general. To cover this gap, the paper presented an overview of the factors that are important to be taken into consideration while developing and managing a SA in a CDePE. The factors described in the study are necessary, but not sufficient conditions for a successful SA. Nevertheless, addressing the factors covered in this paper will significantly increase the chances of an organisation to build a successful SA.

This work emerged as a result of an analysis of the modern trends and the hot topics of the information security discipline. The value of the paper is also in sketching a contemporary picture of a successful SA adapted to the interconnected landscape and in outlining areas worthy

of attention and subsequent research. Hence, it may be of interest to managers, system architects, information security professionals and young researchers.

References

[AlSa10] Aljafari, R., Sarnikar, S.: A Risk Assessment Framework for Inter-Organizational Knowledge Sharing. Sprouts: Working Papers on Information, 2010 [online]. Available at: http://sprouts.aisnet.org/880/1/KMDSS_Sprouts.pdf [Accessed: 10 July 2011]

[Ande01] Anderson R.: Why Information Security is Hard – An Economic Perspective. Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual, pp. 358-365

[BoJe02] Boyce J., Jennings D.: Information Assurance: Managing Organizational IT Security Risks. Butterworth-Heinemann (Elsevier Science), 2002, p.13

[BSIS05] BS ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems - Requirements. 2005, p.2, def. 3.7, 3.8

[BSIS11] Draft BS ISO/IEC 27010 Information Technology - Security techniques - Information security management for inter-sector and inter-organizational communications. Reference number of document: ISO/IEC FCD 27010, 2011

[CNSS10] Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010, p.37

[Good10] Goodchild J.: Survey: Fear of data loss, security risks via social media sites on the upswing, 2010 [online]. Available at: http://www.csoonline.com/article/616218/survey-fear-of-data-loss-security-risks-via-social-media-sites-on-the-upswing [Accessed: 10 July 2011]

[HiTa08] Hilton J., Tawileh A.: Sustained Control of Critical Corporate Information. 5th Middle East Chief Information Officer Conference & IT Exhibition, ME CIO 2008. Summit, Nov. 25, 26 & 27, 2008, Bahrain [online]. Available at http://www.jeremy-hilton.com/node/1 [Accessed: 30 July 2011]

[ISACA08] Information Systems Audit and Control Association: ISACA Glossary of Terms, 2008 [online]. Available at: http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf [Accessed: 10 July 2011]

[Isec11a] IsecT Ltd.: ISO/IEC TR 27016 - IT Security - Security techniques - Information security management – Organizational economics (DRAFT) [online]. Available at: http://www.iso27001security.com/html/27016.html [Accessed: 10 July 2011]

[Isec11b] IsecT Ltd.: SO/IEC 27036 - IT Security - Security techniques - Information security for supplier relationships (DRAFT) [online]. Available at: http://www.iso27001security.com/html/27036.html [Accessed: 10 July 2011]

[ISO09] ISO/IEC 27000:2009 (E) Information technology - Security techniques - Information security management systems - Overview and vocabulary, def. 2.19

[KoDK00] Kokolakis S., Demopoulos A., Kiountouzis E.: The use of business process modelling in information systems security analysis and design. Information Management & Computer Security, 2000, Vol. 8 Iss: 3, p.108

[OGJF07] The Open Group, Jericho Forum: Business rationale for de-perimeterisation, 2007 [online]. Available at:

https://www.opengroup.org/jericho/Business_Case_for_DP_v1.0.pdf [Accessed: 10 July 2011]

[OMG11] The Object Management Group: Business Process Model and Notation, Version 2.0, 2011 [online]. Available at: http://www.omg.org/spec/BPMN/2.0/PDF/ [Accessed: 10 July 2011]

[RFMP07] Rodríguez A., Fernández-Medina E., Piattini M.: A BPMN Extension for the Modeling of Security Requirements in Business Processes. EICE - Transactions on Information and Systems, 2007, Volume E90-D Iss. 4, pp. 745-752

[ShCL05] Sherwood J., Clark A., Lynas D.: Enterprise Security Architecture: A Business-Driven Approach. CMP Books, 2005

[Simm04] Simmonds P.: De-perimeterisation – this decades security challenge, presentation, 2004 [online]. Available at: http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-simmonds.pdf [Accessed: 10 July 2011]

[SKHA08] Sutton S., Khazanchi D., Hampton C., Arnold V.: Risk Analysis in Extended Enterprise Environments: Identification of Critical Risk Factors in B2B E-Commerce Relationships. Journal of the Association for Information Systems, Vol. 9, Nos. 3-4, pp. 151-174, 2008

Index